AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. Hrg. 110–417

AGENCIES IN PERIL: ARE WE DOING ENOUGH TO PROTECT FEDERAL IT AND SECURE SENSITIVE INFORMATION?

HEARING

BEFORE THE

FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY SUBCOMMITTEE

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

MARCH 12, 2008

Available via http://www.gpoaccess.gov/congress/index.html

Printed for the use of the Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

41–458 PDF WASHINGTON : 2008

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK L. PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

SUSAN M. COLLINS, Maine
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
NORM COLEMAN, Minnesota
TOM COBURN, Oklahoma
PETE V. DOMENICI, New Mexico
JOHN WARNER, Virginia
JOHN E. SUNUNU, New Hampshire

MICHAEL L. ALEXANDER, *Staff Director*
BRANDON L. MILHORN, *Minority Staff Director and Chief Counsel*
TRINA DRIESSNACK TYRER, *Chief Clerk*

FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY SUBCOMMITTEE

THOMAS R. CARPER, Delaware, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
BARACK OBAMA, Illinois
CLAIRE McCASKILL, Missouri
JON TESTER, Montana

TOM COBURN, Oklahoma
TED STEVENS, Alaska
GEORGE V. VOINOVICH, Ohio
PETE V. DOMENICI, New Mexico
JOHN E. SUNUNU, New Hampshire

JOHN KILVINGTON, *Staff Director*
KATY FRENCH, *Minority Staff Director*
MONISHA SMITH, *Chief Clerk*

CONTENTS

	Page
Opening statements:	
Senator Carper	1
Senator Coburn	10
Senator Coleman	20

WITNESSES

WEDNESDAY, MARCH 12, 2008

Hon. Karen S. Evans, Administrator for Electronic Government and Information Technology, U.S. Office of Management and Budget	5
Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office	6
Tim Bennett, President, Cyber Security Industry Alliance (CSIA)	8
Hon. Robert T. Howard, Assistant Secretary for Information and Technology, U.S. Department of Veterans Affairs	31
Susan Swart, Chief Information Officer, Bureau of Information Resource Management, U.S. Department of State	33
Darren B. Ash, Deputy Executive Director for Information Services and Chief Information Officer, U.S. Nuclear Regulatory Commission	35
Philip Heneghan, Chief Information Security Officer, U.S. Agency for International Development (USAID)	36

ALPHABETICAL LIST OF WITNESSES

Ash, Darren B.:	
Testimony	35
Prepared statement	115
Bennett, Tim:	
Testimony	8
Prepared statement	92
Evans, Hon. Karen S.:	
Testimony	5
Prepared statement	49
Heneghan, Philip:	
Testimony	36
Prepared statement	124
Howard, Hon. Robert T.:	
Testimony	31
Prepared statement	98
Swart, Susan:	
Testimony	33
Prepared statement	106
Wilshusen, Gregory C.:	
Testimony	6
Prepared statement	54

APPENDIX

Questions and Responses submitted for the Record from:	
Ms. Evans	130
Mr. Wilshusen	140
Mr. Howard	147
Ms. Swart	155
Mr. Ash	174
Mr. Heneghan	189

AGENCIES IN PERIL: ARE WE DOING ENOUGH TO PROTECT FEDERAL IT AND SECURE SENSITIVE INFORMATION?

WEDNESDAY, MARCH 12, 2008

U.S. SENATE,
SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT,
GOVERNMENT INFORMATION, FEDERAL SERVICES,
AND INTERNATIONAL SECURITY,
OF THE COMMITTEE ON HOMELAND SECURITY
AND GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 2:32 p.m., in Room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Subcommittee, presiding.

Present: Senators Carper, Coleman, and Coburn.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Welcome one and all. It is good to see you, and we thank you for making time in your schedules today to visit with us.

I believe this hearing was originally scheduled for tomorrow, and we have asked you to come a day early, and we are grateful that you are able to fit us into your schedule.

We get to do something tomorrow that we call in the Senate "Vote-a-Rama," and it is all day, all night that we vote. And we are working on the budget resolution this week, and from time to time, we stack votes. And we are going to stack a whole lot of votes. We did not vote Monday. We did not vote Tuesday. We did not vote today. We probably will not vote today. And, instead, we are going to just save it all until tomorrow. When we vote every 15 minutes tomorrow, all day long, it would be pretty hard to squeeze in a hearing. We would just get little snippets from the witnesses, and we would be back to vote, so this works out a lot better for us and hopefully for you, too.

But I appreciate or apologize for any inconvenience that has come from this.

I think we are going to be joined by Senator Coleman of Minnesota in a little bit.

Senator Coburn is involved on the floor with the budget, and so he may or may not be able to join us, but he is certainly interested in this issue. He and I have talked about it any number of times, and I suspect that you will be receiving some questions from him

if he does not come in person to ask questions. I am sure you will be hearing from him in the future.

But our thanks to our witnesses for joining us today. This hearing marks what I hope will be really the beginning of our proactive efforts to secure one of our most threatened and important national resources, and that is our sensitive information, not just about us as individuals, as human beings, but our businesses and our governmental units, and so forth.

Every day our government's computers experience thousands of attacks, led by individuals seeking to gain access, and in some cases, to taxpayer records. In other cases, to our medical records; in some cases to our Social Security numbers, to proprietary business information, and to military secrets, just to name a few.

Our public expects that agencies holding this information, particularly their personal information, will take every precaution necessary to ensure that it is secured, and well protected.

However, despite the progress report in the Office of Management and Budget's most recent report, I feel like we are still very much at risk.

Our inability to secure Federal information networks and protect the information they contain leaves American citizens open to threats that involve identity theft. And I guess if we go around the room here, we could ask do you know who has been a victim of identity theft. And let me just ask the audience. Do you know somebody who has been a victim of identity theft? Raise your hand, if you have. That was 17 hands that went up.

That is about a third of the hands of the people that are here.

But not only do we have worries and concerns about our personal identity and identity theft, but the threat that we face even places our national security at risk.

For example, according to a report released I believe last Monday by the Department of Defense, the U.S. Government and our allies around the world have come under attack in the past year by hackers from addresses that appear to originate from the Chinese government. Maybe we will have something to talk with them about at the Olympics. We can sort of—cocktail talk with the Chinese we will raise this as we go through the Olympics.

But these hackers were able to compromise information systems at government agencies, our government agencies, at defense-related think tanks, at contractors and at financial institutions as well.

Germany's domestic intelligence agency, the German Office for the Protection of the Constitution, has accused China of sponsoring these attacks almost daily in an attempt to intensively gather political, military, corporate, strategic, and scientific information in order to bridge their technological gaps as quickly as possible.

Actually most of that last sentence that I gave or that I read was, I think, a quote from the Germans themselves and sort of pointing out what they think is going on here.

The threat of a Nation state cyber attack is very real, too. Last year, in Estonia, an attack led by Russian nationalists was coordinated through online chat rooms and Web sites. This cyber war, if you will, as the newspapers called it, shut down Web sites of Esto-

nian organizations, including the Estonian parliament, banks, ministries, newspapers, and broadcasters.

But we do not have to look overseas to find threats to our information security. Sometimes we only have to look in our own backyard. Just last year, the Veterans Affairs Department had an external hard drive stolen, exposing sensitive personal information on close to, I think, two million of my fellow veterans. But the Veterans Affairs is not the only example. The Department of Defense, the Department of Transportation, the Department of Commerce, the Department of Health and Human Services, Homeland Security, Education, Agriculture, and the Department of State were all compromised by current or former employees. And I understand that in many cases, it is the former employees or former contractors that are doing us in in some of these instances.

But these incidents are not simply unacceptable. They are more than unacceptable. I have a feeling that if a private sector company, like a bank or an insurance company, that is entrusted with sensitive data were as vulnerable as some of our Federal agencies seem to be, they would be out of business pretty quick.

The Federal Information Security Act (FISMA), came out of a recognition a few years ago, I want to say about 2002, the recognition of the critical importance of protecting our information systems. Since then, agencies have made extraordinary progress in implementing crucial information security measures, and they should be acknowledged and complimented for their efforts. And we acknowledge those efforts, and we compliment them where they have occurred.

Having said that, I am concerned that 5 years after the passage or enactment of FISMA, agencies may be falling into the trap of complacency and just checking boxes to show compliance with requirements written into a bill.

So once again, I want to thank our witnesses today for joining us, for your preparation for your testimonies today, and we look forward to hearing how Congress, how we in the Legislative Branch of this government can help in protecting our sensitive information for domestic threats and from foreign threats as well.

We are going to leave the record open for Senator Coburn and others on the Subcommittee who would like to submit opening statements.

We have done a lot of research on each of the witnesses and come up with some interesting things about your past.

But let me just say our first witness will be Hon. Karen Evans, the Administrator for E–Government and Information Technology for the Office of Management and Budget. You have testified before this Subcommittee on several occasions. We are grateful for that and for you being here today.

Ms. Evans directs the activities of the Chief Information Officer Council and oversees the implementation of IT throughout the Federal Government, including responsibilities in the areas of capital planning and investment control, information security, privacy, and the preservation of government information.

Prior to becoming Administrator, Ms. Evans was the Chief Information for the Department of Energy. What years were you there?

Ms. EVANS. I was there for a total of 20 months, so it was 2002.

Senator CARPER. OK.

Ms. EVANS. From 2002.

Senator CARPER. All right. There, Ms. Evans was responsible for the design, implementation, and continuing successful operation of information technology programs and issues throughout the Department.

In addition, Ms. Evans was Director of the Information Resources Management Division, the Office of Justice Programs at the U.S. Department of Justice, and there she was responsible for the management and successful operation of information technology programs.

She holds a bachelors in chemistry and a Masters of Business Administration from a college located in the State where I was born, West Virginia—the University of West Virginia—a Mountaineer. I just had an emotional conversation with some folks earlier today about your football coach, who's headed off to Michigan. I went to Ohio State, so we had a good time on this conversation. But about your football coach—headed off to Michigan, and they—it looks like West Virginia lost all their top five recruits, so people are not too happy.

Our next witness is Greg Wilshusen, Director of Information Security Issues at the Government Accountability Office, where he leads information security-related studies and audits of the Federal Government.

He has over 26 years of auditing, financial management, and information systems experience and is a certified public account, a certified internal auditor, and certified information systems auditor. That is a lot of certifieds.

But he holds a B.S. degree in Business Administration and Accounting from the University of Missouri, and an M.S. in Information Management from George Washington University School of Engineering and Applied Sciences. Welcome.

Our final witness is Tim Bennett, President of the Cyber Security Industry Alliance. Mr. Bennett has served as chief operating officer—I read your bio. I said to Dr. Coburn, I said this guy is going to be really old. I am pretty amazed that you are not. Either you are well preserved or not, but you have done a lot in your life, a lot of interesting stuff, too.

As President of Cyber Security Industry Alliance, Mr. Bennett has served as chief operating officer, executive vice president, senior vice president, international, of the American Electronics Association for 7 years, where he directed all operations for 18 U.S. offices and 2,500 members among other responsibilities.

In addition, Mr. Bennett has worked at the Office of the U.S. Trade Representative as the Deputy Assistant for 8 years, serving as a chief U.S. trade negotiator with Mexico, and one of the lead negotiators for the GATT Uruguay round of multi-lateral trade negotiations. He is here to share with us why NAFTA was a good idea—no that will be testimony for another day.

Earlier in his career, Mr. Bennett was an international economist for the U.S. Department of Labor's Bureau of Internal Labor Affairs and served on the U.S. negotiating team during the Tokyo round of multi-lateral GATT negotiations.

So you are all welcome, and Ms. Evans, before you start, let me just say a special welcome to my friend, Senator Coburn, and to recognize him for any comments he might want to offer.

Senator COBURN. I think you have covered it. Let us hear the testimony. Thank you.

Senator CARPER. All right. Thank you so much.

Each of you, your full testimony will be made a part of the record, and without objection, and we will just have you take it away. Well, if you can hold it to 5, 6, or 7 minutes, that would be fine, but we are not going to run the clock very tightly. Thank you.

Ms. EVANS. Before I start, though, Mr. Chairman, I do want to thank you for the acknowledgement of being a die-hard Mountaineer fan, because I am. So, anyway.

TESTIMONY OF HON. KAREN S. EVANS,[1] ADMINISTRATOR FOR E–GOVERNMENT AND INFORMATION TECHNOLOGY, U.S. OFFICE OF MANAGEMENT AND BUDGET

Ms. EVANS. Good afternoon, and I appreciate the opportunity and thank you for inviting me to speak about the state of Federal information security.

Securing Federal information and information systems has been an Administration priority, and over the last several years, we have focused management attention through a risk-based security framework.

In my written testimony, we highlighted our results from the Annual Federal Information Security Management Act Report. However, I would like to briefly describe some of our initiatives intended to close the remaining performance gaps.

In June 2006, OMB made recommendations to agencies to compensate for the lack of physical security controls when remotely accessing sensitive information. These recommendations were reiterated in OMB Memo 07–17. The recommended actions were to encrypt all sensitive data on mobile computers and devices, allow remote access only with two-factor authentication, use a time out function for remote access in mobile devices, and log and verify use of all computer readable data extracts from databases holding sensitive information.

In order to assist agencies, we are leveraging our buying power. GSA and DOD established a Smart Buy agreement for products certified through the National Institute of Standards, FIPS 140–2 Crypto Module Validation Program.

These certified products are used to encrypt data at rest, and we are currently using the management oversight of the President's Management Agenda Scorecard to ensure implementation and oversight of these recommendations.

While strong security controls can reduce the number of incidences, experience shows some incidences and attacks cannot be prevented. Consequently, an effective detection and response capability is critical.

In Fiscal Year 2007, 12,986 incidences were reported to the Department of Homeland Security Incident Response Center, which is more than twice the number that was reported in Fiscal Year 2006.

[1] The prepared statement of Ms. Evans appears in the Appendix on page 49.

While the increasing number seems alarming, we are finding this increase to be partially attributable to improved incident identification and reporting.

To further improve situational awareness and incident detection, we are working with agencies to reduce the overall number of external connections, including Internet points of presence. As agencies optimize their external connections, security controls to monitor threats will be deployed and correlated to create a government-wide perspective of our networks.

Deployment of Einstein, an intrusion detection system, to all external access points will allow us to collect, analyze, and share aggregate computer security information across the Federal Government.

Einstein will enhance current incident detection abilities, and will raise awareness of threats and vulnerabilities, allowing for corrective action in a timely manner.

These initiatives described in my testimony today, in combination with other Administration initiatives, including IPV–6, Homeland Security Presidential Directive 12, Minimum Computer Communications Capabilities for Continuity of Government and Continuity of Operations Plans, the Federal Desktop Core Configuration, and the IT Infrastructure Line of Business, address our potential security gaps, help agencies optimize their information infrastructure, and facilitate appropriate network consolidation and configuration.

In turn, agencies will be better able to manage their information infrastructure, allowing them to reduce risk to an acceptable level.

In conclusion, there is evidence agencies are making progress in the area of information security and protection of sensitive information. We are improving the quality of information security processes across the Federal Government while concurrently improving our reported performance metrics and compliance with FISMA.

I will be happy to take questions at the appropriate time.

Senator CARPER. Ms. Evans, thank you very much. Mr. Wilshusen.

TESTIMONY OF GREGORY C. WILSHUSEN,[1] DIRECTOR OF INFORMATION TECHNOLOGY ISSUES, U.S. GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Mr. Chairman, Ranking Member Coburn, I am pleased to be here today to testify on FISMA and the state of federal information security.

Rarely has the need for the Federal Government to implement effective controls over its information systems and information been more important.

Virtually all Federal operations are supported by automated systems and electronic information, and agencies would find it difficult, if not impossible, to carry out their missions, and account for their resources without them.

At the same time, Federal systems and critical infrastructures are increasingly being targeted for exploitation by a growing array

[1] The prepared statement of Mr. Wilshusen appears in the Appendix on page 54.

of adversaries, including criminal groups, foreign nation states, hackers, terrorists, virus writers and disgruntled insiders.

Thus, it is imperative that agencies safeguard these systems to protect against such risks as the loss or theft of resources, the disclosure or modification of sensitive information, including national security, law enforcement, proprietary business, and personally identifiable information, and the disruption of critical operations.

Today, I will summarize agency progress in performing key information security control activities, the effectiveness of information security of Federal agencies, and opportunities to strengthen security.

In Fiscal Year 2007, the Federal Government reported improved information security performance relative to key performance metrics established by OMB.

For example, the percent of certified and accredited systems government-wide reportedly increased from 88 percent to 92 percent. These gains continue historical trends that we reported on last year.

Despite reported progress, 20 of 24 major Federal agencies continue to experience significant information security control deficiencies. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information.

Moreover, agencies did not always configure network devices to prevent unauthorized access and ensure system integrity; patch key servers and workstations in a timely manner; and maintain complete continuity of operations plans for key information systems.

An underlying cause for these weaknesses is that agencies have not fully or effectively implemented the agency-wide information security programs required by FISMA.

As a result, Federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information as well as the inadvertent or deliberate disruption of system operations and services.

Such risks are illustrated in part by an increasing number of security incidents reported by Federal agencies. Nevertheless, opportunities exist to bolster Federal information security. Federal agencies can implement the hundreds of recommendations made by GAO and their IGs to resolve previously reported control deficiencies and information security program shortfalls.

In addition, OMB and other Federal agencies have initiated several government-wide initiatives that are intended to improve security over Federal systems and information.

For example, OMB has established an information systems line of business to share common processes and functions for managing information system security, and it has directed agencies to adopt the security configurations developed by NIST, DOD, and DHS for certain Windows operating systems.

Consideration could also be given to enhancing policies and practices related to security control testing and evaluations of agencies' information security programs required by FISMA.

In summary, although Federal agencies report performing key control activities on an increasing percentage of their systems, per-

sistent weaknesses in agencies' information security continue to threaten the confidentiality, integrity, and availability of Federal systems and information.

Until Federal agencies resolve their significant deficiencies and implement effective security programs, their systems and information will remain at undue and unnecessary risk.

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

Senator CARPER. Mr. Wilshusen, thank you very much. Mr. Bennett, you are recognized. Thanks for joining us.

TESTIMONY OF TIM BENNETT,[1] PRESIDENT, CYBER SECURITY INDUSTRY ALLIANCE (CSIA)

Mr. BENNETT. Thank you. Chairman Carper, Ranking Member Coburn, thank you for this opportunity to appear before the Subcommittee to discuss the Cyber Security Industry Alliance's thoughts on how to possibly improve FISMA. I know, Mr. Chairman, data security is an issue that you have been interested in and followed on a sustained basis, both in this Subcommittee and in the Banking Committee, and we appreciate that. I would also like to note, in light of prior comments, whether on the record or off the record, "Go Bucks."

This hearing is most timely and further bolsters current——

Senator CARPER. After I met Senator Coburn, I found out there was another OSU.

Mr. BENNETT. Yes.

Senator CARPER. There is another OSU in Oregon, and the guy who used to be President of Ohio State is now the President of Oregon State. He says he is sticking with the OSUs. He still has Oklahoma, though.

Senator COBURN. No, we just got a new president.

Senator CARPER. All right. OK.

Mr. BENNETT. Well, this hearing is most timely and further bolsters current congressional consideration of the need for strengthening information security within the Federal Government. As we have painfully learned, Federal systems are frequently vulnerable to the now relentless onslaught of cyber attacks, and the oversight by the Congress is an important element in holding Federal agencies accountable for improved information security, as well as highlighting ongoing challenges and vulnerabilities.

While today's hearing is not focused on a specific legislative proposal, we believe the 110th Congress has an important opportunity to enhance FISMA to improve the information security posture of Federal Government agencies. Even though the last few years have yielded some improvements in Federal information security, there are unacceptable vulnerabilities in Federal Government information systems that urgently need to be addressed. The Federal Government should be the leader in adopting effective information system practices based on understanding and addressing risks to sensitive information and not be the poster child for what can go wrong.

[1] The prepared statement of Mr. Bennett appears in the Appendix on page 92.

The time for strengthening FISMA is now, given the escalating, large-scale information security intrusions and data losses that have occurred at our Federal agencies over the past several years. Unsurprisingly, the Information Technology Association of America's recent report based on its annual survey of Federal CIOs found for the second year in a row, that the broad area of IT security and cyber security remains the top challenge faced by Federal CIOs.

CISA member company Symantec revealed in its 2007 Internet Security Threat Report that the government sector is the third most targeted sector for global cyber attacks and wholly responsible for 26 percent of all data breaches that may lead to identity theft.

Mr. Chairman, you mentioned in your opening statement the series of attacks perpetrated by hackers operating through Chinese Internet server against our computer systems at several Federal agencies. Hackers were able to penetrate Federal systems and use rootkits, a form of software that allows hackers to mask their presence, to send information back out of the Federal agency systems.

Federal agencies scored an average grade of C-minus on 2007's information security report card. Last year's average grade was a very small improvement over 2006 when the agencies scored an average of D-plus. These are barely passing grades.

Some argue that FISMA does not adequately measure information security. A high FISMA grade does not mean the agency is secure, or vice versa. That is because FISMA grades reflect compliance with mandated processes. They do not, in my view, measure how much these processes have actually increased information security. In particular, the selection of information security controls is subjective and, thus, not consistent across Federal agencies.

Agencies determine on their own what level of risk is acceptable for a given system. They can then implement the corresponding controls, certify and accredit them, and thus be compliant and receive a high grade, regardless of the level of risk they have deemed acceptable.

There were encouraging signs of progress in the 2007 report, but we continue to be concerned that many mission critical agencies like DOD and DHS are still lagging in their compliance. These and other agencies are lacking in implementing configuration plans, in performing annual tests of security controls, and are inconsistent in reporting incidents. The annual report card does, however, indicate that the Federal Government overall has made some improvements in the areas of developing configuration plans, employee security training, and certifying and accrediting systems.

FISMA does not tell the whole story when it comes to agencies' information security practices. Nowhere is an agency's ability to detect and respond to intrusions measured in FISMA. In fact, a senior DHS official testified before the House Homeland Security Committee on February 28, 2008 that intrusion detection is inconsistent across the Federal Government.

FISMA is a great baseline log, but clearly much needs to be done in this area. We need to incentivize strong information protection policies and pursue a goal of security rather than compliance.

We need to ask ourselves if we can make FISMA better as new threats evolve. Certainly, we want to avoid a check-the-box men-

tality, and do not want FISMA to be reduced to a largely paperwork drill among departments and agencies, consuming an inordinate amount of resources for reporting progress while yielding few genuine security improvements.

Unfortunately, in some cases, that is what it has become.

With the benefit of 5 years' experience under FISMA and several insightful reports by GAO, it is now possible to identify possible improvements that can address those weaknesses in FISMA implementation that have now become apparent. With global attacks on data networks increasing at an alarming rate, in a more organized and sophisticated manner, and often originating from state-sponsored sources, there is precious little time to lose.

CSIA believes that amending legislation is needed to give the weight and suasion of law to the eight improvements that we are recommending in our written testimony.

In closing, I commend the Subcommittee for examining whether enough is being done to protect Federal IT and secure sensitive information systems, and asking how we can improve FISMA and Federal agency information security practices going forward.

FISMA can be strengthened if we develop processes and metrics that truly measure information security and help guide investments in personnel, capabilities, and information security safeguards that can more effectively secure our complex Federal computing enterprises. We need to get beyond focusing only on compliance processes. We need to encourage risk-based approaches to information security. We need to embrace the public-private partnership that information security requires, and we need to take steps immediately that improve both the policy and the practice of information security. The overriding objective should be to move Federal agencies to act in a manner that equates strong information security practices with overall mission accomplishment. We all know what is at stake. Thank you.

Senator CARPER. Mr. Bennett, thank you very much. And Senator Coburn has another pressing engagement. He is going to have to slip out of here in a little bit, but I have asked him to lead off with questions. I am just happy you are here.

OPENING STATEMENT OF SENATOR COBURN

Senator COBURN. Thank you, Chairman. Let me thank each of you for what you do and for being here. Ms. Evans, I appreciate so much the work you do. How much of the work of FISMA is paperwork versus real security protection? And how much of a measurement of compliance is measurement of compliance of paperwork rather than security protection?

Ms. EVANS. Well, the way that I would prefer to answer the question is that it all depends on how the agency goes about doing the work. If the agency is going about doing the work because OMB is telling them they have to do it, then it is a paperwork exercise. If the agency is going about the work in order to achieve the goal, which is better information security, then it is measuring the information security of what is happening there at that Department.

FISMA has put together a framework. The policy supporting it has put together a framework, but it really is about if you are going to do it just to comply with OMB and to comply with the an-

nual reporting requirement, then it is purely a paperwork exercise at that agency.

Senator COBURN. So it does not mean anything. If they are compliant with FISMA, it does not necessarily have a reflection of how compliant we are in terms of security, cyber security?

Ms. EVANS. Well, the way that I would say it is is that you need to use FISMA as an indicator. It is an indicator, just like any of the other types of metrics that we would collect; and that the other thing that FISMA has, which some of the other metrics that we do not have, is that the law itself put the independent evaluation in there, which allows the IGs to come in and measure the value or the quality of that process.

So it is not just an agency reporting mechanism but it is also an evaluation of the quality of that process. So if you look at the information that when you start looking at it overall and then looking department by department, then you would be able to see this particular department is doing it, may be doing it as a compliance exercise or is not necessarily as mature.

For example, we have picked certain areas where we have asked the IG to go in and evaluate the quality. One, which is controversial, is certification and accreditation.

If an agency says I have a 100 percent of my systems certified and accredited, but the IG says that process is poor, then we need to go in and work with that agency because the agency is going about that process. We need to figure out is it just compliance or——

Senator COBURN. Well, that is what I am trying to get to. How much of it is doing the paperwork, meeting the certification? The goal is secure networks.

Ms. EVANS. Sure.

Senator COBURN. And so what do we need to do in terms of the reauthorization of this bill to make sure that everybody is working towards security, not compliance?

Ms. EVANS. Well, my view is that the bill itself is fine with the way that the framework is set up. I think some of the discussions of what we have talked about, the types of metrics that we are collecting or maybe some improvement in the guidance that comes from NIST to help agencies work through that process and be more definitive.

For example, a good example where an agency can choose and they need to choose the risk, we got more specific with some of the policy memos as it related to personally identifiable information, where we worked specifically with NIST. NIST went through and did a checklist, a very specific checklist and pointed to very discrete portions of their guidance, which really helped agencies get through that instead of looking at a document this big and then trying to figure it out on their own.

Senator COBURN. OK. So let us say we got an agency that is compliant that's not secure. What does OMB do?

Ms. EVANS. Well, what we would do is we would go through and see what that actually means, when you say they're compliant because——

Senator COBURN. I am saying they filled out the paperwork. They are certifiable, but when the IG comes in to test to see if they are secure, they are not. What do you do?

Ms. EVANS. Well, then what we do is we use the authorities that we have, for example, all the investments go on the management watch list. The existing projects will also go on the high-risk list, because what we want to do is make sure that you are not spending more money to put out new investments on top of infrastructure that is not secure.

Senator COBURN. OK.

Ms. EVANS. And that you do not have the proper controls in place that in order to ensure that you are monitoring then on a consistent basis and on the constant basis. So we would then work with the agency to make sure that there is a good remediation plan in place, looking at what are the weaknesses the IG has defined, and then work through that to make sure that they can then close that gap of what the IG has said is keeping them from having a good security program in place where they are constantly assessing the risk.

Senator COBURN. OK. Let me ask this of Mr. Wilshusen. You said their compliance has gone from 88 to 92 percent. Mr. Bennett said when we measure performance, they have gone from D-plus to C-minus. We are measuring two different things, are we not?

One is compliance, which does not necessarily mean security. And Mr. Bennett's performance measurement is about security, is that correct? Am I understanding that right?

Mr. WILSHUSEN. Well, I would say that in terms of the compliance, many of the performance metrics that OMB has established for FISMA reporting, on which agencies are supposed to report on their compliance with the Act, they are, in fact, just identifying the number or the percentage of systems that meet a particular control activity.

Senator COBURN. Right.

Mr. WILSHUSEN. It does not reflect how well or how effective that control——

Senator COBURN. Right.

Mr. WILSHUSEN [continuing]. Activity is in many of the cases. And, as a result, you do have that dichotomy of agencies reporting significant improvements in terms of the number of systems and number of personnel performing control activities. Whereas the effectiveness of their security controls is still questionable.

Senator COBURN. It could be going down?

Mr. WILSHUSEN. It could be. One measure of that we look at is the 20 out of 24 of the CFO Act agencies that——

Senator COBURN. Yes, I saw it.

Mr. WILSHUSEN [continuing]. Identified significant or their IGs identified significant control deficiencies or material weaknesses as part of their financial statement audits, the difference being is that in those reviews, in those audits, the IGs are assessing the effectiveness of information system controls or the financial systems, not just merely compliance with particular control activities.

Senator COBURN. OK. In your assessment, give me short answers because I am running out of time.

Mr. WILSHUSEN. OK. Sorry.

Senator COBURN. Yes, but I am out of time. They have been waiting on me 15 minutes.

Mr. WILSHUSEN. I see.

Senator COBURN. We have had almost a doubling of reported events. What percentage of that you think is increased reporting that were there anyway versus actually a worsening of a security situation—just a guess. I am not holding you to it. What do you think, Mr. Wilshusen?

Mr. WILSHUSEN. I would say I do not know that answer specifically.

Senator COBURN. Does anybody know that answer?

Ms. EVANS. Actually, we have the numbers based on what U.S.-CERT has given to us. The increased reporting based on our enhanced reporting requirements for personally identifiable information has increased. When you look at the report, it ends up that the actual number is about 348 actual incidences, when you start looking at unauthorized access, when you look at these numbers that are in the chart.

So because the rest of the reporting comes from lost and stolen equipment, and so there is an increase in lost and stolen equipment based on the way that we clarified the reporting requirements. But that leads to other issues dealing with security, which is the focus of this, and so what we are able to do then is see based on the types of reporting that comes in what type of corrective actions we need to take government-wide.

But to the question that you are asking about compliance and the metrics and this is one area where we do take a lot of feedback. We pick certification and accreditation because we believe that measures the lifecycle of what an agency is supposed to do from start to finish when they collect information and how they protect it. So if you do it right, that you are assessing the risk saying this kind of information I am having, this is the type of IT system I am going to use, these are the types of controls, these are what the users do, this is the residual risk, and the owner has to sign off and say I accept that.

So that is why we picked that process. When you start pulling out D-minus, C-plus, 92 percent and all those, you still have to get to the quality, which is the independent evaluation of the IG. So that is why we look at that in conjunction with the two. The D-minus grade that you are talking about that the House has given us.

Senator COBURN. Actually, it was C-minus. You are doing better than D-minus.

Ms. EVANS. We had a D-minus. We had a C, and I agree I would not accept that from my children. You can ask them.

So that is why we have worked to put in more of these government-wide solutions that are getting to the root cause of the issue.

Senator COBURN. So when IG comes or GAO come to look at this, do they actually test for security or do you test for compliance to the law? Which are you testing for?

Mr. WILSHUSEN. Well, when we do our reviews, we test for security. We test the actual——

Senator COBURN. So you are actually testing to see——

Mr. WILSHUSEN [continuing]. Security.

Senator COBURN [continuing]. If, in fact—you are trying to probe it and break it?

Mr. WILSHUSEN. That is correct.

Senator COBURN. And see if they can catch you?

Mr. WILSHUSEN. That is exactly right.

Senator COBURN. And so, on the basis of that, are we better off than we were a year ago?

Mr. WILSHUSEN. I would say we are not better off than we were, say, a year ago.

Senator COBURN. OK. That is a key answer.

Mr. WILSHUSEN. In that we continue to find significant control deficiencies on the audits that we perform.

Senator COBURN. Twenty out of 24?

Mr. WILSHUSEN. And that would include those that the IGs have identified, too.

Senator COBURN. All right.

Mr. WILSHUSEN. But I could just—if I may just—and I know you have——

Senator COBURN. OK.

Mr. WILSHUSEN [continuing]. To leave. I have two comments based on what Ms. Evans mentioned.

One is that most of the performance measures relate to strictly identifying whether control activity has been performed. There are a few instances where OMB asked the IG to comment on the quality of certain processes, but there are a number of other processes that are not asked or requested to comment on the quality of them, including, for example, security testing and evaluation of controls, which is a key critical control activity in which we often find during our audits where agencies' control activities or testing activities are insufficient because we identify a number of vulnerabilities that they do not on the same systems.

Senator COBURN. OK.

Mr. WILSHUSEN. In addition, the patch management, as well as the incident detection capabilities, are not necessarily assessed as part of the independent evaluation.

There is also a concern about the consistency of the independent evaluations performed by the IGs across the 24 agencies.

Senator COBURN. In other words, some are tougher probes than others?

Mr. WILSHUSEN. Yes, sir.

Senator COBURN. OK. The last question, and I am going to leave and let you answer it and my staff will give it to me, because I just received a notice my contact is getting ready to leave.

Do you think that the U.S.-CERT has captured data on all attacks or are they only on what is reported? And is there a difference? Mr. Bennett.

Mr. BENNETT. Only on what is reported.

Senator COBURN. Yes, so we do not know?

Mr. BENNETT. That is correct.

Senator COBURN. So basically, we are not to the point where we can really assess our security?

Mr. BENNETT. That is correct, and I am going to grab you real quick. On the OMB report released earlier this week about the doubling of the number of incidences reported, that does reflect im-

proved reporting. But what we have seen—certainly in the private sector—is the number of attacks exploded in 2007.

Senator COBURN. Yes.

Mr. BENNETT. The chart goes like this. So, there is no doubt——

Senator COBURN. So some of it is real and some of it is not?

Mr. BENNETT. It is real, and the Federal Government would not be immune from that increased malicious activity.

Senator COBURN. Thank you. Thank you, Mr. Chairman.

Senator CARPER. Let me sort of pick up where Dr. Coburn was leaving off. Why do you suppose we are seeing this explosion? You said in 2007 it just sort of took off. What is going on out there?

Mr. BENNETT. Well, I'll give you my take and also the others, and there are a lot of people in the audience behind me that are real experts on this.

A number of things. One, we saw organized crime move into this activity in a more sustained, organized fashion, more sophistication. The amount of money made in cyber crime, according to FBI report, now far exceeds that made in the total international drug trade and the gap is increasing.

It is easier to do. It is safer. It can be done from an offshore location. Chances of apprehension are substantially reduced. So we are seeing that.

And a lot of it is coming from offshore locations hitting targets around the world, primarily the United States, but not just the United States.

Senator CARPER. Well, what are some other countries that are being victimized besides us?

Mr. BENNETT. Well, the Attorney General of Australia just made a public statement earlier this week that the government agencies of Australia have been attacked and when asked to name a country, he mentioned China. So, there are certainly other governments.

You referred in your opening statement to Germany. Of course, the Estonian attack is noted. But there are also organized crime gangs in Russia, Romania, and Bulgaria. We have also heard Indonesia and Malaysia—so it is thriving, and it is profit-driven. It is a very entrepreneurial market now. And so it has gone away from random attacks, kiddy hacking, all these types of thing, to a very organized business activity. We have even seen evidence of going after certain databases, stealing certain personal information with the intent to hold it for a number of years. That reflects a long-term business plan.

So we are seeing a rapid evolution in the type of activity.

Mr. WILSHUSEN. And I would just like to add—and I would agree, too, with everything that Mr. Bennett mentioned—that there is probably better incident reporting on the part of the agencies. The May 2006, VA data theft, I think, was a Federal wake-up call on the importance of reporting incidents and reporting them promptly. And the increased emphasis on reporting that OMB has placed on the issue has also increased the number of incidents that are reported.

In addition, I would like to add that the threats are evolving; the threats to Federal systems are evolving. They are becoming more targeted, and sophisticated. And with the prevalence of information

security weaknesses and deficiencies within the Federal systems, it makes the likelihood of increased security incidents very possible; and the fact the Federal Government maintains and collects a lot of information that is very attractive to potential adversaries.

Senator CARPER. Ms. Evans.

Ms. EVANS. So what I would like to address is what you do when you have this information, and it is not so much making——

Senator CARPER. When you say what you do?

Ms. EVANS. What we do.

Senator CARPER. What is it you do?

Ms. EVANS. What we do when we have the——

Senator CARPER. Who is the you?

Ms. EVANS. The Federal Government, OMB, U.S.-CERT and how what we do with this stuff to get to the result of improved information security because that is really what we are trying to do. It is not so much—and I think this is the piece that we keep talking about here is you can enhance and you can insist on whether you have 100 percent reporting in here. Is the goal to get the 100 percent reporting or is the goal to be able to analyze the information that is coming in and fix what the systemic problem is?

And I would argue that there is enough information. We may not, we are improving our reporting requirements, then using this information to go forward and put solutions in place to reduce risk.

When you start looking at all of the things that my esteemed colleagues have talked about what is at the root of that problem? What are they exploiting? Why do I have material weaknesses? How do they get in? What are they doing?

Nine times out of 10, this is a configuration management, patch management issue.

Senator CARPER. When you say configuration management patch management, just put that in English——

Ms. EVANS. OK.

Senator CARPER [continuing]. That even I can understand it.

Ms. EVANS. So what will happen is if I am running an operation, so, say, I am back at a department and I am running an operation. Depending on whether I have that federated across the department or whether it is being centrally managed, so that only one person controls what comes in and what goes out on a desktop, like how a desktop is set up.

If you have allowed a thousand different types of configurations to flourish, because that stimulates a lot of creativity and innovation, that also increases your risk, because now you have to have the resources to manage a thousand different types of configurations. You have to have the resources to then look at a thousand different configurations and see what risks that come out on a daily basis that are related to that.

If I manage one, can manage one more effectively, then I can manage a thousand. And so what happens is then when organized crime comes along or any of these other ones, think of it as your house. You have a burglar alarm system—everyone knows that when you first put up that first sign and they are driving down the road, and they see that your house is monitored, they pass you and go to the next one.

Well, if everybody in your neighborhood has that sign up, the threshold has now gone up; right? So now the criminals are going to come by and start rattling doors.

Senator CARPER. What we did in our neighborhood, we went around the neighborhood, and we took out other people's signs.

Ms. EVANS. Well, there you go. [Laughter.]

But that is how it works. And so configuration management is raising it up a level so then what they start doing is tapping around and that is what these mean, like scans and probes and things. They tap around to see if a door is open or if a window is open.

If you have left the window open, and they will want to come into your house. So what we are trying to do in a very concerted way with what the Federal Desktop Core Configuration is lock down all the windows and doors; right? The sign is up, and then we are assessing the environment based on the risk. And then you can patch faster, if there is a vulnerability that comes out; right?

So, say, somebody's sign fell down. You would have to put a patch back up. This allows us to do that faster because we know everybody is supposed to have the sign. One person is missing the sign. We need to go back and put that sign up for the person.

That is what we are trying to do across the board as an entity.

Senator CARPER. Mr. Bennett, what is good or bad about the approach that Ms. Evans has just described for us?

Mr. BENNETT. Well, let me address that by saying this is an enormous problem. FISMA was a wise approach by the government, by the Congress to try and address it, and FISMA itself was in evolution in prior legislation.

What OMB has tried to do is try to manage this enormous Federal Government information system, for which we do not even yet have a complete inventory. It is a tremendous challenge. They are taking the best approach, and they have been tweaking and evolving over the years and putting out memoranda to guide the agencies on how to improve as they learn, but what we are suggesting is based upon our experience in working with the Federal agencies is—and the GAO reports there is too much of a reliance upon the procedures and the processes and despite Ms. Evans saying that the primary issues are just configuration, there still remains a problem of addressing the issue that Senator Coburn was getting at—are we coming after compliance or are we coming after security?

And what we are hearing is it is not coming after security, and in private conversations that I have had with the CIO offices of certain Federal agencies and in talking with them how is your FISMA compliance, enlighten me. They will say do you want the official answer or do you want the off the record answer. And just that response right there, I think underlines part of the problem that we are not getting at the primary goal of the mission of the agencies has to be aligned with protecting their information systems.

The Federal Government is probably the largest collector of information in the world. This information has—lots of it has value. And a lot of it is personally identifiable information. That information needs to be protected, and that needs to be recognized by the most senior levels of the agencies. We feel there are deficiencies.

It has been pointed out in GAO reports. We have recommendations, and we feel it is going to have to take legislation, not administrative action.

Having been a Federal employee for 11½ years, I think a Federal agency, an employee responds more when something is in law rather than hearing from OMB or another agency that we are asking you to do such and such. So that is our bottom line on that.

Mr. WILSHUSEN. May I please add a comment?

Senator CARPER. Mr. Wilshusen, sure. We have been joined by Senator Coleman. Welcome, this is our first panel. It is really quite a fascinating discussion so far. And we are happy that you are here, and, if you would like to ask questions of this panel, that would be great.

And we will let them go for a couple more minutes, and then I will recognize you.

Senator COLEMAN. Great. Thank you, Mr. Chairman. I may have one or two questions.

Senator CARPER. Good. Thanks for joining us.

Mr. WILSHUSEN. OK. I would just like to add one thing that Ms. Evans mentioned was the Federal Desktop Core Configuration Initiative. We think that has a lot of promise.

Senator CARPER. Why do you say that? Why do you think it has a lot of promise?

Mr. WILSHUSEN Because in our audits, many of the security vulnerabilities that we identify and are able to exploit are ones that exists due to insecure configurations of operating systems.

And the Federal Desktop Core Configuration, for example, is coming up with relatively secure configurations of the Windows XP and Vista operating systems. By having these operating systems configured securely, particularly if we can get them right out of the box when they are acquired, it provides a greater opportunity to improve the security than is the usual case with operating systems—that come in in their least secure state and require the agency then to come in and implement security in the operating systems.

So by having the ability to have these core configurations and through the leveraged power of the Federal procurement to have these configurations right out of the box will help strengthen security.

Once it is installed, you still need to maintain that over time because the computing environment is not static. It is very dynamic, so there still needs to be effective monitoring mechanisms in place, but it is a benefit that will help reduce some of the vulnerabilities of that we often find.

Senator CARPER. All right. Well, it sounds like what we are up against here—and I want to go back to this scorecard you mentioned. D-plus to C-minus; modest improvement, but improvement. Whose scorecard was that?

Ms. EVANS. It is the House Government Reform.

Mr. BENNETT. It is the House Government Oversight and Reform Committee.

Senator CARPER. All right. Each one reflects an evaluation for a particular discrete year? Is that what?

Ms. EVANS. Yes, they rank it each year, and they release the methodology associated with that. It is based on—GAO also looks at it, and then what will happen is they will take the information from the agencies, and they will either plus or minus points based on certain methodology every year, and GAO works with the House side in order to come up with what that methodology should be.

Senator CARPER. And what years were covered, 2006 or 2007? Do you all know?

Mr. WILSHUSEN. They have not done one for 2007 yet.

Senator CARPER. I see.

Mr. WILSHUSEN. There have been computer report cards over the last several years beginning with, I think, it was Representative Horn.

Ms. EVANS. Right. It started with Representative Horn, so he did 2001 forward, because I remember that was my first hearing 6 weeks into the job and over at Energy.

But it is discrete against the report, so it is another view of looking at this same report. So the plus ups or the discussions with the House side again is that scorecard really measuring security, or is it just measuring the compliance with the information that comes into FISMA. So it is the same debate. It is just another view of looking at it.

Senator CARPER. Yes. And we keep coming back to that issue. Are we measuring compliance or are we measuring security. I am reminded of my old job. Before Senator Coleman came here, he was a mayor of a big city in Minnesota. But I was governor, and we worked a lot on education reform, trying to spell out what students ought to know and be able to do in math, science, English, and social studies. We spelled out our academic standards in those subjects.

And we began to measure student progress toward mastering those academic standards in math, science, English, and social studies. Up until that point, there had been no way to judge academic performance by how much money we spent per student or how—what kind of degrees the teachers had. We judged inputs and process more than we did outputs and outcomes.

And this debate reminds me a little bit of what we went through in education.

Do you all think we are doing a better job in terms of measuring outcomes as opposed to a process? Are we measuring the right stuff?

Mr. WILSHUSEN. I would say as part of the FISMA reporting process that the metrics that OMB has established that we are not effectively measuring the effectiveness of security controls or the quality of the control processes because, for the most part, they are measuring just the performance of a control activity, not its effectiveness. And I think there could be some other measures that are appropriate to help show what the effectiveness is.

OMB does ask the IGs to comment on the quality of certain processes, but there are other processes that could also be evaluated as related to its quality.

Senator CARPER. All right.

Ms. EVANS. So I would like to add to this that every year when we do the annual reporting requirements, we send out the updated

draft, and we ask for different metrics, if people want to improve the metrics or change the metrics in order to get to some of the issues that we are talking about today.

We send it to the IG community. We also send it to GAO, to enhance or add additional pieces. We have added additional areas dealing with privacy, so we are now measuring privacy in a government-wide capacity, and we have added those metrics.

But some of the suggestions that have come in when we have looked at them, we have evaluated whether they have always been accepted or not, whether we are actually still getting to is that another output metric or is that really a performance metric.

So another example, real quick example, that I would like to give is what we are trying to do is use this information to inform solutions that get us to that result.

So one of the things that came in that we see, the increase in incident unauthorized access that we were previously talking about, that is an 85 percent increase and that is from lost or stolen equipment.

That gets back to the additional guidance that we gave the agencies about encrypting data on devices that are mobile. And then what we turned around and did was put in a BPA, a government-wide BPA——

Senator CARPER. What is a BPA?

Ms. EVANS. It is a blanket purchase agreement——

Senator CARPER. Thank you.

Ms. EVANS [continuing]. Which allows agencies to use it so that they do not have to procure their own solutions and that everything is on that particular contracting vehicle so that they can then go, leverage our buying power, and have encryption tools then put in place.

So we are using the data that comes in that may be output data to get to more solutions, more results, more performance types of activities instead of trying to really, since we have not gotten good metrics—we feel good metrics that measure performance and effectiveness to try to get to solutions that are really getting to the results, and we are using the data to inform those types of solutions that we are putting in place.

Senator CARPER. All right. Let me stop right there and recognize Senator Coleman. Glad that you are here. Thanks for joining us.

OPENING STATEMENT OF SENATOR COLEMAN

Senator COLEMAN. Pleasure to be here, Mr. Chairman, and thank you for the opportunity to participate in this discussion.

Mr. Chairman, I have a more complete statement I would like entered into the record.

Senator CARPER. Without objection, it will be put in.

[The prepared statement of Senator Coleman follows:]

OPENING PREPARED STATEMENT OF SENATOR COLEMAN

I want to begin by thanking Chairman Carper and Ranking Member Coburn for holding this hearing and for permitting me to attend as I am not a Member of this Subcommittee. As the number of cyber attacks on Federal Government networks continues to increase, it is important that we review agency compliance with the laws in place to prevent those attacks such as FISMA and if they need to be strengthened.

One area of concern I have is what the Federal Government is doing to fulfill its responsibility in maintaining and protecting sensitive Personally Identifiable Information (PII) that Americans are required to provide for a wide array of reasons, including paying taxes, receiving medical and disability benefits, and obtaining retirement compensation. This PII includes names, addresses, Social Security numbers, biometric records, and other data that is linked or linkable to an individual. Identity theft and fraud are national problems that affect approximately 10 million Americans each year so it is critical the Federal Government take steps to ensure PII does not fall into the wrong hands.

In the wake of the VA data breach in 2006, I asked GAO to conduct a government-wide review of current policies on the books to protect American's personal information held by government agencies. The findings released in this report are very troubling—seeming to indicate that agency after agency is failing to make securing citizens' personal information a high priority.

As a result of this GAO Report, Senator Collins and I sent a letter to every Agency requesting in writing a timeline of when they will meet the recommendations put in place by the Office of Management and Budget (OMB) for increased cyber-security. I want to thank the VA who has responded and indicated they are compliant or have achieved significant milestones with the OMB memoranda. I also want to thank USAID who has responded and offered details for compliance. I look forward to receiving responses from other agencies as well so we can get an accurate picture of where things stand.

The fact is the clock is ticking and we need to know when the agencies are going to have the protections in place to stop the numerous data breaches we have seen over the past few years. Our citizens deserve nothing less. The bottom line is the Federal Government has a responsibility to ensure the personal information it collects from its citizens is properly secured and protected. The sooner the Federal Government acts, the sooner Americans will be protected from the damaging consequences these breaches can have on their personal lives.

Senator COLEMAN. In wake of the Veterans Affairs data breach in 2006, I had asked GAO to conduct a government-wide review of current policies on the books to protect America's personal information held by government agencies.

And I think the findings here—Ms. Evans, I appreciate the work that has been done. The findings are troubling. It still seems to indicate that we are moving forward at the pace that we need to move forward.

Senator Collins and I, as a result of the GAO report, sent a letter to every agency asking in writing and timeline of when they will meet recommendations put in place by OMB for increased cyber security, and I am not going to get into all the details of that. Certain agencies have done very well and responded, and others are still not there. And I think the clock is ticking, and we have to move forward.

But my more complete statement will touch upon that. The question I have is about looking for solutions and just so I can tell two anecdotes, Mr. Chairman, before the question.

One is in some of my dealings with IRS and other agencies what I have found consistently as folks come back and saying we cannot move quickly enough on the text because we do not have the capacity. We do not have the people, the skills to do the software, to do the kind of things that need to be done. I find that troubling. I tied that into a discussion that I had as a Member of Homeland Security and Governmental Affairs Committee and doing oversight of Hurricane Katrina. And a witness was the IG for one of the Inspector General—I think Homeland Security, and he was saying that we had all this food in the pipeline, but we did not know where it was. We did not have the technical capacity. And my question

was literally well, why do you not call FEDEX or UPS—that the capacity is out there in the private side.

And so my question is that so many of the things that we are discussing here are not unique to government—the challenges are not unique to government. The private sector faces similar challenges. In many instances, they may have greater capacity to come up with solutions than we do for whatever reason. And so my question is what degrees are departments and agencies partnering with the private sector? Are there vehicles passed to do that? And does the same hold true for a State and local government agencies?

Ms. EVANS. OK. So first, on State and local government agencies, they can work right off of the same solutions that we have. So when I talked about the encryption that we had in place and that blanket purchase agreement that we put in place, we use the authorities under the E–Government Act to extend that out to State and local governments beyond what is normally available to them under what they call Schedule 70, which are the IT schedules that are managed by the General Services Administration.

So what happened in that particular case was all the tools that we identified that we worked with DOD—was key in this—that is all extended out to State and local governments. They have exercised that. They have the same problems that we have done.

As a matter of fact, the State person from New York who works on cyber security sent me a note before the hearing last week and 15 States have used that. They have had a savings of over $34 million using the encryption products that are available there.

So we have done that so that they can learn from us on that.

As far as public and private partnerships, the E–Government Act, all of our authorities currently now allow us to do that.

And the Federal Desktop Core Configuration, what we were just talking about, is a prime example of public-private partnership. We went to Microsoft, building off of existing relationships that the Department of Defense had and the Department of Homeland Security and said OK, now Defense has done this. This is a best practice.

We want to take this to the entire Federal Government. What is the impact of that? And they worked with us jointly. When we talk about a secure desktop configuration, that is 700 security configurations that are being set on the desktop.

And what Microsoft is doing is supporting that through the regular distribution channels. So there is no impact to the market on this, other than the Federal Government improves from that. And the way that we have done it is in a very transparent way using NIST and so all of that is published. All that information is out on the NIST Web site. All of it is available for everyone, not just us—countries, anyone—can download that information and use the same secure configurations that we are and work with Microsoft through the same existing types of applications and contracts that they had to do it.

Senator COLEMAN. Mr. Wilshusen, would you—and perhaps what I would add to that is are we—and I appreciate the fact that States and locals can kind of work off what we are developing. Are we confident that the systems that we are using are, in fact, the best

practices that equal those practices that are being employed in the most high tech, fully funded private companies?

Mr. WILSHUSEN. Well, I would say in terms of the IT contractor Federal Government partnership is that in most of the Federal agencies they do rely extensively on contractors to provide IT services and in many cases even information security services.

And one of the key requirements for the Federal agencies, though, is to make sure and provide the appropriate oversight and monitoring of the activities of the contractors, to make sure that if they are operating systems is on the agency's behalf that those systems are also adequately protected.

We did a review a couple of years ago in which we found that many of the agencies at that time had not developed policies and procedures for effectively monitoring the activities of the contractors to assure that they were implementing the security requirements under FISMA and the like.

That probably does not answer your question.

Senator COLEMAN. No, what you are telling me is even as we do with contracts, is we have to have some of the same concerns about access to data——

Ms. EVANS. Yes.

Mr. WILSHUSEN. Absolutely.

Senator COLEMAN [continuing]. And security. My question went to the concern that I have had in dealing with technology to see the Federal Government saying we are not using, always using, the best practice, not using the highest level of material that is available. And I just want to make sure as we tackle this area that we are not just kind of inventing the wheel—reinventing the wheel here, but if it has been invented and used somewhere else that we are able to absorb it and use it quickly.

Well, I think the example that Ms. Evans provided with regard to the Federal Desktop Core Configuration is one of those instances where the Federal Government and Microsoft and its partners are taking a leading role in identifying basic security requirements that can be applied on a mass basis.

Senator COLEMAN. Thank you, Mr. Chairman.

Senator CARPER. You bet. Those are really good questions. Are there not other companies or organizations that use outcome metrics to measure security? I think we touched on this, but let me just go back. Are there not? Can somebody respond to that?

Mr. WILSHUSEN. We have not done a review of what private sector organizations have done in terms of conducting and identifying meaningful, useful performance outcome-based performance metrics. But that would certainly be something that we would be willing to do with you.

Senator CARPER. Are the policies that are in place set up to be responsible to the new emerging threats? This has to be tough, because there are more and more bad guys out there. They are not just hackers and young people looking for a thrill. They are governments, or the Chinese or others, Russian nationalists. They are folks that have criminal intent, and they are looking to hit the jackpot and taking advantage of these situations.

In terms of the threats that we see, just give us some ideas. Has half of this activity, attempts to penetrate our system, is it coming

from hackers? How much is coming from, like foreign nationals? How much might be coming from criminal organizations? Any sense for at least for our systems, the stuff that we are trying to protect?

Ms. EVANS. I would refer us back to the report itself, which categorizes the different types of incidences. So some of the specific examples that you are giving would fall under the category that we have under investigation. And that shows an increase from last year of 912 incidences to 4,000 incidences. And it can be that it is under investigation——

Senator CARPER. Sorry. Say those numbers again?

Ms. EVANS. Last year, we reported. So all the different categories that you just talked about would be in what we categorize in the report as under investigation. And so last year, for Fiscal Year 2006, we reported 912, and this year (2007) we were——

Senator CARPER. This year being 2007?

Ms. EVANS [continuing]. Reporting 4,056.

Senator CARPER. OK.

Ms. EVANS. Now several of those are related again to the increased reporting that we had because of the lost and stolen equipment, so it is under investigation because we involved law enforcement from that perspective.

So a lot of what you are asking falls into that category, and I think that without getting into all the specifics of what you are saying is that the better category to look at is what is under investigation.

Senator CARPER. All right.

Mr. WILSHUSEN. One other category potentially could be the unauthorized access that is reported to U.S.-CERT, too, because those are actual instances where an intruder or an unauthorized individual gain access to information that they did not have a right to.

Senator CARPER. OK. The State of Delaware is the home to a number of large financial institutions. Some of them are credit card operations, others do other kinds of financial services—and some of the best in the world.

I used to watch as MBNA, which was one of the largest credit card banks in the world and now is part of Bank of America, when I remember a dozen or so years ago, they started hiring people who had been in the FBI, folks who had been with top folks in the Armed Services, and I was struck by how they were really going after people with a law enforcement background.

And what they were doing back in the last decade was beefing up their ability to protect their sensitive information from these kinds of threats. I did not realize it at the time, but eventually I did.

What can we learn from them? This question has already been asked to an extent. But what can we learn from financial institutions? What did Willie Sutton used to say when they said, why do you rob banks? He said that is where the money is. And if I were a hacker and I had criminal intent and I was looking to find financial gain, I do not know that I would necessarily go after the government first. I might go after these financial institutions. But what can we learn from them? What are we learning from them? And just as the threat changes, the nature of the threat changes

constantly, it sounds like, and we have to get better and better, I am sure the same is true for some of these financial institutions and others that they are trying to protect their information.

All right. Mr. Bennett, anything you would like to offer?

Mr. BENNETT. Yes. Thank you. First, I think in the private sector you find that the approach to information security in most cases, certainly in the financial services sector, is a continuous approach. And that is something that I think the Federal agencies could learn; that you cannot just do a report once a year or periodically, but it is a continuous effort. There are thousands of attacks a day. DOD gets over a million probes a day. It takes constant monitoring. That then spins off to the issues of adequate resources and training, budget, and personnel.

The second thing is in the private sector, there has been a convergence at the top levels, an awareness that the success of the entity, of the corporation, of the business is aligned with its information security practices. Its reputation, the intellectual property, the reputation of the company should there be a massive data breach, the profitability of the organization if the intellectual property has been stolen, its ability to do successful merger negotiations could be undermined if another party has been stealing their negotiating position before they even walk into that negotiating room, and there are stories of that.

These all impact a company and can have an impact on the market and the future of that company immediately. So security is aligned with mission accomplishment, and I think that is an area that the Federal Government could learn from the Federal agencies.

The most senior officials at our agencies need to understand that protecting their information systems and the information that they contain needs to be protected on an ongoing basis in the best possible risk-assessed fashion that fits within their budget.

You cannot have a situation where Cabinet officers go to a meeting with foreign government and before they even show up, their counterpart on the other side of the table already has their briefing paper and their talking points or might even know the U.S. negotiating parameters.

I would not be surprised if this has not already occurred.

And then for the Cabinet officer to return and be stunned and be upset with his staff who leaked that. Well, it was not leaked. You had a foreign party that was in your data system before you even headed out to Dulles Airport.

So we need the top levels to appreciate the critical importance to the economic security, national security of this country, and the importance of protecting their data systems.

Senator CARPER. All right. I want to talk about incentives. One of the things we like to do in the oversight work in this Subcommittee, and really on our full Committee, is to look not in order to change behavior or to get the kind of behavior we want from Federal agencies, not just to penalize them or to wrap them on the knuckles. We want to incentivize them to, which is a positive reinforcement of the good behavior that we see and we want others to emulate. But incentives can be a powerful motivator, I am sure we

will all agree, for achieving goals. And without them, many times we are going to fall short of where we want to be.

If information security is one of our top priorities and it clearly needs to be, what type of incentives can we provide to help agencies put in place the policies and the procedures that are needed to have more effective information security programs?

Ms. EVANS. Well, I will take the first shot at this, because it is actually following back up off of what my colleague, Mr. Bennett, has said, and that is having the agency head, and, in this case, from the OMB Director to the President of the United States involved in this, which we are. This has been an Administration priority that has been demonstrated through the National Cyber Security Strategy, through our investment in cyber security in the budget and having the resources, looking at workforce issues—all of the things that we have talked about. But one strong thing and one thing that the agencies respond to that Congress could do, which we believe we are doing, is the public accountability.

And so through the President's management agenda, by giving something as simple as a red, yellow, and green, because we have focused a lot about the scorecard that Congress issues on cyber security; that means a lot to Federal agencies, the public acknowledgement that they are improving; that they are achieving the results. That is something that Congress can do and has done.

What we have a tendency to focus on are the bad things of where an agency is not doing the things that they need to do. That makes better news. Those are better stories to put out there, not necessarily that this agency——

Senator CARPER. Are you suggesting that the media tends to report bad news? [Laughter.]

Ms. EVANS. Yes, sir. So what I am suggesting is what really drives a lot of public service and the reason why the folks are there in those agencies is to deliver that mission for the American people. They do not want to lose the information. They do not want to put citizens at risk.

So when an agency is doing a really good job and a comprehensive job, the acknowledgement of that in a public forum to say they are doing a good job goes a long way, and is a huge incentive.

Senator CARPER. All right. Thank you. Mr. Bennett.

Mr. BENNETT. Yes. I think what we have learned in the private sector and I am sure translates to the public sector is that you are going to get the greatest return on security when there is individual accountability on security. It cannot just be agency-wide and such as the agency-wide grades that we have been talking about.

So perhaps certain metrics or parameters have to be put in the individual performance appraisals, and if there is poor performance, certainly in the private sector, there would be the ultimate outcome of dismissal of employment, termination of employment. Whether that is possible under the Federal system, I do not know.

But, that increased accountability has to be there.

At the same time, good performance does have to be rewarded, both in public recognition, but also in monetary bonuses to the employees, bonus vacation days, things of that nature that I believe are permitted under the Federal system.

That type of recognition is also good. There is also the budgetary authority; maybe an agency should be penalized if it is getting a D-minus or an F; whereas, but not the spending on security with the agency, and if they get good grades, set by certain parameters, then somehow in the budget process, either reallocation within an agency or in the next appropriation process, that agency should be rewarded with that money dedicated—I know earmarks are a problem—but dedicated to spending for improved cyber security. And then auditing—if you get a good grade, maybe you will not be audited as often. You come up with poor grades; we are going to start auditing you more often.

Senator CARPER. Senator Coleman.

Senator COLEMAN. Mr. Chairman, I wanted to get to the second panel. But your very question, actually the area of—and I am not sure if I will have time——

Senator CARPER. Well, when we go to the second panel, we will let you ask your question.

Senator COLEMAN. I appreciate this concept of a security line with the mission accomplished——

Senator CARPER. Yes.

Senator COLEMAN [continuing]. That is really critical. Thanks.

Senator CARPER. Just one last question for this panel, and it is a workforce question. Ms. Evans, you said back in, I think it might have been December when we held a hearing. I think we were authorizing the E–Government Act—that you recognized that you did not have effective measures in place to fill the necessary workforce gaps in IT-related positions.

And since then, has OMB created effective or more effective measures and is there a comprehensive plan that attempts to address some or all of these shortages?

Ms. EVANS. So we have recently released the workforce assessment, and what we have done is we have broken it out to identify the gaps, and then each and every agency now has a workforce plan. They have identified the target competency level within each of these areas; cyber security is one of them, and they have a plan that closes the gap. For example, in this area, what they are doing is they are measuring certifications and they are putting together a training program associated with that.

What I am now looking at is OK so we have taken it to the next level. It is not just the number of people hired, but it is now certifications associated with cyber security. What we are now looking at through the cyber initiative is education overall so that we can look to make sure that the education programs and the certifications that these agencies are getting for their employees will be—and I am going to use the term harmonized—so that you know that if I get the education at one university, it is going to be the same education at the other university so that when I come into the workforce I have the same set of skills.

And so that is a longer-term effort that we are working on now. But we are working with the National Science Foundation and few other of the programs that we have in place to harmonize that education process.

Senator CARPER. All right. Before we excuse this panel, just give us some good heartfelt advice for those of us in the Legislative

Branch of what we can do to be a better partner in this effort. We have a lot at stake. It is a tough battle, a tough challenge that we face. It sounds like it is getting tougher, and we want to make sure that we are being supportive.

Part of what we are doing is trying to play an oversight role. I think the House has been doing that as well. And it is important for us to do that, too.

But it is not enough just to put a spotlight on the areas where we may have some disappointing performance, but it is important that we find ways that we can incentivize better behavior and also ways that we can be constructive.

So in closing out, if you all would just share with us an idea or two, you might have on how we can be constructive and helpful.

Mr. Bennett mentioned, for example, he mentioned legislative—some legislative work that we had to do.

Mr. BENNETT. Right.

Senator CARPER. And, feel free if you agree with that or disagree with that that would be helpful to hear, too. Mr. Bennett, do you want to go ahead?

Mr. BENNETT. Thank you, Mr. Chairman. Well, I think our approach would be—the overall problem of information security is enormous; is very difficult to get your arms around it. But there are incremental steps that can be taken and should be taken. With respect to protection of our Federal information systems, we have made our recommendations in our written testimony. We feel that they are all manageable. They are not by way of criticism of the men and women who are working on this within the Federal agencies, but instead we are saying based upon experience, this is a way now to take us forward based on the past 5 years experience and lock in and improve security to the extent we can.

We believe the cyber crime bill that this chamber passed in November by unanimous consent now sitting with the House will help give increased authority and increased penalties for the U.S Department of Justice to use in fighting cyber crime. We believe that the next Congress is going to need to take on a broader data security bill that includes issues of data breach notification that both you, and Senator Coleman, have been extremely active on in this particular chamber and that we support—protecting personally identifiable information.

We need to bring all entities that hold large amounts of information, our universities, which are one of the biggest targets of attack. Home users, government, businesses—they all need to bring their standards up such as the financial services sector has done with the PCI standards. We need to start bringing everybody's awareness up through public education, which is another component here, and also it is going to take legislation; otherwise, they will not do it.

We need a broad data security and breach notification bill hopefully in the next Congress to bring the overall standard up against protection, because quite frankly, the bad guys are winning. They evolve extremely rapidly. We are now even seeing malicious code being tweaked on a daily basis in some cases to get around patching, so it is a leapfrog process. They have tremendous financial resources that a Federal agency cannot match. So we need to

take whatever steps we can, but it is warfare. It is warfare against organized crime, individual hackers, and state-sponsored.

Senator CARPER. All right. Mr. Wilshusen, any parting advice for us on the legislative end?

Mr. WILSHUSEN. Well, I would just say that there could be some opportunities to tweak FISMA to make it more strenuous and clear in certain areas in terms of certain requirements that need to be performed perhaps as it relates to the testing and evaluation security controls, some of the FISMA reporting requirements, as well as the annual independent evaluations performed by the IGs.

Senator CARPER. All right. Thank you. Ms. Evans.

Ms. EVANS. I would agree that maybe some clarification as agencies go forward, but I would caution against major changes to FISMA, only from the aspect of agencies understand it. Now whether we agree with whether it is producing the right result or not, the framework is a sound framework.

And what my concern would be is to do a major change to it would then mean that we have to reinstitute policies, reeducate the agencies, when we are really trying to be focused on what the results are.

I would encourage more of the types of activities that Senator Coleman and Senator Collins did following up on certain things, going back out to see if the solutions have actually been implemented, asking agencies to produce results of that and show, give evidence that they have actually implemented those solutions, and those types of things

And that is where Congress can be very helpful in making sure, and that follow up is very powerful, because you are following up on policies and statutes that are in place to make sure the agencies are really putting those solutions in place.

Senator CARPER. All right. Ms. Evans, Mr. Wilshusen, and Mr. Bennett, thank you so much for being with us today, for your thoughts and your willingness. One of the questions I am going to come back to you, Mr. Bennett, you gave us, I think, in your written testimony a number of recommendations. And I would say to Ms. Evans and Mr. Wilshusen, one of the things that I am going to do is come back to you, each of you, and just ask you to evaluate the recommendations—which one do you agree with, which one would you modify, which ones do you disagree with, but that will be most helpful. All right. Thank you very much.

Mr. BENNETT. Thank you.

Senator CARPER. Welcome to the four members of our second panel. We are glad that you are here, and we thank you for joining us. I am going to take just a moment and introduce each of you, if I can and then we will call on you to give us your testimonies.

We just start with Hon. Robert Howard, Assistant Secretary for Information and Technology. Mr. Howard serves as the Department's Chief Information Officer, advising the Secretary of Veterans Affairs on all matters pertaining to acquisition and management of IT systems.

Prior to his nomination, he retired as a Major General from the U.s. Army in 1996, where he served for 33 years. How did you get your commission?

Mr. HOWARD. ROTC, sir.

Senator CARPER. Me, too. Good for you. Where did you go to school?

Mr. HOWARD. Northeastern University.

Senator CARPER. All right. And while on active duty, Mr. Howard served in a variety of command and staff assignments in the continental United States, Europe, and in Asia; two tours of duty in Vietnam—a part of the world where I spent some time myself. I think you and I must be about the same age.

Our next witness is Susan Swart, Chief Information Officer at the Department of State. Ms. Swart is a member of the Senior Foreign Service for the rank of Minister of Counselor. What do people call you when they address you—Minister-Counselor Swart?

Ms. SWART. No title.

Senator CARPER. All right. When I was governor, they addressed me as excellency. And how about mayor?

Senator COLEMAN. Mayor.

Senator CARPER. All right. But Ms. Swart is a member of the Senior Foreign Service with the rank of Minister-Counselor and was recently appointed as the Chief Information Officer in February 2008. Congratulations.

Ms. SWART. Thank you.

Senator CARPER. Prior to assuming her new position, she was the Deputy Chief Information Officer for Business Planning and Customer Service and the Chief Knowledge Officer from April 2006. I like that—the customer service. That is good.

Our third witness is Daren Ash, and Chief Information Officer and Deputy Executive Director for Information Services at the Nuclear Regulatory Commission. Mr. Ash has over 15 years of Federal service. How many years at the NRC?

Mr. ASH. About 10 months.

Senator CARPER. All right. Prior to joining the NRC, Mr. Ash worked as the Department of Transportation's Associate Chief Information Officer for IT Investment Management, and for close to 2 years, he led DOT's information assurance and the security privacy and enterprise architecture, capital planning, and information resource management activities.

The final witness is Phil Heneghan, Chief Information Security Officer and Chief Privacy Officer at the U.S. Agency for International Development. During the last 5 years, he has been responsible for managing the USAID Information Systems Security Program.

Mr. Heneghan led the development of the FISMA program that improved the agency's FISMA grade from an "F" in 2003 to a grade of "A-plus?"

Mr. HENEGHAN. Yes, sir.

Senator CARPER. Were they grading on a curve? What do you think? No? [Laughter.]

That is pretty amazing—in 2005, at least that was the grade appointed by the House Committee on Oversight and Government Reform.

USAID has maintained the A-plus for its information security program for the past 3 years. Great fun.

Mr. Howard, you are recognized first, and again use 5, 6, or 7 minutes for your statements and then we will ask some questions. All of your entire written statement will be admitted for the record.

Mr. HOWARD. Thank you, sir.

Senator CARPER. Sure. Thank you. And let me just say thank you for your service in the Armed Forces of our country.

Mr. HOWARD. And for yours, sir.

Senator CARPER. My pleasure.

TESTIMONY OF THE HON. ROBERT HOWARD,[1] CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF VETERANS AFFAIRS

Mr. HOWARD. Good afternoon, Chairman Carper, Senator Coleman. Thank you for your invitation to discuss the ability of the Department of Veterans Affairs to protect and secure sensitive data.

Information protection is a top priority within VA and is highlighted as one of the five principal priorities in the Fiscal Year 2006–11 VA Strategic Plan.

As you are well aware, May 3, 2006 was the day of the theft which led to the temporary loss of personally identifiable information of up to 17.5 million veterans, some of their spouses and some active duty personnel.

Although the follow-on investigation confirmed that information was never accessed, that day was a wake-up call, not only for VA, but for the entire Federal Government as well as the private sector.

As a result of that incident, we began to improve our security posture and create the environment needed to better protect any sensitive information entrusted to us.

Clearly, the centralization of information and technology within VA has had a positive impact regarding the protection of sensitive information. Within this new structure, we have established a separate organization, called Information Protection and Risk Management, that is dedicated to improving our overall data security posture.

A new Deputy Assistant Secretary position has been established to lead this organization and help provide the important focus that is needed.

I would like to take a few moments and just mention a few that are in the room with me today. This is a very important team we have. Several key leaders from this organization are, in fact, here. Adair Martinez is my Deputy Assistant Secretary for this organization. Jaren Doherty is our new Chief Information Security Officer——

Senator CARPER. Could I just ask you, as your names are mentioned, just raise your hand so we are able to put a face with name?

Mr. HOWARD. Yes, sir.

Senator CARPER. Adair Martinez. OK. Thank you.

Mr. HOWARD. Jaren Doherty is our new Chief Information Security Officer, which we have been seeking for 2 years. He is now on board. He oversees cyber security. Kathryn Maginnis is in charge

[1] The prepared statement of Mr. Howard appears in the Appendix on page 98.

of incident response and risk management. Sally Wallace leads our efforts in the area of privacy and records management. And Charlie Gephart is our Director of Field Security Operations, who has all the field security individuals throughout the organization.

Andy Lopez has recently established our business—Office of Business Continuity. And in addition, there is Arnie Claudio, the Director of our Office of IT Oversight and Compliance, a very important capability as I will explain in a moment.

Sir, as I mentioned, this is a very important team for VA because these individuals form the leadership core for information protection. They are all focused on the implementation of a wide variety of activities that are moving us to a much more secure posture than which currently exists in VA.

One of the most important steps we have taken is to help create a robust information security environment, the development of a comprehensive action plan. We call that the Data Security-Assessment and Strengthening of Controls program.

It focuses on three major areas: Managerial activities, for example, the establishment of policies and directive; technical activities—the example there would be better software tools, such as encrypted thumb drives; and operational activities, and examples there would be establishment of procedures to provide an enhanced employee training environment and overarching programs to enhance individual employees' awareness of their information security responsibilities.

This particular program, which includes several hundred specific actions, is oriented on improving the position of the VA in the entire area of information protection.

To date, we have had about 40 percent of the actions completed.

One especially important action was the completion and publication of VA Handbook 6500 back in September 2007. This handbook describes the VA Information Security program, and it also includes the national rules of behavior, a document that employees must sign before they are given access to our computer systems and sensitive information.

While we have made progress, there is still much to be done. With respect to FISMA, there are five problematic areas for VA: Annual testing and system inventory; the plan of action and milestone process; certification and accreditation of IT Systems; configuration management; and security awareness training. These are problem areas for us.

We continue to make progress in each of these, and the actions to correct related deficiencies are all included in that comprehensive action plan that I just mentioned.

Incident response in our program for oversight and compliance are two very important initiatives where we have made substantial progress. And these activities I believe are definitely making a difference throughout VA. But even with all we have accomplished, we still experience security and privacy incidents. We consider any data breach to be serious if veteran or employee sensitive personally identifiable information is at risk. Many of these incidents are the result of human error and carelessness, which is why it is so important to establish a culture and a strong environment of

awareness and individual responsibility throughout the organization.

In closing, we have a variety of aggressive programs in place that will ultimately help us achieve the Gold Standard in data security which, since the summer of 2006, has been a major goal of VA. Much more remains to be done, but I remain personally committed to working toward achieving this gold standard goal, and I can assure you that VA senior leaders are equally committed.

Thank you for your time and attention today, and I am prepared to answer any questions you may have.

Senator CARPER. General Howard, thanks very much. Ms. Swart. Welcome.

TESTIMONY OF SUSAN SWART,[1] CHIEF INFORMATION OFFICER, BUREAUM OF INFORMATION RESOURES MANAGEMENT, U.S. DEPARTMENT OF STATE

Ms. SWART. Good afternoon, Chairman Carper and Senator Coleman. I am pleased to have this opportunity to testify before the Subcommittee concerning the protection information and information technology. My statement will provide an overview of the Department of State's Information Security Program, followed by a few suggestions on enhancing FISMA.

The Department employs a defense in depth security strategy providing multiple levels of protection to address the global nature of our operations.

Over our global unclassified network, we process weekly about 25 million e-mails and instant messages from more than 50,000 employees and contractors at 100 domestic and 260 overseas locations.

Weekly we block 3.5 million SPAM e-mails, intercept 4,500 viruses, and detect over a million external probes on our network. Cognizant of these risks, the Department leveraged it's experience handling classified information when we deployed Internet access across the enterprise and limited Internet access points.

In a continuation of this theme, the Department has been actively involved with the trusted Internet connection effort. The Department employs network vulnerability scanning tools that provide systems administrators worldwide with daily validation reports. These reports include information on patch management, anti-virus updates, and security configuration compliance.

The tools provide appropriate and timely risk management data to administrators who have the means to address issues at the local level.

Now I would like to highlight some of the specific efforts that support the Department's defense in depth security strategy.

To further FISMA's goal of providing better information security, the Department established a Deputy Assistant Secretary level Information Security Steering Committee representing a cross section of Department officials.

The forum provides a high level opportunity to ensure that the principles of sound information security management are instilled upon all Department employees as they fulfill their roles regardless of geographic location.

[1] The prepared statement of Ms. Swart appears in the Appendix on page 106.

In 2003, the Department of State was cited by an independent financial auditor for having a fragmented information security program that allowed for vulnerabilities to arise in the areas of external and internal systems security controls. As a result, the Department's information security program was identified as a material weakness.

Through the efforts of numerous Department officials, continuous and measurable progress was made in addressing the independent auditor's concerns, and in the span of 2 years, the material weakness was downgraded to a reportable condition and then a deficiency.

Given our present progress, the matter is expected to be formally closed at the end of this fiscal year.

We have also strengthened our certification and accreditation. In 2006, the Department restructured its process and allowed for appropriate ownership of certification and accreditation within the bureaus while providing centralized oversight and expertise.

These changes have been cost effective and transparent. Specifically, certification and accreditation costs were reduced by more than 70 percent in the second half of Fiscal Year 2007 while maintaining a 100 percent of system certified and accredited.

The Department has been an ardent supporter of the information systems security line of business. Presently, the Department of State and USAID information security awareness training is used by four other agencies totaling over 40,000 government employees and contractors in addition to our own.

The Department's accomplishments in the area of privacy include the development of a breach notification policy, procedures for a core response group in the event of a breach, reduction and elimination of the use or dissemination of Social Security numbers, and enhanced attention to privacy impact assessments in the certification and accreditation process.

The Department has a process in place for encrypting all of its mobile computing devices. Department mobile users may only access the Department's unclassified network through a two-factor authentication system.

Reauthentication is required after 15 minutes of inactivity, which exceeds the standard.

While the Department and the rest of the community has made great strides under FISMA, there is room for improvement.

As GAO has noted, FISMA is structured in a manner where disparities in audit scope, methodology, and content exist. A possible FISMA enhancement is the development of a common Inspector General evaluation framework. Another enhancement is the addition of quantifiable standardized repeatable metrics that allow an agency to detect and react to cyber security threats and manage vulnerabilities.

The Department has a variety of security service including continuous network monitoring, intrusion detection, technical countermeasures, threat analysis, and physical and technical security programs, none of which are completely reflected in the current FISMA metrics.

Mr. Chairman, I want to conclude by reiterating the State Department's unyielding commitment to information security. I thank

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

Senator CARPER. Ms. Swart, thank you very much for that testimony. And we will now turn to Mr. Ash. Welcome.

TESTIMONY OF DARREN B. ASH,[1] DEPUTY EXECUTIVE DIRECTOR FOR INFORMATION SERVICES AND CHIEF INFORMATION OFFICER, U.S. NUCLEAR REGULATORY COMMISSION

Mr. ASH. Thank you. Mr. Chairman, thank you for the opportunity to appear today to discuss the U.S. Nuclear Regulatory Commission's efforts to protect its information technology assets and sensitive information.

The NRC is very much aware of the magnitude of the computer security challenge and the importance of strengthening our defenses to meet it.

While a computer security program has been in existence at the NRC since 1980, in November 2007, the agency established a new organization, the Computer Security Office, as the focal point for agency-wide efforts. In addition to addressing the core requirements of FISMA, the Computer Security Office works with other NRC offices on strategies to protect sensitive information.

In September 2007, the NRC Inspector General identified two significant deficiencies: A lack of current certification and accreditation and a lack of annual contingency plan testing for most of the agency's systems. The NRC declared its Information Security Program as a material weakness.

Over the succeeding months, the NRC has taken aggressive action to strengthen our Information Security Program across a broad range of activities. These include the following: Certifying and accrediting 12 systems since April 2007, representing 32 percent of the 37 major applications and general support systems. The NRC plans to certify and accredit 10 additional systems by June 2008 and expects that all remaining systems will be certified and accredited in Fiscal Year 2009; consolidating systems within our inventory, and, where possible, modernizing legacy applications sooner; and requiring that tests of system contingency plans be conducted by the end of June 2008 as well as linking the requirement to Senior Executives' performance.

The NRC also recognizes the importance of providing staff the information security training necessary to carry out their assigned duties effectively. Rapid technology changes make it necessary to constantly refresh the skills and expertise of employees to keep pace with these changes. To date, the NRC has provided comprehensive information security awareness and general security training to all employees.

Despite the challenges, the NRC remains firmly committed to meeting the standards and requirements of FISMA. Nonetheless, I believe implementation improvements are needed. Compliance, as currently measured, does not permit an accurate view of the effectiveness of its implementation because metrics concentrate on development of plans, policies, and procedures, and the implementa-

[1] The prepared statement of Mr. Ash appears in the Appendix on page 115.

tion of controls. These metrics assume that all controls are of equal weight and importance. In practice, this is not true. For instance, FISMA could be adjusted to include a requirement to report on agency controls to prevent data leaks. Furthermore, reporting should give greater weight to the implementation of controls that defend against high impact threats and that counter the most significant vulnerabilities.

I believe that FISMA requirements are sufficiently comprehensive and flexible to permit an agency to balance compliance requirements against overall needs for security. However, overemphasis on the annual report card does not allow for a clear picture of the relative security posture of agencies. Implementing security that aims to simply satisfy reporting requirements will not necessarily lead to an effective Information Security Program.

In summary, executive management at the highest levels—Chairman Klein, the Commission, has taken responsibility for the security of NRC's information systems and FISMA compliance. The NRC is taking strong and deliberate steps to build a sound Information Security Program to address the security of NRC's information systems and correct FISMA compliance shortfalls. My goal is to provide an effective security program that weighs risk, openness, and cost as an institutionalized part of NRC business practices.

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

Senator CARPER. Thank you, Mr. Ash. Mr. Heneghan. I am interested to hear how you guys got all those A-pluses.

TESTIMONY OF PHILIP HENEGHAN,[1] CHIEF INFORMATION SECURITY OFFICER, U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT

Mr. HENEGHAN. Thank you, Chairman Carper and Members of the Subcommittee, for the opportunity to testify on USAID's information security program and our implementation of FISMA.

I would like to begin by describing USAID's mission and the unique information security challenges created by this mission. Then I would like to report on how our risk-based information security program has successfully implemented FISMA. I will also discuss how we use innovative techniques and technologies to measure and manage the risk to our information and systems.

USAID's mission requires us to work in developing countries and work in close partnerships with many different PVOs, indigenous organizations, universities, American businesses, international agencies, other governments, and NGOs.

USAID's Office of Foreign Disaster Assistance (OFDA) also responds to complex emergencies and disasters, such as the recent events in Bangladesh, Ethiopia, Kenya, and Sudan. This requires USAID to support different risk models for network operations and creates many challenges for implementing a worldwide information security program.

Most of the USAID information technology activity occurs on AIDNET, which is a single worldwide network made up of 9,000

[1] The prepared statement of Mr. Heneghan appears in the Appendix on page 124.

interconnected workstations and 8,000 other network infrastructure devices. Approximately 3,000 of the workstations are here in Washington, with the remaining 6,000 workstations located in more than 70 countries around the world.

AIDNET is constantly changing. We recently established a new site in Banda, Indonesia, moved 11 other mission locations, will soon set up another site in Pakistan, and are regularly changing the communication channels for all sites back to Washington.

We need to understand, manage, and monitor these to our network so that we can identify any change in the risk we have accepted. Our risk-based program requires us to be continually aware of the changing structure of our network and our focus on measurement ensures we can.

Our information security program uses a risk-based management approach to effectively implement appropriate operational, technical, and managerial controls. To support this approach, we lean heavily on technologies that automate the collection and reporting of security information and metrics.

For instance, through technology we have automated our security awareness training with a USAID-developed program we call Tip of the Day. The Tip of the Day program provides a brief security lesson and prompts the user to answer a question about that lesson before the user logs into one of our networks. We have partnered with our colleagues at the Department of State to make this and other security training available to others in the Federal Government and are proud that this innovative program has been selected as a component of the Information System Security Line of Business.

For the past 4 years, we have used a robust vulnerability management program that continually scans the 17,000 systems on our network to measure their security posture. This program ensures that each system is evaluated about 10 times a month.

In 2006, we moved to the next level and implemented a risk modeling program that couples this vulnerability data with our network access rules to model our network and report any changes impacting the risks we have accepted.

This virtual modeling occurs daily and provides a true picture of our exposure to identified threats. We have also centralized the management of our entire security infrastructure in Washington to collect and analyze security events and network metrics from hundreds of remote security systems around the world.

As one of the six Einstein pilot agencies since 2006, we have exchanged situational awareness information that has benefited our agency and the wider Federal community.

This was the beginning of a strong partnership with US-CERT, including the GFIRST Program. GFIRST has provided a secure communications channel to the Federal community for us, and we are an active participant. Of course, these metrics and technologies would be useless if we did not engage the executives, managers, and system administrators responsible for individual systems and networks.

This is an area where I believe we have implemented one of the foundational tenets of FISMA. For each system and network, we have identified the executive who owns the system, and, as a re-

sult, has responsibility for and is in the best position to make risk-based decisions regarding the system's security controls.

Our experience has shown that if provided the right metrics, system owners apply the necessary resources to ensure that their systems remain at an appropriately secure level. Our responsibility is to provide those system owners with the metrics they need to make information security decisions based on risk.

Towards the goal of keeping executives informed of their security posture, we produce monthly security reports on our systems and networks and provide them to over 100 executives throughout the agency.

We deliver these metrics in a report card format so that our leadership team can readily understand and act upon the information. We have found that because our reports are accurate, consistently produced, and actionable, they are extremely effective and, as a result, USAID maintains a high level of security on all our systems.

Our experience with FISMA has generally been very positive. We have adopted the risk management principles of the law, including the regulatory guidance, and have built a robust information security program.

Protecting systems and information, though, is an ongoing effort. The threat is constantly changing, and attack methodologies are continually evolving.

Therefore, we are always concerned about the threats we do not yet know about. However, by understanding our environment and our baseline through the use of technology and process, we are in a better position to identify deviations that may indicate a new threat. We can then reduce our risk exposure by implementing new operational, technical, or managerial controls.

I appreciate the opportunity to appear before you today, and I look forward to any questions you may have.

Senator CARPER. All right. Thanks very much. Do I understand that you have gotten these A-pluses for 3 years in a row?

Mr. HENEGHAN. Yes.

Senator CARPER. And the first report card that you got was a failing grade?

Mr. HENEGHAN. Well, luckily for me, I started my job 1 week after we got an F.

Senator CARPER. One week after?

Mr. HENEGHAN. Yes. I had nowhere to go but up.

Senator CARPER. Yes. And you have.

Mr. HENEGHAN. And we got a C-minus the next year.

Senator CARPER. And then after that?

Mr. HENEGHAN. We have stayed at an A-plus since then.

Senator CARPER. You already mentioned this, alluded to it, but just walk us though again—why do you think we have seen the original, initial improvement and then the ability to sustain performance at what most would say a very high level.

How do you explain the success?

Mr. HENEGHAN. I think agency senior management took security seriously. And by finding the executives who are responsible for the systems, I think that is the better way to do it. I guess prior to the time I was there, all of the system certification and accreditation happened within the CIO's office, and we moved that out to the

owners of the systems—the CFO, for example. He is responsible for accrediting the system.

Now the certification would happen by myself across the agency—so that I can accept for the agency reasonable risk, but not allow the CFO or someone else to have more risk on the agency.

But giving them ownership has solved a lot of problems for us. That is the primary thing that we have done.

Our awareness program makes everyone aware of security. The fact that every day everyone has to answer a question has created a climate of awareness on security.

Senator CARPER. Yes. Do other agencies come to USAID and say, what is your secret here? What are you all doing and how can we emulate this? Does that happen?

Mr. HENEGHAN. Yes, that has, and a number of people——

Senator CARPER. But from whom? Anybody at this table?

Mr. HENEGHAN. Yes. State and——

Ms. SWART. Our Chief Information Security Officer, John Streuferd, used to be the Chief Information Security Officer at AID.

Senator CARPER. But did you steal him?

Ms. SWART. Yes. And our security posture is much better.

Senator CARPER. Is that right?

Senator CARPER. So in the end it is about people?

Ms. SWART. Yes.

Senator CARPER. Yes.

Ms. SWART. Can I point him out since I mentioned him?

Senator CARPER. Sure. Thank you. All right.

The agencies seem to be on the front lines in protecting our government's data. We have a responsibility, too, but the actual Executive Branch agencies are really on the front line, and I would like to get an agency's point of view on FISMA and how it has been implemented maybe for the last 5 years since it was enacted.

And could each of you maybe just briefly summarize whether or not you feel FISMA has created reliable metrics to measure your agency's information security programs? And, if not, what kind of metrics or measurements would you like to see instead? General Howard.

Mr. HOWARD. Yes, sir. I believe the metrics are fine, in FISMA . . . it is really a matter of discipline in following the instructions, getting full involvement from the leadership, as was mentioned a couple of times here at the table. The law itself is, I think, adequate. It is up to us now to deal with it and get it done, and that is where the problem is. It is not a problem with the guidance. The guidance is pretty clear. The problem is, as you well know, getting people behind it. It is a people issue, whether it is leaders or all the way down to the individual employees. I mean, that would be my opinion.

Senator CARPER. And how do we address that part of the problem?

Mr. HOWARD. Sir, the agencies have to address it. In the VA, for example, we have an intense effort to try to turn around awareness in the sense of individual responsibility, and we are not there yet. There is no doubt about it. We got a long way to go.

In the area of FISMA, as you well know, we have not done well. Last year, we got an incomplete, and we did not even get the thing in.

This year, we at least completed all of the controls that were supposed to be done. That took some doing, but we got it done. We are heading up, but I can tell you right now, there is an awful lot of work remaining.

Senator CARPER. All right. Thank you. Ms. Swart.

Ms. SWART. I think that FISMA could be improved by adding metrics that look at some of the things we are doing—scanning, network intrusion, anti-virus patching—that directly have an impact on our ability to thwart attacks, that would be an improvement.

I think FISMA—it has been good because it has raised awareness. I mean, 5 years ago, you would not have an Assistant Secretary that would pay attention to system security, and now we have done what we call 90-day pushes to get some attention of system owners that work for those Assistant Secretaries. They are engaged in that activity. And they are personally following up. So, from an awareness point of view, across the agency it has been very successful. People are tuned into the importance of securing our systems, so in that respect, it is good.

It would also be helpful to have a common yardstick for the IGs across the Federal Government to measure our performance. I think that would also give a better sense of how well agencies are doing compared to each other. You would get a better sense of whether the F that we had in 2006 is the same F that somebody else had in 2006.

Senator CARPER. All right. Mr. Ash, I saw you nodding your head at something Ms. Swart was saying. Tell us what that was about?

Mr. ASH. It goes to the point that Ms. Swart talked about the IG. And is the F that the NRC has—that we have is it the same F that the State Department has.

Is what the IG in their audit—how they assess State Department's compliance—is it the same approach that NRC's Inspector General took?

I included it as part of my written testimony, but that gets back to the point of we need a consistent approach—it is not a matter of the law. But it is a matter of how the Inspectors General address an audit consistently across the Federal space.

It is a good way—being able to have that commonsense of, is an F an F across the board? Is an A an A? Is USAID's A the same as another agency's?

Senator CARPER. Theirs is an A-plus.

Mr. ASH. Oh, I am sorry, an A-plus.

But going back to your other question I want to answer—your question gets back to, for me, it is commonsense metrics. How effective are we in defending the perimeter, defending—implementing controls? How effective are we in enforcing and actually applying rules of behavior, not just signing a rules of behavior form, but actually knowing that we are actually adhering to it?

Those are the types of real time, real metrics that give me a better sense of how effective is it. It is not just how many certification and accreditations we have implemented, how effective our pro-

gram process is, but again the people. Are the people educated? Do they understand why we are doing this? Do the executives understand this and are they really following through on the rules of behavior?

Senator CARPER. Are we measuring effectiveness now?

Mr. ASH. I think in some aspects yes. Probably the one area that I have always been a firm believer in is what they call the plan of action and milestone process, where we identify risk, where we identify a vulnerability. An effective security program means that you are doing a good job identifying what those risks and vulnerabilities are, tracking them, documenting and tracking them and ultimately resolving them; again, addressing ultimately those risks and vulnerabilities, but having a legitimate, managed process to do that.

Senator CARPER. All right. Mr. Heneghan.

Mr. HENEGHAN. The eight points in the FISMA law, I think, are effective. I do agree that better metrics to make sure, as Susan was saying, that you are aware of how many intrusions are happening to you; are your systems being patched. Do you have a good vulnerability management system. There is a lot of metrics associated with that, but I think OMB could ask for as part of the current FISMA reporting process, and I think those type of metrics would help get to the results that everyone here is looking for.

Senator CARPER. All right. Was there anything that folks on the first panel said that you just really resonated with you strongly, that you said, that is for sure? I really think that is a great point.

Was there anything that you heard from the first panel that you said, I do not agree with that? Maybe a point or two from each of you on that. Mr. Ash, you want to go first?

Mr. ASH. I think the one comment that resonated with me from a negative perspective was the comment that was made by the industry representative about the Inspectors General——

Senator CARPER. Which comment was that?

Mr. ASH [continuing]. That if you are doing well, maybe you take a pass on having an audit the following year.

I do not think that is a valid or an appropriate approach. I think the Inspectors General have a defined responsibility, and I think for me, for the NRC, it continues to identify—having an annual audit will always give me an opportunity to identify weaknesses.

Senator CARPER. OK. All right. That might be something on the minus side. Anything on the plus side that you want to just underline and underscore for us?

Mr. ASH. I agree with Ms. Evans' comment about FISMA getting away from paper, and for agencies that are doing well, it means that they have really taken it to heart. It is not just the paper-based process. It really is you are doing security for the right reasons. You are doing it for the agency, and you are doing it for the mission.

Senator CARPER. All right. Thank you. Ms. Swart.

Ms. SWART. I think both of the gentlemen on the first panel commented again about the metrics and the standard yardstick, so I definitely agree with that.

On the negative side, the comment that because of the way FISMA is viewed to be a paper exercise, which I do not think most

agencies view it as, that leads to complacency about security. I do not think that is true.

I think that, at least based on the experience in our agency, security is a very important activity, growing in visibility, and yes, there are improvements that we can make and better ways to measure it, but I do not think that agencies are complacent. It is too visible and becoming more visible, so I do not think that was an accurate statement.

Senator CARPER. All right. Thank you. Mr. Heneghan.

Mr. HENEGHAN. This might have been a question, but I think that using technology that is available in the marketplace and bringing that to bear on our systems. We have done that for our risk modeling program, which is primarily only used by Banks, but we use our vulnerability management process, again, a commercial product. So I think using the commercial market—because technology is changing so fast. They are keeping up with it, and we need to stay with them to keep up.

Senator CARPER. All right. Thank you. General Howard.

Mr. HOWARD. I would like to comment on the incident report. Again, I think you were the one who asked why there are so many incidents in the VA, there is no question as to why there are—we are reporting them with rigor.

Incidents clearly existed before, but now we report all of them as matter of policy. Do not even think twice. If you think you have an incident, get it reported, because we have got one hour for the information to get to the US-CERT. So, when you operate that way, you are going to have a lot of incidents.

Fortunately, most of them are minor, but, every once in a while, we have one that is rather serious, requiring an investigation or whatever.

Every one of them, though, we pay attention to, even if it is only involving one veteran. We notify the individual. And if we believe his information may have been compromised, credit monitoring is offered.

Senator CARPER. I guess at the VA, as you all know, and let me just say there are some things that you do at the VA are terrific—the way you have harnessed information technology for the delivery of health care, something that we are emulating, trying to do in Delaware, statewide, is wonderful and as a veteran who appreciates that we are now able to save money, save lives, make employees, the agency employees, more productive. I think that is just great stuff.

Mr. HOWARD. Sir, I am glad you mentioned that.

Senator CARPER. Yes.

Mr. HOWARD. Could I make another comment on that?

Senator CARPER. Please. Yes.

Mr. HOWARD. Because what you are talking about is a major challenge for us within VA and the whole area of information protection.

It is a balance issue. Let me give you a good example—the Standard Desktop Configuration that was mentioned earlier. We are now going through that in the VA—we are the second largest organization—240,000 people, desktop computers and laptops all over the place.

When we first started, we had 18,000 separate applications that we had to work through. In some of these, if you apply the configuration controls, you put them out of business. I will give you a specific example—blind rehabilitation was a small computer program that was put together some years back. We will solve the problem, but you cannot automatically introduce some of these controls without testing them and being very careful in not shutting down some aspects of the business—a doctor trying to care for a veteran.

That is a very real problem in the VA, to strike that balance and get it right. We know what we need to do, but we cannot shut the business down at the same time. And we do not have time. We know we have to keep moving as rapidly as we can.

Senator CARPER. General Howard, you have been very frank and candid in saying that we do a much better job of identifying and reporting, which is commendable, but you said we have got a long way to go before where we need to be.

Do you all take advantage of an agency like USAID and just reach out to them and say well, how did you do it, and what can we learn from them?

Mr. HOWARD. Sir, we have talked to other government agencies, not USAID. We learned the hard way in May 2006. It was pretty obvious to us what needed to be done. But we have talked to other government agencies, as other government agencies have talked to us, too, lots of them.

Senator CARPER. OK. Mr. Heneghan, if General Howard wanted to talk to you before he left today, would you give him a couple of minutes?

Mr. HENEGHAN. Certainly.

Senator CARPER. So all right. Good. I think another issue that is core to complying with FISMA is the—we talked a little bit about this, too, but the independent evaluation conducted by IGs. These evaluations are crucial for a number of reasons, but, in part, because they allow agencies to work with their IGs in identifying vulnerabilities and trying to cc some of the weaknesses that have been uncovered.

Having said that, I understand that not all independent assessments conducted by agencies are to the same standard. And some agencies receive the benefit of a thorough assessment of their IT security while other agencies frankly do not. And let me just ask do you feel that this is the case and, if so, should there be a baseline standard for—set really for all independent assessments?

Ms. SWART. Yes. I think that is what a lot of us just said. Just to give an example. If you have one inventory system that you did not inventory, what should the impact be on your score or on the points, and that could be different agency to agency. Or if you are talking about awareness training, do you really need to train all the employees, including an employee like a gardener that would never access the system.

Those are just two examples that show how the OIG looks at something could impact the way they evaluate system security at one agency versus another agency.

But I do say it is very important to have the independent validation of the OIG and not just completely rely on the reporting of the IT, the CIOs.

Senator CARPER. Right. Anybody else want to add to that point?

Mr. HOWARD. One activity that we have put in place, sir, that has proved to be very helpful is our oversight and compliance capability. It is very robust. We put that in place about a year ago. Arnie Claudio, that I introduced earlier runs that. Since last January, over 155 assessments—we use the word assessment, not inspection or investigation, because we want it to be a helpful activity, identify issues and problems and help remediate them on the spot, if necessary. That is the way we have designed it, and I can tell you that has been extremely helpful to us.

It is also helpful not only in reporting problems, whether it is a rogue Internet connection, with a wire thrown out a window or helping to increase awareness among employees throughout the organization.

Senator CARPER. OK. Anybody else on this point? Yes, Mr. Heneghan.

Mr. HENEGHAN. Actually, I think the IGs would like to have a standard as well. I mean, it is not——

Senator CARPER. Why do you say that?

Mr. HENEGHAN [continuing]. Because they are struggling with the same questions we are. Do you count a gardener or not.

Senator CARPER. Gardeners or IGs?

Mr. HENEGHAN. IG types.

Senator CARPER. Maybe both.

Mr. HENEGHAN. So I think that they would like to know and do the right thing so that they could have a good measure.

Senator CARPER. Well, that is a good point.

I realize the afternoon is drawing late, but a number of the big incidents that we have heard about in the past and there is a couple that you have alluded to several of those, but some of those big incidents did not stem from a foreign country or from a disgruntled hacker, but really from current employees.

Let me just ask how do your agencies continually test and evaluate your employees' knowledge of IT security? How do your agencies hold your employees accountable, from senior managers, all the way down to an intern, and finally you think what you are doing is enough?

Mr. HOWARD. Sir, training and education is very key, and, of course, there is a requirement for 100 percent training and education in security and privacy every year. We go through that. The other key aspect is leadership involvement. We have training programs focused on our leaders, what their responsibilities really are, because you are a former military person. This is a squad leader activity. If you are not looking at the troops and talking to them and making sure they are doing what they are supposed to do, you are going to have problems.

Senator CARPER. Yes, if the leader does not think it is important, nobody else will.

Mr. HOWARD. Exactly right. And I am not talking about just at the top—all the way down, right at the job site, if you will.

So the issue of training is important. And then disciplinary action. We have taken disciplinary action in some cases. It is a people issue, no question about it.

But the other thing I would say you also have to provide them the tools. In the VA, we have gone to encrypted thumb drives, and the reason that we have done that is, our young doctors and young interns, they are like your kids. It is hard to discipline them and get them to stay focused on the importance of the information that they are walking around with this thumb drive. So we mandated the use of encrypted thumb drives, and they have to carry this information around to do their job.

Now they can do it with some degree of comfort, because if they loose their thumb drive in the parking lot, it is a rock. I mean, it is not going to be of any value to anybody. The same is true with encrypted laptops—or VA laptops are encrypted now. If somebody steals one, they are useless. You cannot get into them.

Senator CARPER. All right. Are there others, on the issue of education? Go ahead, please. Ms. Swart.

Ms. SWART. We are one of the providers to other agencies, as I mentioned, in partnership with AID. We do annual awareness training, so if you want to keep your logon to the system, you do this training. You take a test. It includes both information security questions and privacy questions on an annual basis.

Senator CARPER. But for your employees, they cannot logon to their system?

Ms. SWART. If after a year, automatically they will be asked to take this online test. And if they do not take it, they are locked out.

On the personal responsibility side, we do have a computer security incident program that does provide for penalties for information security type infractions or violations that is patterned on what we do for classified information.

Senator CARPER. OK. Mr. Ash.

Mr. ASH. The NRC has seen a great deal of value in not just computer-based training, but in-person training. The last couple of years, the agency has used in-person training to make sure that employees have had the opportunity not just to hear what the requirements are and the expectations, but also have the opportunity to address their concerns and ask questions.

It is the best opportunity in terms of just interfacing and direct interaction with people that know what the requirements are and can help educate.

At times there can be—depending on how the computer-based training is set up, if you do not really test them, I mean, really test them, what value is it? And that is what I have come to appreciate about the NRC's approach—again, the in-person training.

Senator CARPER. Mr. Heneghan.

Mr. HENEGHAN. Our Tip of the Day program, again, from the headlines news. We will put out a tip on a *Washington Post* article that came out. Everyone gets an idea of what is going on; that it is an important issue.

It is tough to know how effective training is, but I think we have a greater incident reporting now from individuals because they know of this. They are much more aware of it.

An example I used, just last week, someone was out in the food court, where there was a couple of Federal agencies, doing a survey and asking a lot of detailed questions about how people remotely login. That person immediately reported it, because we have tips

out there that say be careful of people asking you questions like this. And GSA escorted the person off the premises.

It gives me a good feeling that our awareness program is effective. It has also been used by our Office of General Counsel, when we take action against individuals because they know they shouldn't be doing it, and, in fact, over the last year, they have answered four questions that say, yes, I am not supposed to do this. I know that. And our Office of General Counsel uses that to see people out the door, if they are prone to be policy violators.

Senator CARPER. All right. You may have heard I asked the first panel at the close of their presentations and responses, I asked them to give some advice to us in the Legislative Branch, some advice on what we should do more of or less of that would be constructive here. And we got a variety of ideas, and I think generally quite helpful ones.

I am going to ask you all the same question in just a moment, but before I do, I have a question for Mr. Ash.

I was fortunate to go with Chairman Kline, the Chairman of the Nuclear Regulatory Commission, up to Peach Bottom a month or so ago, where it had some security lapse problems, and we went up there to find out what happened and see what is being done to make sure it does not happen again. There are any of 103 other nuclear power plants. I chair a subcommittee, on nuclear safety, along with Senator Voinovich of Ohio.

But one of the things that we have learned that takes place within the nuclear power plant industry and within the NRC itself, the Nuclear Regulatory Commission, is it sounds like every 3 years there is a force on force exercise, where bad guys, who are really good guys that are trained to be bad guys, attempt to penetrate the IT systems or the electronic—they are not doing anything electronically. They use real force—and to go in and try to take over physically a plant, a nuclear power plant.

And then they do a fair amount of debriefing and lessons learned and that sort of thing. But it is real to the extent nobody gets killed. But it is a very real exercise, and I think from what I hear it is actually quite informative, and you actually measure not process, but actually measure whether or not people are secure and they are ready at one of these 104 plants to take on an assault.

When you think of that approach to security and you look at our approach to security with respect to protecting our information, our databases and all. Can we learn a lesson from the force on force that we see in the nuclear power plants? Is there something that they are doing there that could help inform what we are doing to protect our other information and these data breaches?

Mr. ASH. Yes. I think the easiest answer, the easiest lesson, is continue to test. Force on force exercise—I told you I joined the NRC a little over 10 months ago, and had the opportunity early on in my tenure to observe a force on force exercise out in Illinois. Absolutely amazing just to see the approach that they take. Again, the objective is to identify weaknesses and to measure how successful—obviously if the perpetrators can be successful, but how successful are the security measures that are put in place by the plant and the licensees and the security force.

But going back to my original point: Continue to test—penetration testing; social engineering testing—all opportunities, because those are what the bad guys are going to use, opportunities to send malicious e-mails, phishing expeditions. I mean, phishing with a "ph"—means to try and get you as an employee of an agency to give up a password, give up sensitive information or give up access when you are not really aware of it. That is probably the best lesson learned that I think we could take from what the NRC does with the force-on-force type exercises.

Senator CARPER. All right. Good. Thank you.

Mr. ASH. You are welcome.

Senator CARPER. All right. Ms. Swart, did you want to say something?

Ms. SWART. The government does do these cyber storm exercises, which do provide those kinds of testing. There is one going on right now that we are participating in other agencies that are sponsored I believe by the Department of——

Senator CARPER. You call them cyber storms?

Ms. SWART. Yes.

Senator CARPER. Do they have code names or anything?

Ms. SWART. I think that is the code name.

Senator CARPER. All right. Advice for us, some in the Legislative Branch?

Mr. HOWARD. Sir, keep the pressure on. It helps us to balance the issue that I mentioned before. Keep the attention on this important area of information protection. It is very helpful to us, in spite of the fact we are up here, every once in a while getting beaten up, it is a good thing that you keep the pressure in this area. It is helpful to us.

Senator CARPER. Good. Thank you. Ms. Swart, what can we do that might be constructive or really that would be constructive?

Ms. SWART. I would second that about the visibility. Also just the things that we have said about improving the way we do the measuring through the existing process, not necessarily changing the law.

Senator CARPER. All right. Thank you. Mr. Ash.

Mr. ASH. I will second that one; third that I guess. The other point that I guess that I would like to make is continue to encourage the Executive Branch and the Federal Government to look at and implement solutions that can help us. It is difficult enough for a small agency to implement trusted Internet connections. That is why I appreciate what OMB and the agencies are doing—the Desktop Configurations. Encourage that. Support it. That is what I would ask.

Senator CARPER. All right. Thank you. Mr. Heneghan.

Mr. HENEGHAN. I would just reiterate the metrics, but also I think not changing the law because that would cause a whole other process, but actually just tweaking it a little bit would be the way to do it. And get more metrics out there that we can compare each other against and everyone will start to feel comfortable that it is a good measurement process.

Senator CARPER. OK. Mr. Bennett, in his testimony, in his written testimony, listed a number of recommendations for our consideration. And I do not know if you all have had a chance to look

at those recommendations. I am not going to ask you to comment on them today here at the hearing, as we draw to a close. But one of the things that I am going to ask you in writing as a follow up is just to share your comments on the recommendations. Which do you like? Which do you think maybe do not meet muster, and which would you tweak a little bit and maybe they would meet muster?

If you all could help us with that, I would appreciate it.

Again, other Members of our Subcommittee I suspect Dr. Coburn and I know— I started to say Dr. Coleman—but Mayor Coleman, Senator Coleman, I am sure they have some questions to provide in writing. My guess is that some other Members of our Subcommittee will, too. And we would appreciate if you would respond to those as fully and as promptly as you can.

I am just very grateful on behalf of all of us, not just on the Subcommittee, not just on our Committee, not just the Senate, but the work that you are doing is real important, and you know that. And I understood that coming into this hearing, but I am certainly reminded of it even more so today—important for our country, important for our national security, important for our financial security—just important for a lot of peace of mind for people. So those of you who are getting A-pluses and those that are on your way to getting those A-pluses, stay on that glide slope and we will breathe a little bit easier in the future.

With that having been said, this Subcommittee is adjourned, and we wish you a good evening. Thank you.

[Whereupon, at 4:55 p.m., the Subcommittee was adjourned.]

APPENDIX

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
SENATE HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY

March 12, 2008

Good afternoon, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about the state of Federal information security, and the implementation of controls to improve information security.

Securing Federal information and information systems has been an Administration priority, and over the last several years we have focused management attention on improving our security processes and protection measures. We have approached the challenges presented in our Federal operating environment by building a strong Federal information security framework. This framework stresses implementation of risk-based and cost-effective information security controls to provide the appropriate levels of information protection. Since the passage of the Federal Information Security Management Act of 2002 (FISMA), we continue to make progress. Throughout this testimony, we will highlight our results, and briefly describe some of our initiatives intended to close remaining performance gaps.

Information Security Progress and Priorities

The Federal Information Security Management Act (FISMA) was passed by Congress and signed into law by the President as part of the E-Government Act of 2002 (Pub. L. No. 107-347). This law, and the resulting policies and guidance, set a base framework from which agencies have developed their information security programs. OMB policies and subsequent National Institute of Standards and Technology (NIST) guidance focus on a risk-based, cost-effective approach and reflect the balance between strong security and mission needs. As required by 44 U.S.C. § 3543, Federal agencies must comply with standards developed by NIST and promulgated by the Secretary of Commerce, and identify information security protections consistent with these standards. Agencies are responsible for implementing the policies and guidance for their unique mission requirements within their capital planning and investment control processes. Agency officials who manage and operate the agency business programs are ultimately responsible and accountable for ensuring security is integrated into those program

operations. Our oversight is achieved in two primary ways -- via the budget and capital planning process, and through independent program reviews.

On March 1, 2008, we submitted the Government-wide fifth annual report to Congress, entitled "Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002," http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf

Since 2002, we have been monitoring government-wide progress in implementing key FISMA performance metrics. We would like to note, in fiscal year 2007 we met a significant milestone by certifying and accrediting (C&A) over 90% of all systems. The C&A process, as described in NIST guidance, includes a comprehensive assessment of the management, operational, and technical security controls; and, an official management decision given by a senior agency official to authorize operation of an information system. The certification process is in place to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements and managing the system's risk to an acceptable level.

Baseline security controls for selection and testing throughout the system C&A have been outlined in NIST's Federal information security control catalog. Security control requirements are determined when agencies categorize their information and information systems for risk impact levels (high, moderate, or low). Systems containing information with higher risk impact level, have stronger required baseline controls than information systems containing less sensitive information.

As you can see in the table below, since 2002, we have increased our percentage of C&A'ed systems from 47% to 92%, while increasing the total number of systems by nearly 30%. Concurrently, we have also improved our rate of contingency plan testing and annual follow-up testing of system security controls. At the end of 2007, 80% of the 25 major agencies reported a C&A rate between 90% and 100% for operational systems. This makes it clear that progress is spread across Federal agencies and not limited to agencies with a large inventory.

Security Status and Progress from Fiscal Year 2002 to Fiscal Year 2007						
Percentage of Systems with a:	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY2007
Certification and Accreditation	47%	62%	77%	85%	88%	**92%**
Tested Contingency Plan	35%	48%	57%	61%	77%	**86%**
Tested Security Controls	60%	64%	76%	72%	88%	**95%**
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	**10,304**

To validate the quality of agencies' self-reported metrics, we ask agency Inspectors General (IG) to assess the quality of the processes behind the reported

numbers. In fiscal year 2007, 76% of reporting agency IGs rated the overall quality of C&A processes to be "satisfactory" or better in fiscal year 2007, while the number of agencies with the lowest rating (poor) was reduced from 9 in fiscal year 2006, to 4 in fiscal year 2007.

In addition to gauging C&A completion and security control implementation at the system level, we are also working to strengthen security controls on Federal desktops. Over the past year, in collaboration with NIST, the Department of Defense, the National Security Agency, and Microsoft, we have developed a set of information security controls to be implemented on all Federal desktops which are running Microsoft Windows XP or VISTA. This set of controls, known as the Federal Desktop Core Configuration (FDCC) is currently being implemented across the Federal enterprise. By implementing a common configuration, we are gaining better control of our Federal systems, allowing for closer monitoring and correction of potential vulnerabilities. Security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources.

To continue our trend of performance improvement, over the next year we intend to focus information security and privacy management attention on:

- Achieving 100% C&A levels for all operational systems;
- Properly identifying and providing oversight of contractor systems;
- Reducing or eliminating systems in the FISMA inventory uncategorized by risk impact level;
- Improving agency identification and reporting of security incidents;
- Increasing general and job-specific training for Federal employees and contractors;
- Maintaining appropriate privacy documentation for 90% of applicable systems; and,
- Completing activities related to privacy recommendations.

Securing Sensitive Information and Personally Identifiable Information

On June 23, 2006, we released Memorandum M-06-16, entitled "Protection of Sensitive Agency Information." (http://www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf) In this memorandum, recommendations were made to compensate for the lack of physical security controls when sensitive information is removed from, or accessed from outside the agency location. The memo contained a requirements checklist, along with the following recommended actions:

1. Encrypt all data on mobile computers/devices which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
2. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;

3. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes inactivity; and
4. Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required.

To make the Federal government's identity theft awareness, prevention, detection, and prosecution efforts more effective and efficient, the President's Identity Theft Task Force issued "Combating Identity Theft: A Strategic Plan." The strategic plan instructed the OMB and the Department of Homeland Security (DHS) to develop a paper identifying common risks (or "mistakes") and best practices to help improve agency security and privacy programs. The risks, best practices, and important resources are inter-related and complementary. Agencies apply them when administering their information security and privacy programs. The report can be found at: http://csrc.nist.gov/pcig/document/Common-Risks-Impeding-Adequate-Protection-Govt-Info.pdf).

Subsequently, building on the work of the President's Identity Theft Task Force, OMB issued Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," in May 2007. The purpose of Memorandum M-07-16 is to enhance agency protections on personally identifiable information through the establishment of agency breach notification policies and risk mitigation frameworks. Memorandum M-07-16 reiterated the recommended security measures from Memorandum M-06-16, and further required these actions to be taken as they relate to personally identifiable information.

In each agency's Fourth Quarter FY 2007 President's Management Agenda E-Government scorecard, OMB included language requiring agencies to submit a status update by December 14, 2007, as well as a date when each agency would be in full compliance of the M-07-16 requirements. We are working with agencies to refine these plans, and will continue to leverage the quarterly scorecard process as a management tool, to ensure agencies continue to improve required security control implementation.

Detecting Access to Federal Information Systems

While strong security controls can help reduce the number of information security incidents, experience shows some incidents and attacks cannot be prevented. Consequently, an effective incident detection and response capability is critical.

As shown in the table below, in fiscal year 2007, 12,986 incidents were reported to the DHS incident response center for six categories of incidents, which is more than twice the amount of incidents reported in fiscal year 2006.

Incident Reporting to DHS US-CERT			
Incident Categories	FY 2005	FY 2006	FY 2007
1. Unauthorized Access	304	706	2,321
2. Denial of Service	31	37	36
3. Malicious Code	1,806	1,465	1,607
4. Improper Usage	370	638	3,305
5. Scans/Probes/Attempted Access	976	1,388	1,661
6. Under Investigation	82	912	4,056
Total Incidents Reported	3,569	5,146	12,986

While the increasing number of reported incidents seems alarming, we are finding this increase to be at least partially attributable to improved incident identification and reporting. As agencies become more aware of their operating environment, they are likely to detect previously undetectable incidents.

To further improve situational awareness and incident detection, agencies are engaged in the Trusted Internet Connections initiative (TIC), and Einstein tool deployment. Through the Trusted Internet Connections (TIC) initiative, we are working with agencies to reduce the overall number of external connections, including Internet points of presence. As agencies optimize their external connections, security controls to monitor threats will be deployed and correlated to create a government-wide perspective of our networks. To facilitate monitoring of external connections, The Department of Homeland Security (DHS) supports an application named Einstein. Einstein is an intrusion detection system, able to collect, analyze, and share aggregated computer security information across the Federal government. Einstein will enhance current incident detection abilities, and will raise government-wide awareness of information security threats and vulnerabilities. This awareness will enable agencies and DHS to take corrective action in a timely manner. We are currently working with DHS to build upon their existing deployments and extend Einstein to all of the Federal agencies.

Conclusion

In conclusion, there is evidence agencies are making progress in the area of information security and the protection of sensitive information. We are improving the quality of information security processes across the Federal government, while concurrently improving our reported performance metrics and compliance with FISMA. To further strengthen our information security and privacy posture, we are actively engaging agencies in government-wide initiatives. Through these government-wide initiatives, we are enabling Federal agencies to better focus their information security activities and resources.

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at 2:30 p.m. EDT
Wednesday, March 12, 2008

INFORMATION SECURITY

Progress Reported, but Weaknesses at Federal Agencies Persist

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-08-571T

GAO
Accountability-Integrity-Reliability

Highlights

Highlights of GAO-08-571T, a testimony before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

Information security is especially important for federal agencies, where the public's trust is essential and poor information security can have devastating consequences. Since 1997, GAO has identified information security as a governmentwide high-risk issue in each of our biennial reports to Congress. Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002, which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on the current state of federal information security and compliance with FISMA. This testimony summarizes (1) the status of agency performance of information security control activities as reported by major agencies and their inspectors general (IG), (2) the effectiveness of information security at federal agencies, and (3) opportunities to improve federal information security. In preparing for this testimony, GAO analyzed agency, IG, Office of Management and Budget (OMB), and GAO reports on information security and reviewed OMB FISMA reporting instructions, information technology security guidance, and information on reported security incidents.

To view the full product, including the scope and methodology, click on GAO-08-571T. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

INFORMATION SECURITY

Progress Reported, but Weaknesses at Federal Agencies Persist

What GAO Found

Over the past several years, 24 major federal agencies have consistently reported progress in performing information security control activities in their annual FISMA reports. For fiscal year 2007, the federal government continued to report improved information security performance relative to key performance metrics established by OMB. For example, an increasing percentage of systems governmentwide had been tested and evaluated, had tested contingency plans, and had been certified and accredited. However, IGs at several agencies sometimes disagreed with the agency reported information and identified weaknesses in the processes used to implement these and other security program activities.

Despite agency reported progress, major federal agencies continue to experience significant information security control deficiencies that limit the effectiveness of their efforts to protect the confidentiality, integrity, and availability of their information and information systems. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. In addition, agencies did not always effectively manage the configuration of network devices to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, assign duties to different individuals or groups so that one individual did not control all aspects of a process or transaction, and maintain complete continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs. As a result, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. Such risks are illustrated, in part, by an increasing number of security incidents experienced by federal agencies.

Nevertheless, opportunities exist to bolster federal information security. Federal agencies could implement the hundreds of recommendations made by GAO and IGs to resolve prior significant control deficiencies and information security program shortfalls. In addition, OMB and other federal agencies have initiated several governmentwide initiatives that are intended to improve security over federal systems and information. For example, OMB has established an information systems security line of business to share common processes and functions for managing information systems security and directed agencies to adopt the security configurations developed by the National Institute of Standards and Technology and Departments of Defense and Homeland Security for certain Windows operating systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing to discuss information security over federal systems. Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The need for a vigilant approach to information security is demonstrated by the dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology. 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 a loss of privacy, identity theft, and other financial crimes.

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

In my testimony today, I will summarize (1) the status of agency performance of information security control activities as reported by major agencies and their inspectors general (IG), (2) the effectiveness of information security at federal agencies, and (3) opportunities to improve federal information security. In preparing for this testimony, we analyzed the Office of Management and

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

Budget's (OMB) FISMA report for fiscal year 2007[3] and the annual FISMA reports and the performance and accountability reports for 24 major federal agencies;[4] examined agency, IG, and our reports on information security; and reviewed OMB FISMA reporting instructions, information technology (IT) security guidance, and information on reported security incidents. We conducted our work, in support of this testimony, from February 2008 through March 2008, in the Washington, D.C. area. The work on which this testimony is based was performed 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.

Results in Brief

Over the past several years, major federal agencies have consistently reported progress in performing certain information security control activities. In fiscal year 2007, the percentage of certified and accredited[5] systems governmentwide reportedly increased from 88 percent to 92 percent. Gains were also reported in testing of security controls – from 88 percent of systems to 95

[3]Office of Management and Budget, *Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002*, March 1, 2008.

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

[5]OMB requires that agency management officials formally authorize their information systems to process information and accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan.

percent of systems – and for contingency plan testing – from 77 percent to 86 percent. These gains continue a historical trend that we reported on last year.[6] However, IGs at several agencies sometimes disagreed with the agency reported information and identified weaknesses in the processes used to implement these and other security program activities.

Despite the progress reported by agencies, they continue to confront long-standing information security control deficiencies that limit the effectiveness of their efforts in protecting the confidentiality, integrity, and availability of their information and information systems. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. In addition, agencies did not always effectively manage the configuration of network devices to prevent unauthorized access and ensure system integrity, install patches on key servers and workstations in a timely manner, assign duties to different individuals or groups so that one individual did not control all aspects of a process or transaction, and maintain complete continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs. As a result, federal systems and sensitive information are at increased risk of unauthorized access and disclosure, modification, or destruction, as well as inadvertent or deliberate disruption of system operations and services. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies.

Nevertheless, there are opportunities for federal agencies to bolster information security. Federal agencies could implement the hundreds of recommendations made by GAO and IGs to resolve prior significant control deficiencies and information security program shortfalls. In addition, OMB and other federal agencies have initiated several governmentwide initiatives that are intended to improve security over federal systems and information. For

[6]GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007).

example, OMB has established an information system security line of business to share common processes and functions for managing information systems security and directed agencies to adopt the security configurations developed by the National Institute of Standards and Technology and Departments of Defense and Homeland Security for certain Windows operating systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

Background

Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Therefore, it is important for agencies to safeguard their systems against risks such as loss or theft of resources (such as federal payments and collections), modification or destruction of data, and unauthorized uses of computer resources or to launch attacks on other computer systems. Sensitive information, such as taxpayer data, Social Security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes. Critical operations could be disrupted, such as those supporting national defense and emergency services or agencies' missions could be undermined by embarrassing incidents, resulting in diminished confidence in their ability to conduct operations and fulfill their responsibilities.

Critical Systems Face Multiple Cyber Threats

Cyber threats to federal systems and critical infrastructures can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and nontargeted attacks. A targeted attack is when a group or individual specifically attacks a critical infrastructure system. A nontargeted attack occurs when the intended target of the attack is uncertain,

such as when a virus, worm, or malware[7] is released on the Internet with no specific target. The Federal Bureau of Investigation has identified multiple sources of threats to our nation's critical information systems, including foreign nation states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled employees working within an organization. Table 1 summarizes those groups or individuals that are considered to be key sources of cyber threats to our nation's information systems and infrastructures.

[7]Malware" (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

Table 1: Sources of Cyber Threats to Federal Systems and Critical Infrastructures

Threat source	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
Foreign nation states	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. Also, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of the Central Intelligence Agency, can affect the daily lives of Americans across the country.*
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.

Source: Federal Bureau of Investigation, unless otherwise indicated.

*Prepared statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

There is increasing concern among both government officials and industry experts regarding the potential for a cyber attack. According to the Director of National Intelligence,[8] "Our information infrastructure—including the internet, telecommunications

[8] *Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence*, Feb. 5, 2008.

networks, computer systems, and embedded processors and controllers in critical industries—increasingly is being targeted for exploitation and potentially for disruption or destruction, by a growing array of state and non-state adversaries. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year."

Increased Vulnerabilities Could Expose Federal Systems to Attack

As federal information systems increase their connectivity with other networks and the Internet and as the system capabilities continue to increase, federal systems will become increasingly more vulnerable. Data from the National Vulnerability Database, the U.S. government repository of standards-based vulnerability management data, showed that, as of March 6, 2008, there were about 29,000 security vulnerabilities or software defects that can be directly used by a hacker to gain access to a system or network. On average, close to 18 new vulnerabilities are added each day. Furthermore, the database revealed that more than 13,000 products contained security vulnerabilities.

These vulnerabilities become particularly significant when considering the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks. Thus, protecting federal computer systems and the systems that support critical infrastructures has never been more important.

Federal Law and Policy Established Federal Information Security Requirements

FISMA sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. FISMA's framework creates a cycle of risk management activities necessary for an effective security program, and these activities are similar to the principles noted in our study of the risk management activities of leading

private sector organizations[9]—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. More specifically, FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems used or operated by the agency or on behalf of the agency. In this regard, FISMA requires that agencies implement information security programs that, among other things, include

- periodic assessments of the risk;
- risk-based policies and procedures;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations.

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

In addition, agencies must develop and maintain an inventory of major information systems that is updated at least annually and report annually to the Director of OMB and several Congressional Committees on the adequacy and effectiveness of their information security policies, procedures, and practices and compliance with the requirements of the act.

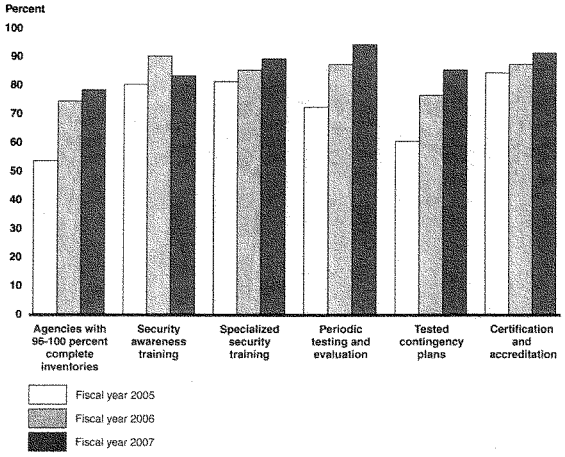
OMB and agency IGs also play key roles under FISMA. Among other responsibilities, OMB is to develop policies, principles, standards, and guidelines on information security and is required to report annually to Congress on agency compliance with the requirements of the act. OMB has provided instructions to federal agencies and their IGs for preparing annual FISMA reports. OMB's reporting instructions focus on performance metrics related to the performance of key control activities such as developing a complete inventory of major information systems, providing security training to personnel, testing and evaluating security controls, testing contingency plans, and certifying and accrediting systems. Its yearly guidance also requires agencies to identify any physical or electronic incidents involving the loss of, or unauthorized access to, personally identifiable information.

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

Agencies Report Progress in Performing Control Activities, but Some IGs Report that Weaknesses Exist

Major federal agencies have continued to report steady progress over the past several years in performing information security control activities, although IGs at several agencies identified inconsistencies with reported information. According to OMB and agency FISMA reports, the federal government continued to improve information security performance in fiscal year 2007 relative to key performance metrics established by OMB. For fiscal year 2007, IGs reported that more agencies had completed approximately 96-100 percent of their inventories and the governmentwide percentage of employees with significant security responsibilities who received specialized training increased. Percentages also increased for systems that had been tested and evaluated at least annually, systems with tested contingency plans, and systems that had been certified and accredited. However, agencies reported a decline in the percentage of employees and contractors who received security awareness training (see fig. 1). In addition, IGs at several agencies sometimes disagreed with the information reported by the agency and have identified weaknesses in the processes used to implement these and other security program activities.

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



Source: GAO analysis of agency FISMA reports

Inventory of Systems

In fiscal year 2007, 24 major federal agencies reported a total of 10,285 systems, composed of 8,933 agency and 1,352 contractor systems. Table 2 summarizes the number of agency and contractor systems reported by the agency by system impact level.

Table 2: Total Number of Agency and Contractor Systems in FY07 by Impact Level

Impact Level	Agency	Contractor	Total
High	1,089	121	1,210
Moderate	3,264	513	3,777
Low	4,351	334	4,685
Not Categorized	229	384	613
Total	8,933	1,352	10,285

Source GAO analysis of agency FY2007 FISMA reports.

IGs reported that 19 agencies had completed approximately 96-100 percent of their inventories, an increase from 18 agencies in 2006. However, IGs identified problems with system inventories at several agencies. For example, three agency IGs did not agree with the reported number of agency systems or systems operated by a contractor or another organization on the agency's behalf and one IG for a large agency reported that it did not agree with the number of agency owned systems. Additionally, one agency IG identified discrepancies in the number of system interfaces and interconnections reported and one IG reported the agency lacked procedures to ensure contractor systems are identified. Without complete and accurate inventories, agencies cannot effectively maintain and secure their systems. In addition, the performance measures used to assess agencies' progress may not accurately reflect the extent to which these security practices have been implemented.

Security Awareness and Specialized Training

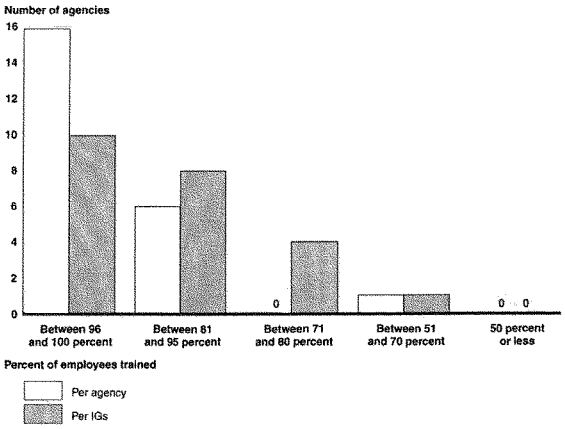
Overall, agencies reported a decline in the percentage of employees and contractors receiving security awareness training. According to agency FISMA reports, 84 percent of total employees and contractors governmentwide received security awareness training in fiscal year 2007, a decrease from 2006 in which 91 percent of employees and contractors governmentwide received security awareness training. However, 10 agencies reported increasing percentages of employees and contractors receiving security awareness training and five other agencies continue to report that 100 percent of their employees and contractors received security awareness training. In addition, each agency reported it had explained policies regarding peer-to-peer file sharing in security awareness training, ethics training, or other agencywide training.

Governmentwide, agencies reported an increasing percentage of employees with significant security responsibilities who received specialized training. In fiscal year 2007, 90 percent of these employees had received specialized training, compared with 86 percent in fiscal year 2006.

Although the majority of agencies reported improvements in both the percentage of employees and contractors receiving security

awareness training and the percentage of employees with significant security responsibilities who received specialized training, several did not. For example, nine agencies reported a decrease in the percentage of employees and contractors who received security awareness training. In addition, several IGs reported weaknesses in agencies security awareness and training efforts. For example, one IG reported that the agency was unable to ensure that contractors received security awareness training and another IG reported that the agency security awareness program needs to increase employees' awareness of social engineering techniques and the importance of protecting their usernames and passwords as a result of successful social engineering attempts. Two agency IGs also noted that weaknesses exist in ensuring that all employees who have specialized responsibilities receive specialized training. Further, eight agency IGs disagree with the percentage of individuals that their agency reported as having received security awareness training. Figure 2 shows a comparison between agency and IG reporting of the percentage of employees receiving security awareness training. Failure to provide up-to-date information security awareness training could contribute to the information security problems at agencies.

Figure 2: Percentage of Employees Receiving Security Awareness Training As Reported by Agencies and IGs



Source. GAO analysis of agency FY2007 FISMA reports.

Note: One agency IG did not provide the percentage of employees and contractors who received security awareness training. This agency is not included.

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

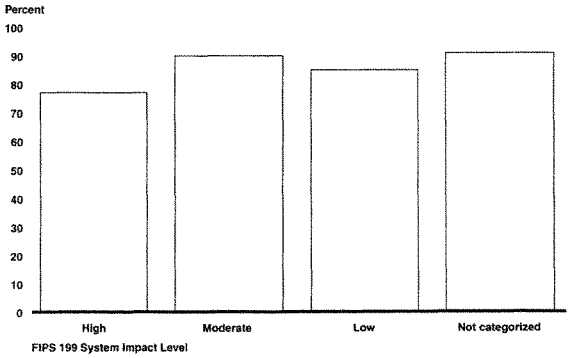
In 2007, federal agencies reported testing and evaluating security controls for 95 percent of their systems, up from 88 percent in 2006. The number of agencies that reported testing and evaluating 90 percent or more of their systems also increased from 16 in 2006 to 23 in 2007. However, IGs reported shortcomings in agency procedures for testing and evaluating security controls at several agencies. For example, 11 IGs reported that their agency did not always ensure that information systems used or operated by a contractor met the requirements of FISMA, OMB policy, NIST guidelines, national security policy, and agency policy. In addition, two IGs reported that agencies did not conduct their annual assessments using current NIST guidance. As a result, these

agencies may not have reasonable assurance that controls are implemented correctly, are operating as intended, and producing the desired outcome with respect to meeting the security requirements of the agency. In addition, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving the agencies' information and systems vulnerable to attack or compromise.

Continuity of Operations

Federal agencies reported that 86 percent of total systems had contingency plans that had been tested, an increase from 77 percent in 2006. However, as we reported in 2006, high-risk systems continue to have the smallest percentage of tested contingency plans—only 77 percent of high-risk systems had tested contingency plans. In contrast, agencies had tested contingency plans for 90 percent of moderate-risk systems, 85 percent of low-risk systems, and 91 percent of uncategorized systems (see fig. 3).

Figure 3: Percentage of Systems with Contingency Plans that Have Been Tested for Fiscal Year 2007 by Risk Level



Source. GAO analysis of agency FY2007 FISMA reports.

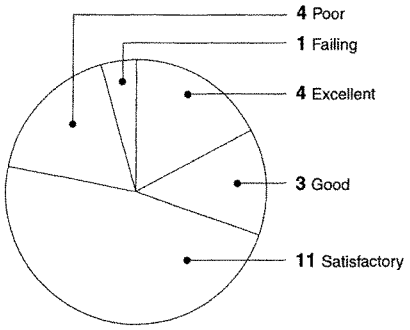
Two IGs reported that systems for their agencies were not tested in accordance with federal government requirements. Without developing and testing contingency plans, agencies have limited assurance that they will be able to recover mission-critical applications, business processes, and information in the event of an unexpected interruption.

Certification and Accreditation

Federal agencies continue to report an increasing percentage of systems that have been certified and accredited. For fiscal year 2007, 92 percent of agencies' systems governmentwide were reported as certified and accredited, as compared with 88 percent in 2006. In addition, agencies reported certifying and accrediting 95 percent of their high-risk systems, an increase from 89 percent in 2006.

Although agencies reported increases in the overall percentage of systems certified and accredited, IGs reported that several agencies continued to experience shortcomings in the quality of their certification and accreditation process. As figure 4 depicts, five IGs rated their agencies' certification and accreditation process as poor or failing, including three agencies that reported over 90 percent of their systems as certified and accredited.

Figure 4: OIG Assessment of Certification and Accreditation Process for Fiscal Year 2007



Source: GAO analysis of agency FY2007 FISMA reports

Note: One agency IG did not rate the quality of the agency certification and accreditation process.

In addition, IGs at six agencies identified specific weaknesses with key documents in the certification and accreditation process such as risk assessments, testing and evaluation, and security plans not being consistent with NIST guidance or finding those items missing from certification and accreditation packages. In other cases where systems were certified and accredited, IGs noted that contingency plans and security controls were not tested annually and security controls were not fully tested and evaluated when significant changes were made to agency systems. Additionally, one agency IG noted that the agency does not follow a formally established and documented process for certification and accreditation. As a result, reported certification and accreditation progress may not be providing an accurate reflection of the actual status of agencies' implementation of this requirement. Furthermore, agencies may not have assurance that accredited systems have controls in place that properly protect those systems.

Policies and Procedures

Agencies had not always implemented security configuration policies. Twenty-three of the major federal agencies reported that they had an agencywide security configuration policy. Although the IGs agreed that their agency had such a policy, several IGs did not agree to the extent to which their agencies implemented the policies or applied the common security configurations as established by NIST. In addition, only seven agencies reported that they complied with NIST security configuration requirements 96 percent or more of the time. If minimally acceptable configuration requirements policies are not properly implemented to systems, agencies will not have assurance that products are configured adequately to protect those systems, which could increase their vulnerability and make them easier to compromise.

As we have previously reported,[10] not all agencies had developed and documented policies and procedures reflecting OMB guidance on protection of personally identifiable information that is either accessed remotely or physically transported outside an agency's secured physical perimeter. Of the 24 major agencies, 22 had developed policies requiring personally identifiable information to be encrypted on mobile computers and devices. Fifteen of the agencies had policies to use a "time-out" function for remote access and mobile devices requiring user reauthentication after 30 minutes of inactivity. Fewer agencies (11) had established policies to log computer-readable data extracts for databases holding sensitive information and erase the data within 90 days after extraction. Several agencies indicated that they were researching technical solutions to address these issues. Furthermore, four IGs reported agencies' progress of implementing OMB guidance as poor or failing and at least 14 IGs reported weaknesses in agencies' implementation of OMB guidance related to the protection of PII. Gaps in their policies and procedures reduce agencies' ability to protect personally identifiable information from improper disclosure.

[10]GAO, *Information Security: Protecting Personally Identifiable Information*, GAO-08-343 (Washington, D.C.: Jan. 25, 2008).

Security Incident Procedures

Shortcomings exist in agencies' security incident reporting procedures. According to OMB, the number of incidents reported by agencies in their annual FISMA reports continued to fluctuate dramatically from the prior year. The majority of IGs reported that these agencies followed documented procedures for identifying and report incidents internally, to US-CERT, and to law enforcement. However, five IGs noted that the agency was not following procedures for internal incident reporting, two noted that their agency was not following reporting procedures to US-CERT, and one noted that the agency was not following reporting procedures to law enforcement (One IG did not complete the assessment for this metric). Several IGs also noted specific weaknesses in incident procedures such as components not reporting incidents reliably or consistently, components not keeping records of incidents, and incomplete or inaccurate incident reports. Without properly accounting for and analyzing security problems and incidents, agencies risk losing valuable information needed to prevent future exploits and understand the nature and cost of threats directed at the agency.

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

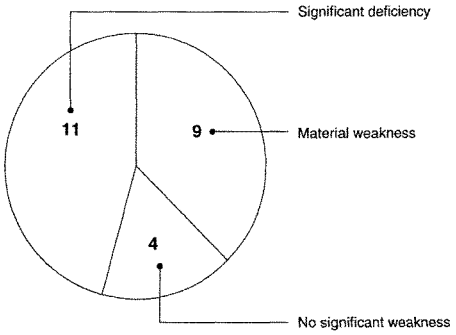
IGs reported weaknesses in their agency's remediation process. According to IG assessments, 10 of the 24 major agencies did not almost always incorporate information security weaknesses for all systems into their remediation plans. Twelve IGs found that vulnerabilities from reviews were not always included in remedial action plans and 10 IGs found that agencies were not always prioritizing weaknesses to help ensure they are addressed in a timely manner. Without a sound remediation process, agencies cannot be assured that information security weaknesses are efficiently and effectively corrected.

Significant Control Deficiencies at Federal Agencies Place Sensitive Information and Systems at Risk

Our work and that of IGs show that significant weaknesses continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the

operations, assets, and personnel of federal agencies. In their fiscal year 2007 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information security controls were either a significant deficiency or a material weakness for financial statement reporting (see fig. 5).[11] Our audits continue to identify similar conditions in both financial and non-financial systems, including agencywide weaknesses as well as weaknesses in critical federal systems.

Figure 5: Number of Major Agencies Reporting Significant Deficiencies in Information Security



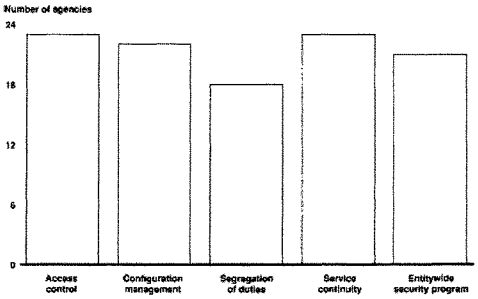
Source GAO analysis of agency performance and accountability reports for FY2007

Persistent weaknesses appear in five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can

[11]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.

independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Figure 6 shows the number of major agencies with weaknesses in these five areas.

Figure 6: Number of Major Agencies Reporting Weaknesses in Control Categories



Source: GAO analysis of agency, IG, and GAO reports for FY2007.

Access Controls Were Not Adequate

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

Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or

information. Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. To illustrate, 23 of 24 major agencies reported weaknesses in such controls. For example, agencies did not consistently (1) identify and authenticate users to prevent unauthorized access, (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate, (3) establish sufficient boundary protection mechanisms, (4) apply encryption to protect sensitive data on networks and portable devices, and (5) log, audit, and monitor security-relevant events. Agencies also lacked effective controls to restrict physical access to information assets. We previously reported that many of the data losses occurring at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

Weaknesses Also Existed in Other Controls

In addition to access controls, other important controls should be in place to protect the confidentiality, integrity, and availability of information. These controls include the policies, procedures, and techniques for ensuring that computer hardware and software are configured in accordance with agency policies and that software patches are installed in a timely manner; appropriately segregating incompatible duties; and establishing plans and procedures to ensure continuity of operations for systems that support the operations and assets of the agency.

However, 22 agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, or patch key servers and workstations in a timely manner. In addition, 18 agencies did not always segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction. Furthermore, 23 agencies did not always ensure that continuity of operations plans contained all essential information or were sufficiently tested. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

Agencywide Security Programs Were Not Fully Implemented

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented all the FISMA-required elements for an agencywide information security program. An agencywide security program, required by FISMA, provides a framework and continuing cycle of activity for assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Our analysis determined that 21 of 24 major federal agencies had weaknesses in their agencywide information security programs. Our recent reports illustrate that agencies often did not adequately design or effectively implement policies for elements key to an information security program.

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

- One agency's risk assessment was completed without the benefit of an inventory of all the interconnections between it and other systems. In another case, an agency had assessed and categorized system risk levels and conducted risk assessments, but did not identify many of the vulnerabilities we found and had not subsequently assessed the risks associated with them.
- Agencies had developed and documented information security policies, standards, and guidelines for information security, but did not always provide specific guidance for securing critical systems or implement guidance concerning systems that processed Privacy Act-protected data.
- Security plans were not always up-to-date or complete.
- Agencies did not ensure all information security employees and contractors, including those who have significant information security responsibilities, received sufficient training.

- Agencies had tested and evaluated information security controls, but their testing was not always comprehensive and did not identify many of the vulnerabilities we identified.
- Agencies did not consistently document weaknesses or resources in remedial action plans.

As a result, agencies do not have reasonable assurance that controls are implemented correctly, operating as intended, or producing the desired outcome with respect to meeting the security requirements of the agency, and responsibilities may be unclear, misunderstood, and improperly implemented. Furthermore, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving their information and systems vulnerable to attack or compromise. Consequently, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. In prior reports, we and the IGs have made hundreds of recommendations to agencies to address specific information security control weaknesses and program shortfalls. Until agencies effectively and fully implement agencywide information security programs, including addressing the hundreds of recommendations that we and IGs have made, federal information and information systems will not be adequately safeguarded to prevent their disruption, unauthorized use, disclosure, or modification.

Incidents at Federal Agencies Place Sensitive Information and Systems at Risk

The need for effective information security policies and practices is further illustrated by the number of security incidents experienced by federal agencies that put sensitive information at risk. Personally identifiable information about millions of 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.

These incidents illustrate that a broad array of federal information and critical infrastructures are at risk.

- The Department of Veterans Affairs (VA) announced that computer equipment containing personally identifiable information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. Until the equipment was recovered, veterans did not know whether their information was likely to be misused. VA sent notices to the affected individuals that explained the breach and offered advice concerning steps to reduce the risk of identity theft. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised.

- The Transportation Security Administration (TSA) announced a data security incident involving approximately 100,000 archived employment records of individuals employed by the agency from January 2002 until August 2005. An external hard drive containing personnel data, such as Social Security number, date of birth, payroll information, and bank account and routing information, was discovered missing from a controlled area at the TSA Headquarters Office of Human Capital.

- A contractor for the Centers for Medicare and Medicaid Services reported the theft of one of its employee's laptop computer from his office. The computer contained personal information including names, telephone numbers, medical record numbers, and dates of birth of 49,572 Medicare beneficiaries.

- The Census Bureau reported 672 missing laptops, of which 246 contained some degree of personal data. Of the missing laptops containing personal information, almost half (104) were stolen, often from employees' vehicles, and another 113 were not returned by former employees. The Commerce Department reported that employees had not been held accountable for not returning their laptops.

- The Department of State experienced a breach on its unclassified network, which daily processes about 750,000 e-mails and instant

messages from more than 40,000 employees and contractors at 100 domestic and 260 overseas locations. The breach involved an e-mail containing what was thought to be an innocuous attachment. However, the e-mail contained code to exploit vulnerabilities in a well-known application for which no security patch existed. Because the vendor was unable to expedite testing and deploy a new patch, the department developed its own temporary fix to protect systems from being further exploited. In addition, the department sanitized the infected computers and servers, rebuilt them, changed all passwords, installed critical patches, and updated their anti-virus software.

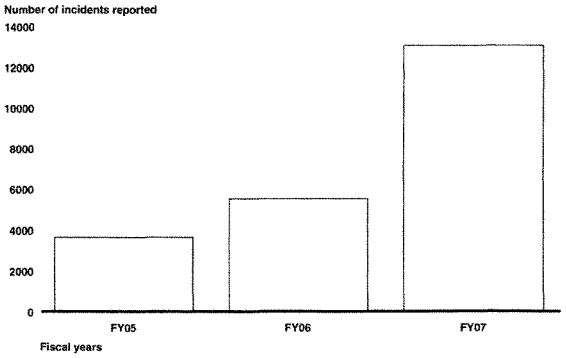
- In August 2006, two circulation pumps at Unit 3 of the Tennessee Valley Authority's Browns Ferry nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.

- Officials at the Department of Commerce's Bureau of Industry and Security discovered a security breach in July 2006. In investigating this incident, officials were able to review firewall logs for an 8-month period prior to the initial detection of the incident, but were unable to clearly define the amount of time that perpetrators were inside its computers, or find any evidence to show that data was lost as a result.

- The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as "Slammer" infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again.

When incidents occur, agencies are to notify the federal information security incident center—US-CERT. As shown in figure 7, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 3,634 incidents reported in fiscal year 2005 to 13,029 incidents in fiscal year 2007, (about a 259 percent increase).

Figure 7: Incidents Reported to US-CERT in Fiscal Years 2005 through 2007



Source GAO analysis of US-CERT data

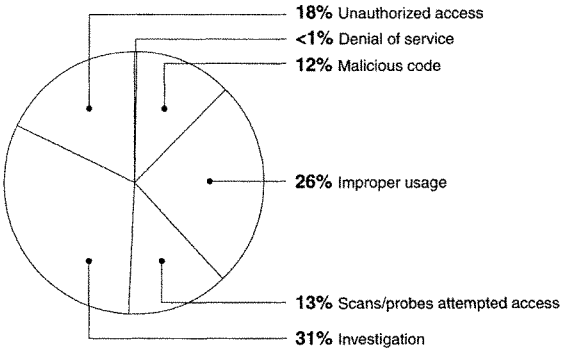
Incidents are categorized by US-CERT in the following manner:

- *Unauthorized access*: In this category, an individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- *Denial of service*: An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in a denial of service attack.
- *Malicious code*: Successful installation of 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*: A person violates acceptable computing use policies.

- *Scans/probes/attempted access*: This category includes any activity that seeks to access or identify 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.
- *Investigation*: Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

As noted in figure 8, the three most prevalent types of incidents reported to US-CERT in fiscal year 2007 were unauthorized access, improper usage, and investigation.

Figure 8: Percentage of Incidents Reported to US-CERT in FY07



Source: GAO analysis of US-CERT data

Opportunities Exist for Enhancing Federal Information Security

In prior reports, GAO and IGs have made hundreds of recommendations to agencies for actions necessary to resolve prior significant control deficiencies and information security program

shortfalls. For example, we recommended agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring and physical security. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies.

In addition, recognizing the need for common solutions to improving security, OMB and certain federal agencies have continued or launched several governmentwide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed below.

- *The Information Systems Security Line of Business*: The goal of this initiative is to improve the level of information systems security across government agencies and reduce costs by sharing common processes and functions for managing information systems security. Several agencies have been designated as service providers for IT security awareness training and FISMA reporting.
- *Federal Desktop Core Configuration*: This initiative directs agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations developed by NIST, DOD, and DHS. The goal of this initiative is to improve information security and reduce overall IT operating costs.
- *SmartBUY*: This program, led by GSA, is to support enterprise-level software management through the aggregate buying of commercial software governmentwide in an effort to achieve cost savings through volume discounts. The SmartBUY initiative was expanded to include commercial off-the-shelf encryption software and to permit all federal agencies to participate in the program. The initiative is to also include licenses for information assurance.

- *Trusted Internet Connections initiative.* This is an effort designed to optimize individual agency network services into a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence, to a target of fifty.

In addition to these initiatives, OMB has issued several policy memorandums over the past two years to help agencies protect sensitive data. For example, it has sent memorandums to agencies to reemphasize their responsibilities under law and policy to (1) appropriately safeguard sensitive and personally identifiable information, (2) train employees on their responsibilities to protect sensitive information, and (3) report security incidents. In May 2007, OMB issued additional detailed guidelines to agencies on safeguarding against and responding to the breach of personally identifiable information, including developing and implementing a risk-based breach notification policy, reviewing and reducing current holdings of personal information, protecting federal information accessed remotely, and developing and implementing a policy outlining the rules of behavior, as well as identifying consequences and potential corrective actions for failure to follow these rules.

Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

- *Clarify requirements for testing and evaluating security controls.* Periodic testing and evaluation of information security controls is a critical element for ensuring that controls are properly designed, operating effectively, and achieving control objectives. FISMA requires that agency information security programs include the testing and evaluation of the effectiveness of information security policies, procedures, and practices, and that such tests be performed with a frequency depending on risk, but no less than annually.

We previously reported[12] that federal agencies had not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. Agency policies often did not include important elements for performing effective testing such as how to determine the frequency, depth, and breadth of testing according to risk. In addition, the methods and practices at six test case agencies were not adequate to ensure that assessments were consistent, of similar quality, or repeatable. For example, these agencies did not define the assessment methods to be used when evaluating security controls, did not test controls as prescribed, and did not include previously reported remedial actions or weaknesses in their test plans to ensure that they had been addressed. In addition, our audits of information security controls often identify weaknesses that agency or contractor personnel who tested the controls of the same systems did not identify. Clarifying or strengthening federal policies and requirements for determining the frequency, depth, and breadth of security controls according to risk could help agencies better assess the effectiveness of the controls protecting the information and systems supporting their programs, operations, and assets.

- *Enhance FISMA reporting requirements.* Periodic reporting of performance measures for FISMA requirements and related analyses provides valuable information on the status and progress of agency efforts to implement effective security management programs.

  In previous reports, we have recommended that OMB improve FISMA reporting by clarifying reporting instructions and requesting IGs to report on the quality of additional performance metrics. OMB has taken steps to enhance its reporting instructions. For example, OMB added questions regarding incident detection and assessments of system inventory. However, the current metrics do not measure how effectively agencies are performing various activities. Current performance measures offer limited assurance of the quality of agency processes that implement key security policies, controls, and practices. For example, agencies are required to test and evaluate

[12]GAO, *Information Security, Agencies Need to Develop and Implement Adequate Policies for Periodic Testing*, GAO-07-65 (Washington, D.C.: Oct. 20, 2006).

the effectiveness of the controls over their systems at least once a year and to report on the number of systems undergoing such tests. However, there is no measure of the quality of agencies' test and evaluation processes. Similarly, OMB's reporting instructions do not address the quality of other activities such as risk categorization, security awareness training, intrusion detection and prevention, or incident reporting. OMB has recognized the need for assurance of quality for certain agency processes. For example, it specifically requested that IGs evaluate the quality of their agency's certification and accreditation process. OMB instructed IGs to rate their agency's certification and accreditation process using the terms "excellent," "good," "satisfactory," "poor," or "failing." For fiscal year 2007, OMB requested that IGs identify the aspect(s) of the certification and accreditation process they included or considered in rating the quality of their agency's process. Examples OMB included were security plan, system impact level, system test and evaluation, security control testing, incident handling, security awareness training, and security configurations (including patch management). While this information is helpful and provides insight on the scope of the rating, IGs are not requested to comment on the quality of these items. Providing information on the quality of the security-related processes used to implement key control activities would further enhance the usefulness of the annually reported data for management and oversight purposes.

As we have previously reported, OMB's reporting guidance and performance measures did not include complete reporting on certain key FISMA-related activities. For example, FISMA requires each agency to include policies and procedures in its security program that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In our report on patch management,[13] we stated that maintaining up-to-date patches is key to complying with this requirement. As such, we recommended that OMB address patch management in its FISMA reporting instructions. OMB's current reporting instructions only request that IGs comment on whether or not they considered

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

patching as part of their agency's certification and accreditation rating but nothing more. As a result, OMB and Congress lack information that could identify governmentwide issues regarding patch management. This information could prove useful in demonstrating whether or not agencies are taking appropriate steps for protecting their systems.

Consider conducting FISMA-mandated annual independent evaluations in accordance with audit standards or a common approach and framework. We previously reported that the annual IG FISMA evaluations lacked a common approach and that the scope and methodology of the evaluations varied across agencies.

Similar to our previous reports, we found that the IGs continue to lack a common methodology, or framework, which culminated in disparities in type of work conducted, scope, methodology, and content of the IGs' annual independent evaluations. To illustrate:

- Of 24 agency IGs, seven reported performing audits that were in accordance with generally accepted government auditing standards and one cited compliance with the Quality Standards for Inspections, issued by the President's Council on Integrity and Efficiency (PCIE).[14] The remaining IGs did not indicate whether or not their evaluations were performed in accordance with professional standards.
- One IG indicated that the evaluation focused specifically on nonfinancial systems, while others cited work conducted for financial systems as part of their evaluations. In addition, multiple IGs indicated that their reviews were focused on selected components, whereas others did not make any reference to the scope or breadth of their work.
- According to their FISMA reports, certain IGs reported interviewing officials and reviewing agency documentation, such as security

[14]The President's Council on Integrity and Efficiency was established by executive order to address integrity, economy, and effectiveness issues that transcend individual government agencies and increase the professionalism and effectiveness of IG personnel throughout government.

plans. In addition, certain IGs also conducted technical vulnerability assessments. In contrast, other IGs did not indicate their methods for evaluating controls.

- The content of the information reported by IGs varied. For example, several IGs only provided a completed OMB template, while others completed the OMB template and provided reports summarizing their evaluations. Content in these reports also differed in that several included comments on whether or not their agency was in compliance with laws and regulations.

- Several reports were comprised of a summary of relevant information security audits conducted during the fiscal year, while others included additional evaluations that addressed specific FISMA-required elements, such as risk assessments and remedial actions. Furthermore, some IGs issued recommendations to their agencies to improve the effectiveness of those agencies' information security programs, while others did not indicate whether or not recommendations were issued.

These inconsistencies could hamper the efforts of the collective IG community to perform their evaluations with optimal effectiveness and efficiency. Conducting the evaluations in accordance with generally accepted government auditing standards and/or a robust commonly used framework or methodology could provide improved effectiveness, increased efficiency, quality control, and consistency in assessing whether the agency has an effective information security program. IGs may be able to use the framework and methodology to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather sufficient, competent evidence efficiently. Having a documented methodology may also offer quality control by providing a standardized methodology, which can help the IG community obtain consistency of application.

Last year we reported on efforts to develop such a framework. In September 2006, the PCIE developed a tool to assist the IG community with conducting its FISMA evaluations. The framework

consists of program and system control areas that map directly to the control areas identified in NIST Special Publication 800-100[15] and NIST Special Publication 800-53,[16] respectively. According to PCIE members, the framework includes broad recommendations rather than a specific methodology due to the varying levels of resources available to each agency IG. According to PCIE members, this framework is one of the efforts to provide a common approach to completing the required evaluations, and PCIE has encouraged IGs to use it.

In summary, agencies have reported progress in implementing control activities, but persistent weaknesses in agency information security controls threaten the confidentiality, integrity, and availability of federal information and information systems, as illustrated by the increasing number of reported security incidents. Opportunities exist to improve information security at federal agencies. OMB and certain federal agencies have initiated efforts that are intended to strengthen the protection of federal information and information systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation of information security performance metrics and independent evaluations. Until such opportunities are seized and fully exploited and the hundreds of GAO and IG recommendations to mitigate information security control deficiencies and implement agencywide information security programs are fully and effectively implemented, federal information and systems will remain at undue and unnecessary risk.

Mr. Chairman, this concludes my statement. I would be happy to answer questions at this time.

[15]NIST, *Special Publication 800-100, Information Security Handbook: A Guide for Managers*, (Gaithersburg, Md: October 2006)

[16]NIST, *Special Publication 800-53, Revision 2, Recommended Security Controls for Federal Information Systems*, (Gaithersburg, Md; December 2007).

Contact and Acknowledgments

If you have any questions regarding this report, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this report include Nancy DeFranceso (Assistant Director), Larry Crosland, Neil Doherty, Rebecca LaPaze, Stephanie Lee, and Jayne Wilson.

Prepared Testimony of
Tim Bennett
President
Cyber Security Industry Alliance

Before the Senate Homeland Security and Government Affairs Committee
Subcommittee on Financial Management, Government Information, Federal Services, and International Security

Wednesday, March 12, 2008
2:30 pm
Dirksen Senate Office Building Room 342

Chairman Carper, Ranking Member Coburn, and other Members of the Subcommittee on Financial Management, Government Information, Federal Services, and International Security, I thank you for the opportunity to share the views of the Cyber Security Industry Alliance (CSIA) on improvements to the Federal Information Security Management Act of 2002 (FISMA). CSIA is a group of leading security technology vendors that are dedicated to ensuring the privacy, reliability, and integrity of information systems through public policy, technology, education, and awareness. It is our belief that a comprehensive approach for enhancing the security and resilience of information systems is fundamental to economic security, national security, and sustained confidence in the Internet.

This hearing is most timely and further bolsters current Congressional consideration of the need for strengthening information security within the U.S. federal government. As we have painfully learned, federal systems are frequently vulnerable to the now relentless onslaught of cyber attacks, and oversight by the Congress is an important element in holding federal agencies accountable for improved information security as well as highlighting ongoing challenges and vulnerabilities. While today's hearing is not focused on a specific legislative proposal, **we believe the 110th Congress has an important opportunity to enhance FISMA to improve the information security posture of U.S. federal government agencies.** Even though the last few years have yielded some improvements in federal information security, there are unacceptable vulnerabilities in federal government information systems that urgently need to be addressed. The federal government should be the leader in adopting effective information systems practices based on understanding and addressing risks to sensitive information and not be the poster child for what can go wrong.

The time for strengthening FISMA is now given the escalating, large scale information security intrusions and data losses that have occurred at our federal agencies over the past couple of years. As the Subcommittee explores amending FISMA, I think that it is particularly important for us to first understand the current evolving threat landscape including the nature and scope of the threats to our government's IT security infrastructure. Unsurprisingly to our members, the Information Technology Association of America's recent report[1] based on its annual survey of federal Chief Information Officers (CIOs) found, for the second year in a row, that "the broad area of IT security and cybersecurity remains the top challenge faced by Federal CIOs."

According to the Identity Theft Resource Center, the number of publicly reported data breaches rose over 40 percent in 2007 from the previous year while at the same time exposing over 127

[1] Transforming I.T. to Support the Mission: Information Technology Association of America's Eighteenth Annual Survey of Federal Chief Information Officers, February 2008

million records in 443 reported data breaches. Additionally, CSIA member company Symantec revealed in its most recent 2007 Internet Security Threat Report (ISTR) that the government sector (after home users and the education sector) is the third most targeted sector for global cyber attacks and wholly responsible for 26 percent of all data breaches that may lead to identity theft.

It has become clear that the infiltration of federal government networks and the possible theft and/or exploitation of information are among the most critical issues confronting our federal government. Several recent press reports tell of a series of attacks perpetrated by hackers operating through Chinese Internet servers against our computer systems at several federal agencies. Hackers were able to penetrate Federal systems and use "rootkits" – a form of software that allows hackers to mask their presence – to send information back out of federal agency systems. Last year, the Department of Homeland Security (DHS) reported that it had experienced 844 "cybersecurity incidents" in fiscal years 2005 and 2006. These incidents and statistics clearly underscore that we are all at risk and present clear warning signs that we must devote serious attention to our nation's information security. While progress has been made, much work remains to be done in order to truly secure our government's IT infrastructure.

FISMA has been fairly successful in getting agencies in general to pay closer attention to their information security obligations. Before FISMA, information security was not a top priority at federal agencies. FISMA has been successful in raising awareness of information security in federal agencies (for both agency leaders and their IT departments). However, federal agencies scored an average grade of "C-" on 2007's information security report card. As you know, these scores were based on FISMA audits conducted throughout the past year. Last year's average grade was a very small improvement over 2006 when agencies scored an average of "D+".

Some argue that FISMA does not adequately measure information security: a high FISMA grade doesn't mean the agency is secure, and vice versa. That is because FISMA grades reflect compliance with mandated processes: they do not, in my view, measure how much these processes have actually increased information security. In particular, the selection of information security controls is subjective and thus not consistent across federal agencies. Agencies determine on their own what level of risk is acceptable for a given system; they can then implement the corresponding controls, and certify and accredit them and thus be compliant and receive a high grade, regardless of the level of risk they have deemed acceptable.

There were encouraging signs of progress in the 2007 report, but we continue to be concerned that many mission critical agencies like the Defense Department and DHS are still lagging in their compliance. These and other agencies are lacking in implementing configuration plans, in performing annual tests of security controls, and are inconsistent in reporting incidents. The annual report card does, however, indicate that the federal government overall has made some improvements in the areas of developing configuration plans, employee security training, and certifying and accrediting systems.

FISMA does not tell the whole story when it comes to agencies' information security practices. Nowhere is an agency's ability to detect and respond to intrusions measured in FISMA. In fact, a senior DHS official testified[2] before the House Homeland Security Committee on February 28 that intrusion detection is inconsistent across the federal government. FISMA is a great baseline log, but clearly much more needs to be done in this area. We need to incentivize strong

[2] U.S. Department of Homeland Security, Under Secretary, National Protection & Programs Directorate, Robert D. Jamison before the House Homeland Security Committee, February 28, 2008

information protection policies and pursue a goal of security rather than compliance. The FISMA process is a good one, but we need to always ask ourselves if we can make it better as new threats evolve. CSIA believes that optimal security policies would require agencies to conduct effective risk assessments, monitor networks more consistently, test penetration, complete forensic analyses, mitigate vulnerabilities, establish effective access controls to protect sensitive information, and use practices such as strong authentication controls which are widely recognized in the private and public sector as effective.

Certainly, we want to avoid a 'check the box' mentality and don't want FISMA to be reduced to a largely paperwork drill among the departments and agencies, consuming an inordinate amount of resources for reporting progress while yielding few genuine security improvements. Unfortunately, in some cases, that is what it has become. Some federal agency CISOs are measured on their compliance scores with FISMA, not on whether they have adequately assessed risk in their respective agency or prevented breaches of sensitive information.
Instead, we want agencies to actively protect their systems instead of just reacting to the latest threat with patches and other responses.

With the benefit of five years' experience under FISMA and several insightful reports by the U.S. General Accountability Office, it is now possible to identify possible improvements that can address those weaknesses in FISMA implementation that have now become apparent. With global attacks on data networks increasing at an alarming rate, in a more organized and sophisticated manner, and often originating from state-sponsored sources, *there is precious little time to lose.*

The Office of Management and Budget (OMB) has been quite proactive in issuing guidance to federal agencies in an effort to improve the benefits of, and compliance with, FISMA implementation. For example, OMB issued guidance to heads of executive departments and agencies on "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" on May 22, 2007. That guidance identified a number steps that federal agencies should take to "...reduce the risks related to a data breach of personally identifiable information" and included recommendations for "...a few simple and cost-effective steps" that included: 1) reducing the volume of collected and retained information to the minimum necessary; 2) limiting access to only those individuals who must have access; and 3) using encryption, strong authentication procedures, and other security controls to make information unusable by authorized individuals.

The OMB Guidance on May 22, 2007, also provided recommendations on how to develop a breach notification policy and processes for notification should a breach of sensitive information occur. It is CSIA's observation that some federal agencies have responded effectively to this guidance and that others are still challenged with it. In addition, the National Institute for Standards and Technology (NIST) has issued several standards, particularly Special Program 800-53: Recommended Security Controls for Federal Information Systems that was based on the internationally accepted standard, ISO 17799. Nonetheless, **CSIA believes that amending legislation is needed to give the weight and suasion of law to the improvements that we are recommending with this testimony.**

The protection of information resources needs to be institutionalized and behavior changed to ensure implementation is both efficient and cost effective. Information security, once viewed as primarily a technical issue, is now a senior management issue key to successful mission accomplishment and business enablement. There needs to be an acknowledgement that security

is risk-based and, as such, nothing is absolutely secure. The effectiveness of information security is based on a number of factors including the agency's management, technical, and operations approach, how this fits the mission, the priority given and resources provided, and the incentives to maintain a long term commitment.

To assist in the Subcommittee's consideration of improvements to FISMA, CSIA offers the recommendations below.

1. **Align responsibilities and authorities to vest the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) with specific power over information security. The current authority of Agency CIOs to *ensure* should become the power to *enforce* cost effective measures of security. This must be accomplished by the CIOs of the organization's different units supporting the department-wide CIO.**

- To effectively establish and maintain a comprehensive information security program for federal agencies, CIOs and CISOs need the enforcement authority, budget authority and personnel resources to carry out this essential mission. Funding needs to be allocated to those organizations and facilities that require the most support.

- The senior management of organizations that do not actively support the information security efforts must be held accountable for the failure of the organization to meet its FISMA responsibilities. Accountability at the individual level, not just agency level, is critical to obtaining improved security.

2. **Require improvements to assessment, continuous monitoring, and remediation in order to develop a comprehensive approach to information systems security.**

- Agencies need to implement strategies for security monitoring that assesses the health and resiliency of information systems on a regular, *continuous* basis.

- Although NIST issued base-line control updates in December 2006, additional emphasis on evaluation consistency for cyber security readiness among agencies is needed. This is complicated by differences in background and expertise at the Agency Inspector General level, and by staffing and budget short-falls in some IG offices.

- Congress should codify CIO/CISO responsibility and authority for testing and continuous monitoring as needed, but more than once a year.

3. **Mandate preparation of a complete inventory of all federal agency IT assets by a certain date.**

- The federal government is responsible for a massive amount of information technology assets that is expanded and maintained by a substantial IT budget. Those assets are located within the U.S. and abroad, within government owned buildings and leased buildings, in the homes of telecommuters and others, and can be stationary and mobile. It is a complicated task to complete a comprehensive inventory, but you can't protect what you don't know about even though an enemy might know about it. Control systems have been added to NIST guidance, but this needs to be incorporated into the law. Although this is presently a requirement, implementation of a complete inventory has yet to be achieved and must be made a priority.

4. **Improve performance measurement and provide incentives to agencies that give information security a high priority.**

- OMB should establish metrics and leading indictors on an annual basis that address agency performance on a 12 to 24 month timeframe. This would provide Agencies with some lead time to identify resources and implement controls to achieve some measure of performance with the identified metrics. Using a security maturity model such as NIST's Program Review for Information Security Management Assistance (PRISMA) would also accomplish the same objectives.

- The large federal agencies and departments are viewed monolithically from the outside. Organizations such as the Departments of Energy, the Interior, or Treasury are viewed as a single organization predicated on the assumption the CIOs have management control over the policies, procedures, and implementation requirements of FISMA. In reality, the operating units must each tailor the requirements and institutionalize good security practices within their organizations. Performance must be measured and collected at both the operating unit and the Agency level.

- With the many competing priorities federal agencies face to deliver mission success in a cost-constrained environment, cyber security is seldom a high priority. Agencies need to be incentivized to provide information security high visibility and a high priority. Incentives could address a broad range of rewards from public acknowledgement to additional funding or personnel bonuses.

5. **Institutionalize security within federal agency culture.**

- Training at all levels and functional responsibilities is critical to the success of agencies' information security program.
- OMB should establish a CISO Council to meet regularly and report to Congress on the effectiveness of sharing best practices, group purchases of automated tools and training courses, and development of a more effective common curriculum for training.

6. **Codify the OMB guideline regarding notification of individuals whose sensitive personal information held by government agencies has been compromised.**

- Given the growing number of incidents where sensitive personal information held by government agencies has been compromised, agencies should be required to notify individuals of data security breaches involving sensitive personal information that pose a risk of identity theft or other harm to the individual. The policies and processes outlined in OMB's May 22, 2007 Guidance titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" should serve as the basis for language in legislation.
- Data breaches of information systems maintained by contractors or other sources working on federal projects should be promptly notified to the Secretary and CIO of the contracting agency. OMB's Fiscal Year 2007 Report to Congress on Implementation of FISMA (released on March 1, 2008) found a decreasing number of federal agencies could confirm that their agency ensures information systems used or operated by a contractor of the agency or other organization on behalf of the agency meets the requirements of FISMA, OMB policy, or NIST guidelines.

7. **Increase Federal Agency IT Security Funding.**

- President Bush's proposed budget for fiscal 2009 includes $7.3 billion for cyber security efforts -- a 9.8 percent increase from last year. We urge Congress to meet and even

exceed these proposed spending levels and help direct it to where it is most needed. In order to meet any new and enhanced FISMA requirements, agencies will continue to need sustained and increased IT security funding. Given the national security at stake, federal agencies should receive additional information security funds in FY2009 to manage the Administration's Trusted Internet Connections initiative and other priorities tied to the new Cyber Initiative. Federal agencies should not be expected to meet these requirements with current funding levels.

8. **Reaffirm objective assessments of commercially available information technologies.**

- Given that new Internet technologies have the potential to dramatically enhance government performance at a substantially lower cost, FISMA should affirm that government agencies conduct an objective assessment of their security and not fall behind the curve by limiting their procurement options because preconceived compliance concerns prevent efforts to achieve greater efficiencies, better service, and improved security.

In closing, I commend the Subcommittee for examining whether enough is being done to protect federal IT and secure sensitive information security, and asking how we can improve FISMA and federal agency information security practices going forward. FISMA can be strengthened if we develop processes and metrics that truly measure information security and help guide investments in personnel, capabilities, and information security safeguards that can more effectively secure complex federal computing enterprises. We need to get beyond focusing only on compliance processes; we need to encourage risk-based approaches to information security. We need to embrace the public-private partnership that information security requires; and we need to take steps immediately that improve both the policy and the practice of information security. The overriding objective should be to move federal agencies to act in a manner that equates strong information security practices with overall mission accomplishment. We all know what's at stake.

Thank you.

STATEMENT OF
THE HONORABLE ROBERT T. HOWARD,
ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY,
DEPARTMENT OF VETERANS AFFAIRS,
BEFORE THE SUBCOMMITTEE
ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT
INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY
U.S. SENATE

MARCH 12, 2008

Good Afternoon Chairman Carper and members of the Subcommittee. Thank you for your invitation to discuss the ability of the Department of Veterans Affairs (VA) to protect and secure sensitive data. Information protection is a top priority within VA and is highlighted as one of the five principal priorities in the FY06-11 VA Strategic Plan. As you are aware, May 3, 2006, was the day of the theft which led to the temporary loss of personally identifiable information (PII) of up to 17.5 million veterans, some of their spouses and some active duty personnel. Although our investigation confirmed that the PII was never accessed, that day was a wake up call, not only for VA, but for the entire federal government as well as the private sector. As a result of that incident, we began to improve our security posture and create the environment needed to better protect the sensitive personal information of veterans and VA employees-as well as any sensitive information entrusted to us. Today, I would like to briefly share with you some of these initiatives.

Clearly, the centralization of Information and Information Technology (IT) within VA has had a positive impact regarding the protection of sensitive information. Within this new structure we have established a separate organization called "Information Protection

and Risk Management (IPRM)" that is dedicated to improving our overall data security posture. A new Deputy Assistant Secretary (DAS) position has been established to lead this organization and help provide the important focus that is needed.

IPRM is thoroughly examining every aspect of our information protection posture in the areas of cyber security, privacy, records management, incident response, field security and business continuity to ensure that sensitive protected information (SPI), primarily PII, and Protected Health Information is not compromised. The goal is to protect the integrity, authenticity and confidentiality of VA's SPI. In essence, VA is committed to ensuring that its data is protected from unauthorized access, modification, destruction, disclosure or disposal while at the same time making it readily available for those who are authorized to use it.

Several key leaders from this organization are here with me today, Adair Martinez, my DAS for IPRM, Jaren Doherty our new Chief Information Security Officer (CISO) who is also in charge of Cyber Security, Kathryn Maginnis who is in charge of Incident Response and Risk Management, Sally Wallace who leads our efforts in the area of Privacy and Records Management, Charlie Gephart our Director of Field Security Operations and Andy Lopez who has recently established our office of Business Continuity. In addition, Arnie Claudio – the Executive Director for the Office of IT Oversight and Compliance (ITOC) - is also here today. These individuals form the VA leadership core for information protection and are focused on the implementation of a

wide variety of activities that are moving us to a much more secure posture than that which currently exists within VA.

One of the most important steps we have taken to help create a robust information security environment is to develop a comprehensive action plan, called the *Data Security - Assessment and Strengthening of Controls* program (DS-ASC). It focuses on three major areas: 1. Managerial--for example the establishment of policies and directives, 2. Technical--for example better software tools and equipment such as encrypted thumb drives, and 3. Operations--examples here would be the establishment of procedures to provide an enhanced employee training environment and overarching programs to enhance individual employees' awareness of their information security responsibilities. The DS-ASC program, which includes several hundred specific actions, is oriented on improving the position of VA in the entire area of information protection. To date, about 40 percent of the actions have been completed.

One especially important action was the completion and publication of VA Handbook 6500, dated September 18, 2007. This handbook describes the VA Information Security program. It contains the primary cyber security procedural and operational requirements Department-wide to ensure compliance with the Federal Information Security Management Act of 2002 (FISMA) and the Information Security provisions of title 38 of the US Code as well as provide for the security of VA information and information systems administered by VA, or on behalf of VA. It also includes the National Rules of

Behavior – a document that employees must sign before they are given access to our computer systems and sensitive information.

Standardized information protection policies, processes and procedures are clearly established in VA Directive and Handbook 6500. These are being implemented, and we are making progress in creating an environment of vigilance and awareness regarding individual responsibility in the area of information protection - an extremely important aspect of our overall program.

While we have made progress, there is still much to be done. With respect to FISMA, there are five problematic areas: Annual Testing and System Inventory; the Plan of Action and Milestones (POA&M) process; Certification & Accreditation of IT Systems; Configuration Management; and Security Awareness Training. I will address our progress in each of these areas.

Annual Testing and System Inventory – During FY07 100 percent of VA's IT systems underwent testing to include testing of contingency plans. We have also recently initiated efforts to improve the FISMA inventory to better characterize contractor-controlled systems.

POA&M Process – We are prioritizing POA&Ms and producing daily reports on the status of remediation actions. We are also tracking all IG-reported deficiencies in our

SMART database so that those deficiencies are accounted for in the total number of POA&Ms reported to OMB.

Certification & Accreditation (C&A) of IT Systems – Based on IG recommendations and an independent verification and validation study, VA has taken an aggressive approach in redesigning the C&A process. An intensive effort is underway to complete this work by the end of FY 08, when we have to certify and accredit (C&A) over 600 IT systems in accordance with FISMA. We have also developed a new process for FY09 and beyond where we will C&A 1/3 of all IT systems each year. Continuous monitoring and control testing will be accomplished by the team that has been established for the ongoing C&A efforts. This team involves all segments of the organization, to include a permanent C&A office as well as regional points of contact for C&A work. I am confident that our FISMA performance in this area will improve as a result of our new C&A processes.

Security and Privacy Awareness Training – Over 90 percent of all VA employees have received security and privacy awareness training. We are also using the Learning Management System (LMS) provided by OPM's HR Line of Business (LOB). This will provide for better tracking of all VA employee and contractor training. By improving the tracking, we believe we will be able to improve the accuracy of our reporting and increase the percentage of all VA employees and contractors who receive security awareness training. This system should be implemented Department-wide by the end of fiscal year 2008.

The improvements in these five areas, coupled with the recent appointment of an experienced CISO, should favorably impact our FISMA performance in FY 2008.

We have also recently transferred our Field Security organization to our DAS for Information Protection and Risk Management. This realignment will further strengthen security support to field organizations and provide all regions direct linkage for implementing information protection strategy, policies, processes and procedures throughout VA. This change meets one of GAO's recommendations.

Our incident response program is another area that has been substantially improved A well organized process is now in place wherein incident notifications received from the field that report possible exposure of sensitive information, including veteran or VA employee PII, are quickly processed, to include simultaneous notification to the U.S. Computer Emergency Response Team (US-CERT). In each case where a veteran's or VA employee's PII could be compromised, notification is sent to them with an offer for credit monitoring and/or credit protection services. In response to Public Law 109-461, Title 9 of the Veterans Benefits, Healthcare and Information Technology Act of 2006, we are also using the GSA Blanket Purchase Agreement (BPA) for independent risk analysis. We have definitely established a very robust and aggressive process for dealing with incidents. These procedures are prescribed in the Directive/ Handbook 6500 and in VA's incident response Standard Operating Procedures (SOP). We would prefer not having any incidents to process, but at least we are now able to deal with them.

We also have made substantial improvements in the area of internal assessments. These assessments focus on compliance with Directive and Handbook 6500. The ITOC was established a year ago. Using a very comprehensive checklist, this organization has already completed over 200 assessments and is having a positive impact across VA. The ITOC assessment program of 24 to 30 assessments per month is far more aggressive than the two per month experienced in the past. ITOC is working Department-wide to correct and help eliminate existing deficiencies found by the Inspector General and the General Accounting Office over the last few years. ITOC is also helping to effect real change to improve VA's FISMA compliance efforts, and continues to work with each VA Administration and Staff Office to mentor, train, and coach in order to promote an environment where the sensitive information entrusted to us is better protected.

Even with all we have accomplished, we still experience security and privacy incidents. Except for a few, these incidents usually involve the sensitive personal information on a small number of individuals. We consider any data breach to be serious if veteran or employee sensitive personal information is at risk. Many of these incidents are the result of human error and carelessness, which is why it is so important to establish a culture and a strong environment of awareness and individual responsibility. The training and education of our workforce is probably the single most important action on our list. While it may be impossible to predict, let alone prevent every security or privacy incident, it is the primary goal of VA's information protection program.

In closing, we have a variety of aggressive programs in place that will ultimately help us achieve the 'Gold Standard' in data security which, since the summer of 2006, has been a major goal of the Department of Veterans Affairs. Much more remains to be done, but I remain personally committed to working toward achieving this *Gold Standard* goal and can assure you that VA senior leaders are equally committed. We all recognize the need to establish a world class security environment wherein we can fully safeguard the sensitive and private information of veterans and employees-and all sensitive information entrusted to us. Thank you for your time and attention today – I'm prepared to answer any questions you may have.

Statement of
Susan Swart
Chief Information Officer
Bureau of Information Resource Management
United States Department of State

Senate Subcommittee on Federal Financial Management,
Government Information, Federal Services, & International Security,
Committee on Homeland Security and Governmental Affairs

Hearing on Agencies in Peril:
Are We Doing Enough to Protect Federal IT
and Secure Sensitive Information?

342 Dirksen Senate Office Building
March 12, 2008
2:30 p.m.

Good afternoon Chairman Carper, Ranking Member Coburn, and distinguished Members of the Subcommittee:

I am pleased to have this opportunity to testify before the Subcommittee concerning the protection of both federal information technology and the information that resides upon that information technology. My statement will offer an overview of the Department's information security program followed by a few suggestions on enhancing FISMA.

To meet Secretary Rice's requirement for the confidentiality, integrity, and availability of IT systems and networks in the conduct of diplomacy, the Department employs a strategic, layered approach to comprehensive risk management of our information and information assets. This security strategy, which we call "Defense in Depth," provides the Department multiple levels of defense and protection through a matrix of operational, technical, and managerial security controls. We focus on identifying and mitigating emerging threats because of our vast overseas exposure.

The diverse and global nature of the Department's operation presents a unique set of challenges to continually provide the highest level of information security compliance. Over our unclassified network, the Department weekly processes about 25,000,000 e-mails and instant messages from our more than 50,000 employees and contractors at 100 domestic and 260 overseas locations. Also, on a weekly basis, we block 3.5 million spam e-mails, intercept 4,500 viruses and detect over a million anomalous external probes to our network. The evolving regulatory environment and the escalating threat environment place a considerable burden upon Department resources. The Department's dynamic personnel landscape, composed of Civil Service, Foreign Service, Locally Engaged Staff and contractors operating at posts throughout the world requires a level of coordination that is unparalleled to that experienced by any other agency. The Department is largely able to overcome any cultural barriers through the use of coalitions and collaborative efforts focused on specific compliance requirements and other tangible improvements. As an example, the Cairo embassy, which employs hundreds of locally engaged staff representing numerous different cultures who speak a number of different

languages is held to the same standard as the Malabo embassy, which employs less than 50 full-time staff. Moreover, the Department is able to leverage the expertise gleaned from its extensive information sharing relationships with other civilian, law enforcement and intelligence agencies to enhance its IT security practices.

At the direction of former Secretary of State Powell, and embraced by Secretary Rice, the Department embarked on an aggressive program to modernize its IT systems and networks ensuring that every employee had Internet access. While Internet access can and has greatly facilitated the conduct of diplomacy, it also brings inherent risks. To begin addressing risks on its sensitive but unclassified network, the Department leveraged its experience handling classified information and narrowed Internet access points. In a continuation of this theme, the Department has been actively involved with the Trusted Internet Connection effort. The Department's architecture includes requisite perimeter security tools and devices, virus detection and response capability, an effective patch management program, network operations and traffic flow analysis, intrusion detection, Einstein deployment and response capability, security configuration controls and compliance verification to name a few. At each of our domestic and overseas locations we employ U.S citizen Information System Security Officers. At 10 overseas locations, we also have highly-trained, mobile, cyber security engineers.

It is worth noting that the cyber security team at State won the National Security Agency's prestigious Frank B. Rowlett Award for its organizational excellence in information assurance in 2005 – a first for the State Department. In 2005 and 2007, the Department's Chief Information Security Officer was one of three finalists selected for the individual excellence in information assurance – another first for the Department of State. Additionally, a number of individual members have won IT community-wide recognition for their contributions and leadership.

In a recent OMB report issued to Congress it was stated:

> The 25 major agencies of the Federal government continue to improve information security performance relative to C&A rates and testing of contingency plans and security controls. Several larger agencies reported

> **especially notable progress** regarding these measures, including NASA, the **Department of State**, Treasury, and DoD (emphasis added).

Some of the specific and measurable efforts the Department has undertaken to achieve a robust, effective and efficient information security program are listed below.

Information Security Steering Committee / Governance

In furtherance of FISMA's goal and intent of providing a comprehensive information security framework, the Department established an Information Security Steering Committee with the hope of bringing together the Department's strongest minds to tackle the complexities and subtleties that information security poses. The Committee is a Deputy Assistant Secretary level working group consisting of a cross section of Department officials including: owners of technology and security senior managers. In addition to meeting statutory requirements, the forum provides a high-level opportunity to ensure that the principles of sound information security management are instilled upon all Department employees as they fulfill their roles, regardless of geographic location.

One of the Committee's first actions was to address the Department's lackluster Congressional FISMA grade[1] by utilizing Integrated Information Security Teams composed of subject matter experts from the different segments of the Department – policy specialists, operators, and managers.

Last year's annual "90 Day Push" project focused on improving two key information security requirements—Annual Testing and System/Website Inventory. With respect to Annual Testing, workshops were conducted to increase the knowledge of all bureaus' that have information systems, explaining the annual testing methodology according to NIST guidance and to assist bureaus' in completing their responsibilities. The sessions encouraged buy-in from the bureaus to hold workshops and complete annual testing requirements. Follow-up hands on testing workshops encouraged system owners to conduct their bureau's systems re-categorizations and self-assessments by the deadline. At the end of last year's annual 90 Day Push, all goals for

[1] The FISMA grades are issued by Congressman Tom Davis in the annual FISMA report card.

Annual Testing were met. With respect to Inventory, an information system inventory data call was conducted. The inventory data call reached out to all overseas posts and domestic bureaus to collect and certify all existing systems and applications. Upon completion, 100% of Department systems and websites were certified and validation has been initiated.

Another example was the establishment of a team charged with developing a Department Information Security Program Plan. The Plan identifies the relevant laws, regulations, and policies; delineates responsibilities; describes the governance mechanism: and, catalogues the elements of the Department's operational, defense-in-depth cyber security strategy. While the Plan was fully approved by the members of the Security Committee, it was done with the understanding that the Plan is a living document responding to changes in technology and the threat environment.

Based upon the hard and tireless efforts of numerous Department officials, the Department expects to receive a significantly improved FISMA grade this year.

In addition to FISMA, the Department takes every opportunity to enhance its information security posture through additional measures and approaches. Accordingly, I would like to highlight a few of these efforts.

Independent Financial Auditor Review

Back in 2003, the Department of State was cited by an independent financial auditor for having a "fragmented information security program" that "allowed for vulnerabilities to arise in the areas of external and internal system security controls." As a result, the Department's information security program was identified as a "material weakness". The audit and the resulting "material weakness", was conducted pursuant to the Federal Managers' Financial Integrity Act of 1982.

Through the collaborative efforts of numerous officials throughout the Department, the Department made definitive, continuous and measurable progress in addressing the independent financial auditor concerns. The Department prepared and updated on a quarterly basis Corrective Action Plans establishing specific actions and defined milestones associated with

correcting cited deficiencies. In the span of two years, the independent financial auditor downgraded the "material weakness" first to a "reportable condition" and then to a "deficiency". Given our present progress, the matter is expected to be formally closed at the end of this fiscal year when the independent financial auditor completes its annual audit per OMB A-123 Circular.

Retooling Certification and Accreditation

In 2006, my predecessor established a working group, comprised of bureau executive directors, to focus on Certification and Accreditation (C&A) of the Department's systems. The working group established three certification pilots to reinforce the requirement for increased bureau involvement in the C&A function. A report of the success of these pilots, and other security governance functions that further the institutionalization of security into program areas was forwarded to the CIO's office. To execute the findings of the report, the Department instituted "Green Teams" composed of subject matter experts to manage and oversee C&As, and "Tiger Teams" to contact and conduct C&As directly with the State Department bureaus. The restructured process allowed for appropriate ownership of C&As within the bureaus, while consistently providing an oversight function and escalation point for both bureaus and Tiger Teams. These changes have been received positively throughout the Department and have been hailed as more cost effective and transparent resulting in increased communications among all interested parties. Specifically, C&A costs were reduced by more than 70% in FY07 Q2 and Q3.

In addition the Department's C&A efforts, the Department's vulnerability scanning tools provide system administrators across the world-wide enterprise with "Daily Validation" reports of vulnerabilities that exist within their zone of control in the following categories: patch management, anti-virus updates, standard operating environment compliance, and configuration compliance of mandated security settings. The tools provide appropriate and timely risk management data to administrators who have the means and ability to address any issues at the local level. Additionally, grades are assigned to ensure continued vigilance and assist senior manager oversight and resource allocation for IT security.

Largely through the combined efforts of the Certification and Accreditation program and the Evaluation and Verification Program, the Department achieved "Green-Green" status on the

Expanded Electronic Government portion of the President's Management Agenda (PMA) Scorecard for four consecutive quarters. "Green-Green" was achieved in Quarter 4 (Q4) in Fiscal Year 2006 (FY06), and in Q1, Q2, and Q3 in FY07. While the Department has slipped from 100% to 98% with its Certification and Accreditation totals, it has been and continues to be the Department goal to remain at 100%.

Information Systems Security Line of Business

From its very earliest stages of development, the Department has been an ardent supporter of the federally-focused Information System Security Line of Business. From the onset, the Department dedicated staff and resources to the initial working group responsible for identifying the aspects of information security that would most readily lend themselves to a Shared Services model. A Shared Services model is where one agency is responsible for providing service to another agency. At the development stage, key Department of State personnel assisted by drafting requisite documents to ensure the most appropriate agency would be selected to serve as a Shared Service Center. During the selection stage, a Joint Department of State and USAID collaborative effort, known as JSAS, was selected by OMB as only one of three agencies to serve as a Shared Service Center for information security awareness training. Presently, the Department of State and USAID information security awareness training solution is providing service to four other agencies totaling over 40,000 government employees and contractors in addition to their own employees and contractors. The Department of State continues to provide support to the Information Systems Security Line of Business through participation on half a dozen working groups.

Protection of Privacy

The Department continues its commitment to comply with Privacy Act provisions, protecting the rights of American citizens and aliens admitted for permanent residence and safeguarding personal information regardless of physical format. More than a decade ago the Assistant Secretary for Administration was designated the Department's Senior Official for Privacy. More recently, the Department formed the Privacy Protection Governance Board to heighten awareness and ensure the protection of personally identifiable information in all aspects of the Department's programs and activities. The Board brings together Assistant Secretaries from

throughout the Department to address the interdependencies among the security, technology, and business aspects requisite to minimizing and reducing the collection, use, and dissemination of personal information -- and especially Social Security Numbers -- and to safeguarding this sensitive information in all formats, particularly in today's dynamic electronic environment. The Department's accomplishments include the development of a Breach Notification Policy; Core Response Group procedures; reduction and elimination of the use or dissemination of Social Security Numbers; communication through websites, collectives, worldwide cables, and Department Notices; awareness building for the business owners of personal information; review of business practices and process; and enhanced attention to Privacy Impact Assessments in the Certification and Accreditation Process as reported in FISMA. While we have made considerable progress, we recognize that more work needs to be done to protect personal information within the Department.

With respect to the OMB 07-16 requirements, the Department has the following practices in place:

The Department of State is in the process of encrypting all of its mobile computing devices. The Department leveraged its PKI contract to provide encryption protection at no additional cost to the Department. The solution is fully compliant with applicable NIST standards and guidelines (FIPS 140-2).

The only means for a Department user to remotely access the Department's unclassified network is through a two-factor authentication system that combines a hand-held random generating password device and a separate password authenticated by the Department's network.

The Department's remote access solution referenced above utilizes a "time-out" function requiring user re-authentication after 15 minutes of inactivity, a standard exceeding the requirement.

As referenced in GAO's PII report, the Department along with ten other agencies are researching technical solutions to address logging for all computer-readable data extracts from databases holding sensitive information and verify that the extracts have been deleted within 90 days.

Possible Enhancements to FISMA Implementation

In December 2002, FISMA represented a valiant step forward in how the federal agency community viewed information security. The statute's requirement to "develop, document and implement" an information security program throughout a system's lifecycle was a shift in philosophy for many personnel. Although Certification and Accreditation and FISMA Plans of Actions & Milestones have now become common-place vernacular for many non-information security personnel, there is still room for improvement in the area of FISMA implementation.

FISMA provides for an annual independent evaluation of the agency's information security program. Although well-intentioned at the time, the independent annual "evaluation" has the potential for creating ambiguities. Notably, GAO reports in April 2005, July 2005, and June 2007 have all identified the lack of a common Inspector General reporting framework as a deficiency of the FISMA evaluation process. In the GAO's own words, the "lack of a common methodology, or framework, has culminated in disparities in audit scope, methodology, and content. As a result, the collective IG community may be performing their evaluations without optimal effectiveness and efficiency." FISMA implementation could be improved through an agreement amongst IG's upon a common evaluation framework.

Another enhancement would be the addition of metrics that account for an agency's ability to detect, respond to and react to cyber security threats and manage vulnerabilities. For example, as the CIO, I have the ability to leverage a wide array of independent Department security services including continuous network monitoring, technical countermeasures, counter intelligence services, threat analysis, and physical and technical security programs, related to a separate mandate to protect life, information and property around the world. The absence of recognition of these efforts may misrepresent our efforts towards FISMA compliance. Prior GAO reports in April 2005 and June 2007 have likewise identified the lack of reporting on incident response metrics as a shortcoming in the FISMA evaluation process.

Mr. Chairman, I want to conclude by reiterating the State Department's unyielding commitment to information security. I thank you and the Subcommittee members for this opportunity to speak before you today and would be pleased to respond to any of your questions.

STATEMENT OF DARREN B. ASH
DEPUTY EXECUTIVE DIRECTOR FOR INFORMATION SERVICES AND CHIEF INFORMATION OFFICER
U.S. NUCLEAR REGULATORY COMMISSION

BEFORE THE

SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY
COMMITTEE ON HOMELAND SECURITYAND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

March 12, 2008

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to appear today to discuss the U.S. Nuclear Regulatory Commission's (NRC's) efforts to protect its information technology assets and sensitive information.

As the Deputy Executive Director for Information Services and the agency's Chief Information Officer (CIO), I report directly to the Executive Director for Operations and oversee information management and information technology activities agency-wide.

To provide some context for today's hearing, I would like to outline the NRC's mission and the information-related security challenges that arise in meeting those responsibilities.

Background on NRC and IT Security Challenges

The mission of the NRC is to license and regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment. The NRC's scope of responsibility includes the regulation of commercial nuclear power plants; research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transport, storage, and disposal of nuclear materials and waste.

The NRC headquarters complex is located in Rockville, Maryland, and we maintain regional offices located in Pennsylvania, Georgia, Illinois, and Texas. The NRC also has resident inspectors assigned at all nuclear power plants and the most significant fuel cycle facilities around the country. We also have a technical training center located in Chattanooga, Tennessee.

The NRC has over 4,300 interconnected computers that exchange approximately 183,000 email messages daily. The agency's external Web site comprises over 35,000 pages of information, which are visited by people in over 200 countries, for a total of about 3.7 million pages viewed each month. In addition, in 2007, the NRC released over 66,000 new documents for public access through our centralized document and records management system that is accessible through NRC's public Web site.

The NRC is very much aware of the magnitude of the computer security challenge and the importance of strengthening defenses to meet it. Along with other agencies, the NRC has

experienced an escalation of attacks from hackers and others who wish to damage the Federal IT infrastructure. Attempts to penetrate agency networks continue to increase, computer viruses proliferate, and unscrupulous individuals are devising more clever ways to entice users, including Federal employees, to open damaging attachments or provide information to spurious Web sites.

On a monthly basis, the NRC blocks an estimated 4.7 million malicious emails. The NRC blocks the malicious emails using reputation filtering; and blocks email sent from sites/domain with a bad or malicious reputation. The NRC further filters 800,000 emails, which typically include over 31,000 "potential" SPAM messages, over 50 e-mail viruses, and over 900 suspicious e-mail attachments. On a daily basis, the NRC experiences over 500 attempts at reconnaissance of its systems, over 390 attempts to exploit the web server(s), at least 5 attempts at denial-of-service attacks, and typically 2 virus occurrences. In 2007, our monthly status reports to the U.S. Computer Emergency Response Team (US-CERT) identified more than 333,000 non-debilitating incidents.

Despite these numbers, the NRC has had to report relatively few intrusions to law enforcement. Specific denial of service attempts were lower for 2007, in part, due to discrepancies in how different intrusion detection system vendors classify denial of service attacks and improvements in the attack analysis, eliminating a large number of false positives. Further, the US-CERT Concept of Operations (ConOps) specifies limited conditions for reporting incidents to law enforcement.

NRC's IT Security Program

The NRC recognizes the importance of providing an effective IT Security Program that is compliant with the Federal Information Security Management Act (FISMA), as well as with the Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) guidance. This program must ensure the effectiveness of security controls over information resources and assets. While a computer security program has been in existence at the NRC since 1980, the agency established a new organization, the Computer Security Office (CSO), as the focal point for agency-wide efforts. In addition to addressing the core requirements of FISMA, the CSO works with other NRC offices on strategies to protect sensitive information.

Protection of Sensitive Unclassified Information

In addition to protecting classified information, the NRC generally stores and processes two types of sensitive unclassified information in the course of fulfilling its safety and security mission.

The first category is termed Safeguards Information (SGI). SGI is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act of 1954, as amended, pertaining to the measures used to safeguard nuclear facilities and materials. While SGI is sensitive unclassified information, it is handled and protected similar to classified confidential national security information, unlike other sensitive unclassified information (e.g., privacy and proprietary information). Access to SGI requires a favorable Federal Bureau of Investigation (FBI) fingerprint check, an indication of trustworthiness normally obtained through a background check, and a valid need-to-know.

The unauthorized release of SGI could result in harm to public health and safety and the common defense and security. Release could also result in the potential to impact the country's nuclear power plants and other facilities and materials licensed and regulated by the NRC.

Information designated as SGI must be protected from unauthorized disclosure and is physically controlled and protected. Protection requirements include secure storage, restricted access, document marking, limited reproduction, protected transmission, controls for information processing on electronic systems, and controls for destruction. SGI information is physically and logically stored, and processed separately from the rest of the agency's information technology.

The second category is Sensitive Unclassified Non-Safeguards Information (SUNSI). SUNSI is defined as any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and federal programs, or the personal privacy of individuals. The groups of SUNSI include Privacy Act and Personally Identifiable Information (PII); allegation information; investigation information; proprietary information; Federal, State, foreign government, and International Agency-Controlled Information; security-related information; and sensitive internal information.

The NRC considers the protection of SUNSI, including personally identifiable information a serious matter. While SUNSI "spills" have occurred and may occur again, I believe that the policies, processes, procedures and protections in place are strong.

Over the last couple of years, the OMB and NIST have defined concrete actions agencies must take to protect unclassified sensitive information better. As reported by the Government Accountability Office (GAO) in their January 2008 report, "Information Security: Protecting Personally Identifiable Information," the NRC has addressed some, but not all of the critical actions. Specific accomplishments and actions of note include:

- Designating the Deputy Chief Information Officer as the Senior Agency Official for Privacy, as required by M-05-08, "Designation of Senior Agency Official for Privacy".
- Conducting a review of NRC's policies and processes, to ensure NRC has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to PII, as required in M-06-15, "Safeguarding Personally Identifiable Information." The results of the review were provided in the FY 2006 annual FISMA report.
- Issuing on June 22, 2006, an agency-wide announcement entitled "Safeguarding Personal Privacy Information" reminding all NRC employees and contractors of their responsibilities to safeguard PII from unauthorized access.
- Providing, along with NRC's FY 2006 annual FISMA report, the results of the Senior Agency Official for Privacy's review per OMB memorandum M-06-15, an Office of Inspector General (OIG) list of systems missing from NRC's inventory of major systems.
- Issuing on September 19, 2006, a policy entitled "Protection of Personally Identifiable Information," to implement provisions of M-06-16, "Protection of Sensitive Agency Information," that:

- Prohibits the removal of electronic PII from NRC-controlled space until all PII on mobile computers or devices is encrypted[1], unless a waiver is granted;
- Prohibits staff from storing PII pertaining to NRC official business on personally-owned hard drives, removable media, and other stand-alone storage devices;
- Prohibits staff from using personally-owned computers for processing or storing PII pertaining to NRC official business other than their own PII;
- Prohibits staff from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted;
- Restricts remote access to PII information on NRC systems by requiring two-factor authentication and enforcing a 30-minute timeout;
- Prohibits emailing of PII outside of NRC's infrastructure except where necessary to conduct agency business; and
- Requires the logging and a retention assessment of PII extracts.

- Issuing on September 19, 2007, the "U.S. Nuclear Regulatory Commission Personally Identifiable Information Breach Notification Policy" and the "U.S. Nuclear Regulatory Commission Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers," as required by M-07-16, "Safeguarding Against and Responding to the Breach of PII." NRC staff was notified of both the breach notification policy and the plan to eliminate the unnecessary collection and use of Social Security numbers via an agency-wide announcement on September 19, 2007. As required by the memorandum, these documents are publicly available on the NRC's Web site at: http://www.nrc.gov/site-help/privacy.html#ssn.

Two recent examples that represent specific actions to protect NRC information systems and sensitive information are NRC's implementation of the Federal Desktop Core Configuration and the development of the National Source Tracking System:

Federal Desktop Core Configuration Compliance

NRC is working towards compliance with the Federal Desktop Core Configuration (FDCC) initiative. The FDCC is a set of information security controls or settings to be implemented on all Federal desktops running Microsoft XP or Vista. By implementing FDCC, the NRC will have a stronger baseline level of security, reducing risks from IT security threats and vulnerabilities. Even prior to February 2008, the NRC met or exceeded 213 of 237 NIST suggested settings (90 percent). The NRC will implement an additional 14 settings by May 2008, totaling 96 percent of the suggested settings. With regard to Application/Registry Settings, the NRC meets or exceeds 37 of 62 NIST suggested settings (60 percent). The NRC will implement an additional 12 settings by May 2008, totaling 79 percent of the suggested settings. The NRC will determine the path forward to close the gap in both instances, especially as the gap impacts user operations.

[1] The NRC does not currently have the resources to encrypt data on all mobile computers or devices. The NRC plans to take additional action to address this issue, along with the other technical requirements established by M-06-16.

National Source Tracking System

Radiation sources are used in many medical, industrial and research applications that are critical to the nation's health, safety and economic strength. To improve tracking of sources, the NRC has been developing a National Source Tracking System (NSTS), as required by the Energy Policy Act of 2005. The NSTS is one of the most important initiatives at the NRC. Its design will allow the NRC and, in a later release, State and other Federal agencies to track transactions involving the higher risk radioactive sources from origin through transfer to disposition thereby reducing the chance of malicious use by terrorists.

NSTS development has been difficult because of the need to ensure adequate cyber security to protect the database from unauthorized access. The NRC has made considerable progress and currently plans to deploy the NSTS by December 2008. These plans depend on the system passing mandatory systems security testing, and receiving an authority to operate. The NRC has categorized NSTS as a "high" system, meaning that confidentiality, integrity, and availability requirements are all categorized as high impact. By categorizing NSTS as high, the NRC is committed to implementing the system with the most stringent set of controls and a very strong security architecture. NSTS will be the NRC's first system to be implemented at this level. Authentication of the NSTS application requires that each user have an NRC-issued digital certificate on a separate hard token to gain access to the system.

FISMA Compliance

The NRC recognizes the importance of providing an overarching, effective information security program that complies with FISMA, as well as OMB and NIST guidance. This program must ensure the effectiveness of security controls over information resources and assets, and provide for development and maintenance of controls required to protect our systems and information.

In September 2007, the NRC Inspector General identified two significant deficiencies: a lack of current certification and accreditation for most of the agency's systems and a lack of annual contingency plan testing was not performed for all systems. The NRC declared the Information Security Program as a material weakness.

Over the succeeding months, the NRC has taken aggressive action to strengthen our IT security program across a broad range of activities. These include the following:

- Establishing and staffing the CSO to be run by a Chief Information Security Officer, who reports directly to me. The new Chief Information Security Officer, Patrick Howard, will join the NRC next week. Mr. Howard was most recently the Chief Information Security Officer for the Department of Housing and Urban Development (HUD). Mr. Howard has a strong background in FISMA and law enforcement, a superb record working with Federal agencies such as HUD and the Department of Transportation, and was instrumental in helping both of these agencies address serious FISMA deficiencies.
- Certifying and accrediting 12 systems since April 2007, representing 32 percent of the 37 major applications and general support systems. The NRC plans to certify and accredit 10 additional systems by June of 2008 and expects that all remaining systems will be certified and accredited by the end of FY 2009.

- Continuing to mature the certification and accreditation process through improved quality assurance activities and independent evaluations.
- Increasing the number of systems that have been categorized using NIST standards.
- Consolidating systems within our inventory and, where possible, modernizing legacy applications sooner.
- Requiring that tests of system contingency plans be conducted by the end of June 2008, and linking the requirement to Senior Executives' performance.

Certification and Accreditation Improvements

In the October 2007 report to OMB, the NRC Inspector General rated the NRC's Certification and Accreditation process as failing. This is due in large part to the very small number of accredited systems at the time of the audit. As referenced above, the agency has made progress during the last eleven months. To facilitate the process, we have hired additional staff to lead the Certification and Accreditation activities, and increased utilizing contractor support to supplement several accreditation activities. Further, we are constantly challenging ourselves to identify additional actions to increase efficiency. An example of this is the NRC's use of the Environmental Protection Agency's ASSERT tool starting in April 2008, which will automate our Certification and Accreditation process. The tool facilitates the development of security requirements and documentation, allows for reuse of security information as it flows through the Certification and Accreditation process, and allows close oversight and tracking of security control testing and implementation status. We believe that these efforts will expedite the Certification and Accreditation process and allow NRC to be fully compliant with NIST standards.

Another important aspect is that the NRC has focused efforts on the Certification and Accreditation of those information systems that are a high priority from a mission perspective and/or those that potentially pose a higher security risk, regardless of whether the system is new or is a legacy system.

Independent Assessment of the NRC Security Program

The NRC utilized outside expertise under contract to perform an independent review and evaluation of our Certification and Accreditation process. The purpose of this contract was to assess the direction the NRC is taking with its information security, better understand effective practices used elsewhere in the Federal government, and identify long-term improvements for Certification and Accreditation of NRC information systems. The NRC utilized Carnegie Mellon University's Software Engineering Institute (SEI), a Federally Funded Research and Development Center (FFRDC) and recognized leader in cyber-security and assessment methodology, to conduct the independent review. Staff from the SEI's CERT Program led the independent review. The independent review looked at the NRC's approach to FISMA compliance and protecting sensitive information. Specifically, this independent review:

- Evaluated the Certification and Accreditation process' compliance with FISMA and its adherence to NIST guidance;
- Reviewed the risk assessment process and risk management principles used in executing the Certification and Accreditation process;
- Determined if the resource commitment to Certification and Accreditation (funding and effort) is reasonable and appropriate; and

- Evaluated the contribution of Certification and Accreditation activities to the overall security posture of the NRC mission and supporting information systems.

The NRC also tasked SEI to conduct a benchmark assessment to compare the NRC's IT Security Program and Certification and Accreditation process to the practices of other Federal agencies. The review compared the current state of compliance with FISMA requirements with respect to percent of systems accredited, as well as the quality of documentation and the level of conservatism in the security controls implemented. The review also compared the cost of accrediting systems and the process used for certification and accreditation with the costs and best practices at the other agencies. The review concluded in January 2008, and identified opportunities for further improvement and acceleration of our Certification and Accreditation, many of which are currently underway.

IT Security Training

The NRC recognizes the importance of providing staff the information security training necessary to carry out their assigned duties effectively. Rapid technology changes make it necessary to constantly refresh the skills and expertise of employees to keep pace with the changes. To date, NRC has provided comprehensive information security awareness and general security training to all employees. Staff members with information security responsibilities also need role-specific training to enable them to fulfill their security responsibilities as information security practices and requirements change.

As a result of our comprehensive training, the NRC's costs for information security training are higher than training costs at other agencies. In FY 2007, NRC delivered and required all NRC staff to take classroom information systems security awareness training course for general users. The agency believed that it was important to sponsor an in-person class to ensure that the users fully understood their role in the organization's Information Security Program. The students were afforded opportunities to interact with instructors and have their concerns and questions answered and addressed.

The NRC annually updates its on-line Security Awareness Training Course for general users. The updated course will be available this month. Additionally, the NRC updates its security awareness courses for Information System Security Officers and System Administrators every three years. The next version of these courses will be delivered this summer.

The NRC plans to enter into an agreement with the Department of State in FY 2008 to ensure that NRC staff receives current, relevant, and consistent information security training. The agreement will allow the NRC to utilize the Department of State's services to meet NRC information security training needs. This agreement will be executed under the auspices of the Federal Information Systems Security Line of Business initiative. The Department of State's training will provide in-person training to Information System Security Officers and Executives. These courses will be customized to NRC's environment and processes so individuals will have a clear understanding of their roles and the responsibilities. In FY 2009, additional courses for Systems Owners and Managers with significant information security responsibilities will be offered. In FY 2010, additional courses will be offered to Windows-based and Linux/Unix-based administrators.

Additionally, the NRC is considering moving from an NRC-provided course for General User Security Awareness to a course provided by the Department of Defense, also under the auspices of the Information Systems Security Line of Business. Some customization of this course will be necessary because of NRC's use of Safeguards Information. The NRC plans to utilize the Department of Defense's course in FY 2009.

Finally, the NRC is sponsoring classes through Microsoft to enhance the technical skills and security knowledge of our Windows-based administrators. The first class was held in January 2008. The class focused on Securing Microsoft Windows 2003 Servers Defense in Depth. Another class is scheduled for late summer 2008 on Microsoft's Active Directory.

Thoughts about FISMA – Strengths and Weaknesses

Despite the challenges facing the NRC, the NRC remains firmly committed to meeting the standards and requirements of FISMA. I believe that among its strengths, FISMA has established a solid framework for an agency-wide IT security program and for the implementation of necessary system security controls. FISMA establishes accountability for information security. The agency head and Chief Information Officer are assigned specific information security responsibilities. FISMA also requires agencies to establish the position of Chief Information Security Officer (or senior agency information security officer). Over the last couple of years, FISMA has also led to a higher level of standardization in information security programs, terminology, policies, and practices across government, which has facilitated establishment of a higher degree of trust between agencies. This is vitally important.

Nonetheless, I believe improvement is needed. FISMA compliance as currently measured does not permit an accurate view of the effectiveness of its implementation because metrics concentrate on development of plans, policies and procedures, and the implementation of controls. These metrics assume that all controls are of equal weight and importance. In practice, this is not true. For instance, FISMA reporting could be adjusted to include a requirement to report on agency controls to prevent data leaks. Furthermore, reporting should give greater weight to the implementation of controls that defend against high impact threats and that counter the most significant vulnerabilities.

I believe that FISMA requirements are sufficiently comprehensive and flexible to permit an agency to balance compliance requirements against overall needs for security. However, over-emphasis on the annual FISMA report card does not allow for a clear picture of the relative security posture of agencies, (e.g., the expanse and complexity of agency information technology infrastructures, size of user populations, and criticality of agency missions). Implementing security that aims to simply satisfy FISMA reporting requirements will not necessarily lead to an effective information security program. There have been instances of "A" agencies suffering significant data breaches and PII "spills." This occurs because agencies are not required to report specifically on actions they are taking to prevent or minimize the opportunity for such incidents. Additionally, the occurrence of security incidents and violations is not factored into annual compliance scoring.

Finally, the role of the Inspectors General cannot be understated. My experiences with the Inspector General, both here and at my previous agencies, despite the audit findings, have been positive. Those with whom I have worked generally have performed accurate, fair assessments of the quality of agency information security programs and activities. The

findings and recommendations have only helped to mature the information security programs over time. My only suggestion is that Inspectors General should be provided tools for objectively performing this important evaluation consistently across the Federal government.

Conclusion

In summary, I reiterate that the NRC is diligently working to ensure secure systems. Executive management at the highest levels of the agency has taken responsibility for the security of NRC's information systems and FISMA compliance. The NRC is taking strong and deliberate steps to build a sound information security program to address the security of NRC's information systems and correct FISMA compliance shortfalls. My goal is to provide an effective security program that weighs risk, openness, and cost as an institutionalized part of NRC business practices in support of NRC's mission to ensure adequate protection of public health and safety, to promote the common defense and security, and to protect the environment.

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

TESTIMONY OF PHILIP HENEGHAN,
CHIEF INFORMATION SECURITY OFFICER,
U.S. AGENCY FOR INTERNATIONAL DEVELOPMENT (USAID)
BEFORE THE SENATE HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS COMMITTEE'S SUBCOMMITTEE ON
FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT
INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL
SECURITY
March 12, 2008

Chairman Carper and Members of the Subcommittee, thank you for the opportunity to testify on USAID's information security program and our implementation of the Federal Information Security Management Act (FISMA). I would like to begin by describing USAID's mission and the unique information security challenges created by this mission. Then I would like to report how our risk-based information security program successfully implements FISMA. I will also discuss how we use innovative techniques and technologies to measure and manage the risk to our information and systems.

USAID's Unique Mission Drives Our Information Systems Security Program

USAID was created as an independent agency in 1961 by the Foreign Assistance Act. Since that time, USAID has been the principal U.S. agency responsible for promoting international development by supporting: economic growth; agriculture and trade; global health; democracy; conflict prevention; and humanitarian assistance.

USAID's mission requires us to work in developing countries and work in close partnership with many different Private Voluntary Organizations (PVOs), indigenous organizations, universities, American businesses, international agencies, other governments, and Non-Governmental Organizations (NGOs). The information technology and telecommunications infrastructure in most of the countries where USAID does its work are not as robust or dependable as the infrastructure here in the United States. Yet, work with our development partners compels us to work with and be part of this developing infrastructure. Some of the information technology infrastructure issues we face in these developing countries include: unreliable power grids, non-existent fiber optic connections, expensive bandwidth, and high latency. USAID's Office of Foreign Disaster Assistance (OFDA) also responds to complex emergencies and disasters, such as the recent events in Bangladesh, Ethiopia, Kenya, and Sudan. This requires USAID to support different risk models for network operations and creates many challenges for implementing a worldwide information security program.

Most of the USAID information technology activity occurs on AIDNET, which is a single worldwide network made up of 9,000 interconnected workstations and 8,000 other network infrastructure devices. Approximately 3,000 of the workstations are here in Washington with the remaining 6,000 workstations located in more than 70 countries around the world.

AIDNET is a very active and dynamic network. We receive approximately 23 million emails a month and block the 20 million of those emails that contain viruses or are spam. USAID's firewalls are located at

more than 50 sites around the world but are managed and controlled centrally in Washington, D.C. These firewalls handle more than 11 million access attempts each day and deny 4 million of those attempts. AIDNET is constantly changing. We recently established a new site in Banda Aceh, Indonesia, moved 11 other mission locations, will soon set up another site in Pakistan, and are regularly changing the communication channels for all sites back to Washington. We need to understand, manage, and monitor these changes to our network so that we can identify any change in the risk we have accepted. Our risk-based program requires us to be continually aware of the changing structure of our network and our focus on measurement ensures we can.

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

Our information security program uses a risk-based management approach to effectively implement appropriate operational, technical, and managerial controls. To support this approach, we lean heavily on technologies that automate the collection and reporting of security information and metrics. For instance, through technology we have automated our security awareness training with a USAID-developed program we call Tip of the Day. The Tip of the Day program provides a brief security lesson and prompts the user to answer a question about that lesson before the user logs into one of our networks. We have partnered with our colleagues at the Department of State to make this and other security training available to others in the Federal Government and are

proud that this innovative program has been selected as a component of the Information System Security Line of Business (ISSLOB).

For the past four years, we have used a robust vulnerability management program that continually scans the 17,000 systems on our network to measure their security posture. This program ensures that each system is evaluated about 10 times a month. In 2006, we moved to the next level and implemented a risk modeling program that couples this vulnerability data with our network access rules (router configurations, firewall rules, and access control lists) to model our network and report any changes impacting the risk we've accepted. This virtual modeling occurs daily and provides a true picture of our exposure to identified threats; in addition, it provides a historical daily snapshot of our dynamic network to help us analyze alerts sent to us by US-CERT. We have also centralized the management of our entire security infrastructure in Washington to collect and analyze security events and network metrics from hundreds of remote security systems around the world.

We augment our situational awareness intelligence with DHS-provided technology. As one of the six Einstein pilot agencies since 2006, we have exchanged situational awareness information that has benefited our agency and the wider federal community. This was the beginning of a strong partnership with US-CERT, including the Government Forum for Incident Responders and Security Teams (GFIRST) program. GFIRST has provided a secure communications channel to the federal community for us, and we are an active participant, recently hosting the monthly GFIRST meeting in February.

Of course, these metrics and technologies would be useless if we did not engage the executives, managers, and systems administrators responsible for the individual systems and networks. This is an area where I believe we have implemented one of the foundational tenets of FISMA. For each system and network we have identified the executive who "owns" the system, and as a result has responsibility for and is in the best position to make risk-based decisions regarding the system's security controls. Our experience has shown that if provided the right metrics, system owners apply the necessary resources to ensure that their systems remain at an appropriately secure level. Our responsibility is to provide those system owners with the metrics they need to make information security decisions based on risk.

For example, when we started inventorying external websites we identified 160 USAID-branded sites. We evaluated these sites not only for compliance with OMB mandates but also scanned them for web-based vulnerabilities. As a result of these risk assessments, USAID executives decided to shut down more than 30 vulnerable sites.

Towards our goal of keeping executives informed of their security posture, we produce monthly security reports on our systems and networks and provide them to over 100 executives throughout the agency. We deliver these metrics in a report card format so that our leadership team can readily understand and act upon the information (we provide more detailed technical information to the managers and system administrators). We have found that because our reports are accurate, consistently produced, and actionable, they are extremely effective and as a result USAID maintains a high level of security on all our systems.

Conclusion

Our experience with FISMA has generally been very positive. We have adopted the risk management principles of the law, including the regulatory guidance, and have built a robust information security program. Protecting systems and information, though, is an ongoing effort. The threat is constantly changing, and attack methodologies are continually evolving. Therefore, we are always concerned about the threats we do not yet know about. However, by understanding our environment and our baseline through the use of technology and process, we are in a better position to identify deviations that may indicate a new threat. We can then reduce our risk exposure by implementing new operational, technical, or managerial controls.

I appreciate the opportunity to appear before you today, and I look forward to any questions that you may have.

Questions and Responses for the Record for Ms. Evans

"Agencies in Peril: Are We Doing Enough to Protect IT and Secure Sensitive Information?"
March 12, 2008

Questions for the Record from Senator Thomas R. Carper

1.) **Mr Bennett's written testimony provided a number of recommendations concerning many of the topics that we have discussed in-depth today and some that we have not. I would ask that you evaluate each recommendation and tell the subcommittee which ones you agree with, which ones you would modify, and which ones you disagree with. Also, if you could, provide us a detailed explanation of why you chose what you did.**

Below are Mr. Bennett's 6 recommendations, and, our position on each:

> ***1. Align responsibilities and authorities to vest the Chief Information Officer (CIO)and Chief Information Security Officer (CISO) with specific power over information security. The current authority of Agency CIOs to ensure should become the power to enforce cost effective measures of security. This must be accomplished by the CIOs of the organization's different units supporting the department-wide CIO.***

Position: We respectfully disagree with Mr. Bennett's recommendation. In order to have sustainable information security practices, program managers must be involved in crafting their information systems in such a way to meet policy requirements, reduce risk, and implement cost effective security measures. The CIO and CISO role is to assist and ensure the program managers have the tools they need and are held accountable for having security measures built into the lifecycle of the information system. To move the Federal CIOs into "enforcement" positions will create a culture of compliance, rather than a culture of results and outcomes where the program managers are mitigating risk associated with their information systems.

Existing authorities under the Clinger Cohen Act as well as the Federal Information Security Management Act (FISMA) provide adequate authority to agency CIOs. The Clinger Cohen Act identifies the CIO as the executive to advise heads of agencies on IT matters (including security), and FISMA requires the head of each agency to "Delegate to the agency Chief Information Officer [...] the authority to ensure compliance with the requirements imposed on the agency under this subchapter" which includes developing and maintaining information security policies, procedures, and control techniques.

In addition, Mr. Bennett suggests individuals are not held accountable for information security. This generalization is incorrect. Many members of the Senior Executive Service have a variety of information policy related performance measures incorporated

into their annual performance plan, and, are being held accountable for their FISMA responsibilities. In addition to accountability established through the Senior Executive Service performance measures, information security is a critical skills area covered under the Human Capital Scorecard. As a critical skills area, agencies are required to show how accountability for performance cascades through the appraisals for all relevant employees.

2. Require improvements to assessment, continuous monitoring, and remediation in order to develop a comprehensive approach to information systems security.

Position: Agree, and action is underway. As Mr. Bennett indicated in his written testimony, NIST has issued updates to their baseline security control document in December, 2006. This document is one in a suite of many NIST technical guidance documents. Recently, NIST released for public comment a draft of their Special Publication 800-39 (SP 800-39), entitled "Managing Risk from Information Systems: An Organizational Perspective." The draft of SP 800-39 can be found at: http://csrc.nist.gov/publications/drafts/800-39/SP800-39-spd-sz.pdf . One objective of this guidance is to present the concept of an agency continuous monitoring program, linking it to the agency's risk level. When used in conjunction with the suite of NIST FISMA related technical guidance, agencies will be able to conduct more comprehensive, risk-based information security activities and programs.

3. Mandate preparation of a complete inventory of all federal agency IT assets by a certain date.

Position: We respectfully disagree with Mr. Bennett's recommendation. Agencies are already required to conduct an enterprise-wide system inventory. This system inventory should capture the universe of Federal systems described in FISMA. The utility and cost-benefit of counting agency IT assets for security purposes is limited. However, the agencies have inventoried desktops specifically for the purpose of implementing the Federal Desktop Core Configuration. If enterprise-wide security controls are deployed, and network connection policies are implemented, the agencies will have awareness for devices connecting to the network to ensure they are appropriately secure.

4. Improve performance measurement and provide incentives to agencies that give information security a high priority.

Position: We respectfully disagree with Mr. Bennett's recommendation. While we agree with the intent of Mr. Bennett's recommendation – to measure performance and to make information security a high priority – we disagree with the proposed implementation. Currently, agencies are being evaluated based on information security performance measures. Two examples of this are: 1) the President's Management Agenda (PMA) E-Government scorecard; and 2) the capital planning and budget review process.

The PMA scorecard outlines high level agency information security criteria, and OMB works with agency senior management to agree upon a plan to reach the set criteria. Senior management are then held to the mutually agreed upon plan. This plan includes metrics on level of security control implementation (percentage of C&A's completed) and quality of security processes (the quality of C&A's and planned remediation actions). As part of the capital planning and budget process, security implementation and quality of processes are part of the review process. Any IT investment which does not meet the criteria is placed on OMB's management watch list. When an investment is added to the management watch list, agencies are required to correct identified project weaknesses and are subject to additional oversight.

5. Institutionalize security within federal agency culture.

Position: Agree, and action is underway. Mr. Bennett's recommendation included training, sharing of best practices, and ability for group purchases as ways to institutionalize security. It is important to highlight 2 key initiatives in this area: 1) the Information Systems Security Line of Business (ISSLOB); and 2) the GSA SmartBUY program.

1. ISSLOB. Agencies are taking advantage of products and services offered by the ISSLOB. This initiative, led by DHS and OMB was introduced in the spring of 2005. An inter-agency Task Force identified common solutions to be shared across government. The Task Force identified common solutions in four areas: security training; FISMA reporting; situational awareness/incident response; and selection, evaluation and implementation of security solutions. All agencies were asked to submit proposals to either become a Shared Service Center (SSC) for other agencies, or migrate to another agency from which they would acquire expert security awareness training services and FISMA reporting services. DHS helped coordinate the selection of SSCs, and agency implementation of these services. The awareness training SSC's focus on developing and providing the training which is required by FISMA. We gather statistics on the number and percentage of employees and contractors trained, and we report these results in our annual FISMA report. In FY2007, we reported the need for improvement in this area, with agencies reporting 85% of employees trained in general information security awareness. We anticipate this metric will improve with the development and implementation of information security training SSCs..

2. SmartBUY. SmartBUY is a Federal government procurement vehicle designed to promote effective enterprise level software management. By leveraging the government's immense buying power, SmartBUY has saved taxpayers millions of dollars through government wide aggregate buying of Commercial Off the Shelf (COTS) software products. Agencies are utilizing new SmartBUY agreements to acquire quality security products at lower costs. In one recent example, GSA and DoD established a SmartBUY agreement for products

certified through the NIST FIPS 140-2 Cryptomodule Validation Program. These certified products will be used to encrypt data at rest. This benefit is not confined solely to Federal agencies, since the Blanket Purchase Agreement (BPA) was written so that states and local governments can also take advantage of this opportunity. The state and local governments are participating under GSA's Cooperative Purchasing Program, which allows them to purchase IT products and services from both GSA's Multiple Award Schedule 70 and Consolidated Schedules that have IT special item numbers. To date 127,296 licenses have been issued across 15 states (including local governments). This has resulted in savings of $24.1 million on purchases of encryption software through use of these Federal DAR contracts and approximately $8 million using the special state and local government offers – for a total of more than $32 million in savings/cost avoidance to date.

In addition to the encryption BPA, GSA (in a companion acquisition effort) worked to complete two BPA's for credit monitoring services deemed necessary by an agency in the event of a breach of personally identifiable information (PII), as well as risk assessment services for when a breach occurs. More information about the BPA related to credit monitoring services can be found in our OMB Memorandum M-07-04, "Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf. More information about the BPA to assist agencies to assess risk associated with data loss can be found in our OMB Memorandum M-08-10, "Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)," at http://www.whitehouse.gov/omb/memoranda/fy2008/m08-10.pdf.

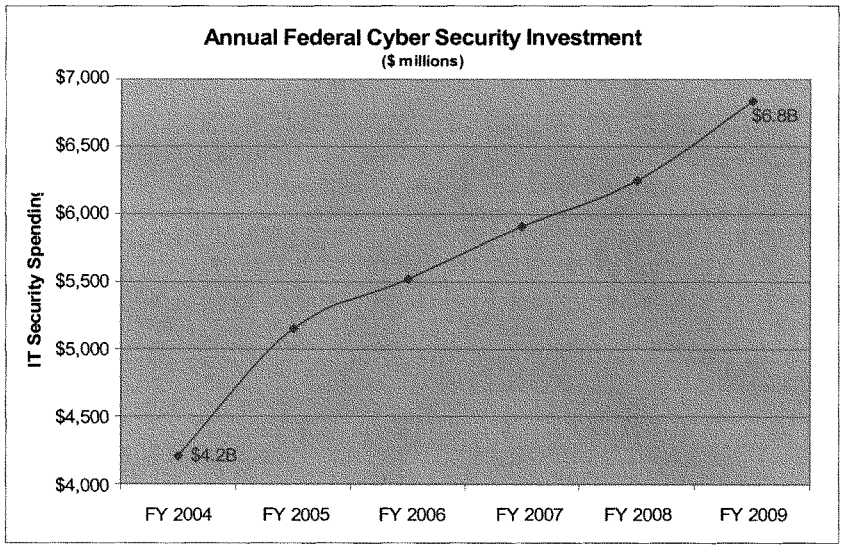
6. Codify the OMB guideline regarding notification of individuals whose sensitive personal information held by government agencies has been compromised.

Position: We respectfully disagree with Mr. Bennett's recommendation. We fully support appropriate notification of individuals, based on the risk of harm to that individual. As stated in our guidance, agencies were required to develop risk based notification policies. We feel that this is a decision that should be made at the agency level, and it should not be codified with additional legislation. Currently, the established FISMA framework gives the Director of OMB responsibility for oversight of agency information security policies and practices. Through the broad oversight function outlined in FISMA, the Director has adequate authority to issue policy and guidance as needed. One related example would be our data breach policy, which was issued on May 22, 2007 (OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information").

7. Increase Federal Agency IT Security Funding.

Position: We respectfully disagree with Mr. Bennett's recommendation. While we agree that adequate funding is required to secure Federal systems, the existing funding needs to be spent wisely and efficiently, and security needs to be funded over the lifecycle of the system investments. While funding has increased over the past 4 years, simply increasing the funding will not necessarily provide agencies with more secure systems. In order to assist agencies in adequately securing their information systems, we are working to provide agencies with cost effective cross government initiatives and tools through the ISSLOB and GSA SmartBUY programs as described above. In addition, we are standardizing required security controls through the Federal Desktop Core Configuration (FDCC) initiative, and optimizing our networks through the Trusted Internet Connection (TIC) initiative. These initiatives will help reduce vulnerabilities in order for agencies to properly manage the risk to their data and services.

As noted in the chart below, in the FY2009 Budget, agencies have requested a total of $6.8 billion dollars in information security funding. This represents an increase of 63% over the FY2004 funding level.



8. Reaffirm objective assessments of commercially available information technologies.

Position: Agree, and action is underway. Mr. Bennett's recommendation emphasizes the importance of objective security assessments, and encouragement of products that would help agencies to achieve greater efficiencies, better service, and improved security. We agree with his recommendation, and actively encourage agencies to seek out commercially available products to meet mission needs.

2.) Since 2002 when FISMA passed the Congress, the federal government has made great strides in increasing security for its information systems. However, much of the progress seems to have been made in the past few years and I think that has a lot to do with you, Ms. Evans, and I would like to commend you for that.

a. Could you comment on what efforts OMB has initiated to help agencies mitigate security risks to their information systems?

b. And also, could you explain how OMB is helping agencies move beyond a reportedly compliance-oriented mindset in managing information systems security?

Answer: OMB has undertaken a variety of activities and initiatives to reduce risk to Government information systems. In particular, we have initiated ISSLOB (as described above), the TIC Initiative, and the FDCC.

- TIC. Agencies establish points of presence on the Internet to provide timely information and services to the public, but each new connection multiplies threats and vulnerabilities. The goal of the TIC initiative is to optimize our individual network services into a common solution for the Federal government. This common solution will facilitate the reduction of our external connections, including our Internet points of presence. By reducing the number of external connections, agencies will be able to optimize their network and reduce vulnerabilities in order to properly manage their risk to their data and services.
- FDCC. Over the past year, in collaboration with NIST, the Department of Defense, the National Security Agency, and Microsoft, we have developed a set of information security controls to be implemented on all Federal desktops running Microsoft Windows XP or Vista. This set of controls, known as the FDCC is currently being implemented across the Federal enterprise. By implementing a common configuration, we are standardizing the level of security implemented on our Federal systems, and allowing for closer monitoring and correction of potential vulnerabilities while reducing our overall operating costs.

Through the initiatives mentioned above, OMB is approaching the Federal government as an enterprise. While we are still tracking system-by-system compliance and implementation of controls, we are ensuring agencies have the tools to look more broadly at the risks faced by their agency enterprise. In concert with these initiatives, there are proposed draft changes to the NIST FISMA Implementation Framework, currently out for public comment. The NIST Special Publication 800-39, *"Managing Risk from Information Systems: An Organizational Perspective,"* focuses on mitigating risk and implementing common security controls across the organization, and, implementation of

continuous monitoring of controls. Through continuous monitoring, agency security will become more dynamic in nature and thus more effective.

3.) **Ms. Evans, you have stated that the President's Management Scorecard provides accountability and feedback to the agencies by using the colors red, yellow, and green to reflect the current security environment. However, many times it shouldn't just be agencies that are held accountable, but individuals.**
   a. **How is accountability linked from the agency level down to the individual IT specialist?**
   b. **And are these employees assessed and rewarded by metrics or parameters in their performance appraisals?**
   c. **What types of positive and negative incentives are used for employees within agencies to promote a secure computing environment?**

Answer: We encourage agencies to incorporate PMA scorecard results into performance appraisals for those who are responsible for implementing the associated policies. Through the performance appraisal process, agencies are able to associate positive and negative incentives to results. As mentioned above, accountability is established through the Senior Executive Service performance measures, and information security is a critical skills area covered under the Human Capital Scorecard. As a critical skills area, agencies are required to show how accountability for performance cascades through the appraisals for all relevant employees. We encourage agencies to clearly articulate expectations and consequences in agencywide policies, such as the agency's "Rules of Behavior" documentation.

Also, for PMA scorecard agencies, the Deputy Secretary or President's Management Council member is held accountable for performance in all PMA scorecard initiative areas. In turn, the agency CIO is held accountable for performance on the E-Government scorecard. Since the scorecard process is incorporated into performance appraisals, and the process is transparent (with both positive and negative results made public), agency scorecard leads have increased accountability and incentive to improve performance.

4.) **There's a famous saying that goes, "If you aren't keeping score, you're just practicing." I get the sense that maybe that might be our situation right now. You've stated in your written testimonies that there is room for improvement when measuring whether an agency is effectively securing its systems. For instance, Mr. Wilshusen stated that OMB's performance metrics for measuring agencies' implementation of information security control activities often do not address the quality or effectiveness of control processes.**
   a. **Why do you think GAO feels OMB's current metrics don't measure the quality and effectiveness?**
   b. **And can you provide examples of measures that would measure the quality or effectives of control processes?**

Answer: We use evaluations conducted by Agency Inspectors General (IGs) to provide an annual independent assessment of key agency information security and privacy processes. We focus on three key processes: Certification and Accreditation (C&A), Plan of Actions and Milestones (POA&M), and Privacy Impact Assessments (PIA). We selected these three processes, since they encompass the selection and testing of security controls, the remediation of weaknesses, and the determination of a system's potential impact on privacy. We feel that these 3 processes holistically encompass an agency's security and privacy activities.

GAO recommends for OMB to request expansion upon the IGs' assessment of C&A processes through the annual FISMA reporting process, to specifically include the quality and effectiveness of security controls. We are willing to work with GAO to develop additional measures which would reach beyond process measures to address information security outcomes.

5.) In any organization, information security is extremely important. In order for it to be recognized as such, there needs to be senior executive level buy-in. Without it, no employee will pay much attention to it. I was wondering;

a. Do you feel agencies have senior executive involvement and if so, are they held accountable for the results of their FISMA reports?

b. How are these individuals held accountable and do you feel this is effective?

c. **Is there more that we can do?**

Answer: In February 2003, the Administration released the "National Strategy to Secure Cyberspace." We have been working hard to implement this strategy, which embraces FISMA as a guiding principle. In addition, agencies have had increasingly more Executive level attention and accountability in the area of information security and privacy implementation since FISMA was passed in 2002. First of all, agency annual FISMA reports are sent to the Director of OMB by the head of each agency. Under statute, the agency head is ultimately responsible for the security of the Agency's systems. Secondly, we encourage agencies to incorporate PMA scorecard results into employee performance appraisals for those who are responsible for implementing associated policies. When quarterly PMA scorecard results are not adequate, the OMB Management team will follow-up with the appropriate senior level executive at the agency. Thirdly, OMB evaluation of agency budget requests is tied to successful implementation of security and privacy requirements. Failure to address security and privacy results in agency investments being placed on OMB's management watch list, with possible restriction of additional development funds for that investment.

6.) **Ms Evans, you stated in your testimony the progress OMB and agencies have made in implementing the Federal Desktop Core Configuration, or "FDCC." The FDCC seems like it is critical to cost-effectively increasing security and I commend you for the progress made this past year. I understand that both agencies and vendors, which agencies purchase their products from, agree with the purpose of the FDCC. However, it is my understanding that there appears to be continuing challenges, particularly with respect to the current policy. Specifically, I have been told there may be insufficient guidance to facilitate compliance by vendors.**

   a. **What is the status of that process, and when are you expecting to provide further guidance to agencies and application providers to facilitate compliance?**

Answer: Agencies were required to submit Federal Desktop Core Configuration (FDCC) compliance reports to NIST by March 31, 2008. To assist Scorecard agencies with submitting the technical information in the required Security Content Automation Protocol (SCAP) validated format, OMB secured SCAP validated FDCC Scanner software for each Scorecard agency. NIST is reviewing the information and will provide their initial analysis soon.

OMB and NIST continue to work with agencies and vendors to establish the final FDCC settings. NIST is administering public comments for proposed settings changes with the first public comment period open from April 1 to April 30, 2008. Comments will be reviewed and posted for a second comment period, from May 1 until May 31, 2008; final review will occur and an updated FDCC will be posted mid-June 2008. We welcome your participation and comments at http://nvd.nist.gov/fdcc/fdcc-updates.cfm

OMB is also working with GSA to identify an independent assessor to develop a policy utilization methodology/tool to help agencies evaluate their adoption of the FDCC.

7.) **Further, consistent with the adoption of the FDCC for Federal "desktops," I have heard that there may be a standardized configuration for "servers" at a future date.**

   a. **Are there any lessons that we can learn from implementing a common configuration across desktops and apply to an "FDCC" for servers?**
   b. **What plans does OMB have to put in place procedures to ensure that all affected parties in both the public and private sector have the ability to comment prior to the development of such a policy, and to actively provide feedback during implementation?**

OMB is specifically focusing on the desktops right now. Many agencies are also working on the standardized configuration for "servers." When these efforts are successful, I believe the agencies will step forward just as the Department of Defense did with the FDCC. The FDCC has been an example of how OMB, NIST, agencies and private industry can work together to develop baseline security configurations.

One of the key lessons learned is that agencies can and do benefit from demonstrated successes of other agencies. The United States Air Force led the way with the successful implementation of its "Gold Standard" core configuration. USAF had worked closely with Microsoft on its baseline implementation and this provided a solid foundation to develop the Federal Desktop Core Configuration (FDCC).

Every agency has the responsibility for its IT security, however sharing best practices, knowledge, standards, policies etc. will enable the agency to act more effectively and efficiently in an ever changing environment.

It is important to note that NIST is not the first or only configuration standard. NIST is currently working with a number of IT vendors on standardizing security settings for a wide variety of IT products and environments through its Security Configuration Checklists Program for IT Products. The NIST process for creating, vetting, and making security checklists available for public use is documented in "NIST SP 800-70 - Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developers."

Given the overwhelming number of Federal Agency desktops using Windows XP, and the significant potential for agencies to up-grade to Vista operating system, OMB wanted to manage the risk for the Federal government as a whole and issued memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems." M-07-11 is an important component of the Government's overall IT security activities.

Agencies and vendors are using resources at http://fdcc.nist.gov/ to help them adopt the FDCC. These resources include group policy objects, virtual hard disks, frequently asked questions, public comments, and a detailed description of the configurations. The frequently asked questions are updated frequently to address a number of topics, including several policy items.

Questions and Responses for the Record
for Mr. Wilshusen

United States Government Accountability Office
Washington, DC 20548

April 24, 2008

The Honorable Thomas R. Carper
Chairman, Subcommittee on Federal Financial Management, Government Information, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: Review of FISMA and Related Guidance

This letter responds to your request that I answer additional questions arising from the March 12, 2008, hearing on the status of federal information security held by the Subcommittee on Federal Financial Management, Government Information, and International Security. In that hearing, we discussed the state of information security at federal agencies. Your questions, along with our responses, follow.

Question 1: In your review of the recommendations presented by the Cyber Security Industry Alliance witness to the subcommittee, do you agree with or disagree with the recommendations and which recommendations would you modify?

GAO response to Question 1: Following are the eight recommendations made by Mr. Bennett in his March 12, 2008, testimony and our assessment of each recommendation.

> **Recommendation 1:** *Align responsibilities and authorities to vest the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) with specific power over information security. The current authority of Agency CIOs to ensure should become the power to enforce cost effective measures of security. This must be accomplished by the CIOs of the organization's different units supporting the department-wide CIO.*
>
> **GAO Response:** We agree that sustained high-level leadership is needed to set the right tone at the top in order to achieve effective information security, and believe that existing Federal Information Security Management Act of 2002 (FISMA) provisions describe a structure to achieve this goal. Under FISMA, agency heads are responsible for providing information security protections for information collected or maintained by or on behalf of the agency and information systems used or operated by an agency or by a contractor. FISMA provides for the agency head to delegate authority to the CIO to ensure compliance with FISMA

and the CIO designates a CISO to carry out the CIO's responsibilities. As such, FISMA provides a mechanism for the agency head to vest authority to enforce information security to the CIO. For example, in response to a July 2006 GAO survey, 17 of 22 major federal agencies reported that their CIO had the authority to enforce compliance with the agency's information security program. However, we have not studied the extent to which implementation of this authority structure varies by agencies, or the advantages and disadvantages of one agency's structure over another's. In addition, attempts have been made to strengthen the CIO's authority to enforce FISMA requirements, as with H.R. 4791, introduced in the current Congress and amended by the House Oversight and Government Reform Committee.

Recommendation 2: *Require improvements to assessment, continuous monitoring, and remediation in order to develop a comprehensive approach to information systems security.*

GAO Response: We agree that opportunities exist for agencies to improve implementation of the existing governmentwide framework for periodic testing and monitoring of information security control effectiveness and remediation of known vulnerabilities. The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have established a baseline for a risk-based framework of policies, standards, and guidelines to assist agencies in the performance of the periodic—but no less than annually—assessment and monitoring of control effectiveness and weakness remediation activities required by FISMA.

FISMA requires that agency information security programs include the testing and evaluation of the effectiveness of information security policies, procedures, and practices, and that such tests be performed with a frequency depending on risk, but no less than annually and include a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency. Periodic testing and evaluation of information security controls is a critical element for ensuring that controls are properly designed, operating effectively, and achieving control objectives. As we have previously reported, clarifying or strengthening federal policies and requirements for testing and evaluating security controls according to risk could help agencies better assess the effectiveness of the controls protecting the information and systems supporting their programs, operations, and assets.

Recommendation 3: *Mandate preparation of a complete inventory of all federal agency IT assets by a certain date.*

GAO Response: Since its enactment in 2002, FISMA has required agencies to produce an annually updated inventory of major information systems (including major national security systems) operated by the agency or under its control,

which includes an identification of the interfaces between each system and all other systems or networks, including those not operated by or under the control of the agency. However, as we have previously reported, not all agencies have yet developed a complete inventory. According to OMB, its Information Systems Security Line of Business initiative identified security services and tools requested by agencies, including vulnerability assessment, network mapping and discovery, and baseline configuration management tools. These tools are intended to help agencies develop an accurate inventory of information resources managed at their agency.

Recommendation 4: *Improve performance measurement and provide incentives to agencies that give information security a high priority.*

GAO Response: We agree that opportunity exists for OMB to improve its process for performance measurement. In previous reports, we have recommended that OMB improve FISMA reporting by clarifying reporting instructions and requesting IGs to report on the quality of additional performance metrics. The current metrics do not measure how effectively agencies are performing various activities. Current performance measures offer limited assurance of the quality of agency processes that implement key security policies, controls, and practices. For example, agencies are required to test and evaluate the effectiveness of the controls over their systems at least once a year and to report on the number of systems undergoing such tests. However, there is no measure of the quality or effectiveness of agencies' test and evaluation processes. Similarly, OMB's reporting instructions do not address the quality of other activities such as risk categorization, security awareness training, intrusion detection and prevention, or incident reporting. Providing information on the effectiveness of security controls and on the quality of the security-related processes used to implement key control activities would further enhance the usefulness of the annually reported data for management and oversight purposes.

Further, we have previously reported that OMB's reporting guidance and performance measures did not include complete reporting on certain key FISMA-related activities. For example, FISMA requires each agency to include policies and procedures in its security program that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. OMB's current reporting instructions only request that IGs comment on whether or not they considered patching as part of their agency's certification and accreditation rating but nothing more. As a result, OMB and Congress lack information that could identify governmentwide issues regarding patch management. This information could prove useful in demonstrating whether or not agencies are taking appropriate steps for protecting their systems.

We cannot render an opinion regarding agency incentives because we have not examined the advantages or disadvantages associated with incentives. However, efforts have been made to ensure that information security remains a high priority. For example, since 1997, we have identified information security as a

governmentwide high-risk issue in each of our biennial reports to Congress.[1] Further, congressional oversight such as the recent hearings in February and March, efforts by OMB through the budget process, the President's Management Agenda Scorecard, and other mechanisms, such as corrective action plans and performance measures, have all contributed to increasing agency management's attention to information security.

Recommendation 5: *Institutionalize security within federal agency culture.*

GAO Response: As we described in our response to Recommendation 1, we agree that opportunities exist for agencies to improve information security and move toward institutionalizing security within federal agency cultures. FISMA provides for a top-down approach to implementing an agencywide information security program, addressing roles and responsibilities of the agency head, senior program officials, the CIO, and the CISO. It also assigns information security responsibilities to OMB, federal agencies, IGs, and NIST. Inherent in each role is the responsibility to promote adequate security practices within the organization.

In addition, to facilitate implementation of common practices and promote awareness, OMB and certain federal agencies have continued or launched several governmentwide initiatives that may enhance information security at federal agencies and foster institutionalized practices. Several of these key initiatives are discussed below.

- *The Information Systems Security Line of Business*: The goal of this initiative is to improve the level of information systems' security across government agencies and reduce costs by sharing common processes and functions for managing information systems' security. Several agencies have been designated as service providers for IT security awareness training and FISMA reporting.
- *Federal Desktop Core Configuration*: This initiative directs agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations developed by NIST and the Departments of Defense and Homeland Security. The goal of this initiative is to improve information security and reduce overall information technology operating costs.
- *SmartBUY*: This program, led by the General Services Administration, is to support enterprise-level software management through the aggregate buying of commercial software governmentwide in an effort to achieve cost savings through volume discounts. The SmartBUY initiative was expanded to include commercial off-the-shelf encryption software and to permit all federal agencies to participate in the program. The initiative is to also include licenses for information assurance.
- *Trusted Internet Connections Initiative*: This is an effort designed to optimize individual agency network services into a common solution for the federal

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

government. The initiative will facilitate the reduction of external connections, including Internet points of presence, to a target of fifty, and, according to DHS, it will more efficiently manage and implement security measures to help bring more comprehensive protections across the federal ".gov" domains.

Further, to promote the sharing of information security practices across the federal government, the creation of a CISO Council could facilitate increased implementation of security practices across agencies. This would be similar to the CIO Council, which serves as the principal interagency forum for improving practices in the design, modernization, use, sharing, and performance of federal government agency information resources.

Recommendation 6: *Codify the OMB guidance regarding notification of individuals whose sensitive personal information held by government agencies has been compromised.*

GAO Response: We agree that the opportunity exists to codify OMB policy regarding breach notification practices. Congress has already enacted legislation requiring protection of personally identifiable information that are agency-specific or that target a specific type of information. For example, the Veterans Benefits, Health Care, and Information Technology Act, enacted in December 2006, establishes information technology security requirements for personally identifiable information that apply specifically to the VA. The act mandates, among other things, that VA develop procedures for detecting, immediately reporting, and responding to security incidents; notify Congress of any significant data breaches involving personally identifiable information; and, if necessary, provide credit protection services to those individuals whose personally identifiable information has been compromised. Attempts have been made to ensure that all agencies consistently develop and implement breach notification policies governing how and under what circumstances affected parties are notified in case of a security breach. For example, pending legislation, H.R. 4791, requires that federal agencies notify individuals in a timely manner whose personally identifiable information may have been compromised or accessed during an information security breach, consistent with policies and procedures issued by OMB.

Recommendation 7: *Increase federal agency IT security funding.*

GAO Response: We have not studied the relative advantages and disadvantages associated with varying levels of security funding and cannot render an opinion on this recommendation. However, OMB has integrated IT security and privacy into the capital planning and investment control process to promote greater attention to security and privacy as fundamental management priorities. To guide agency resource decisions and assist OMB oversight, OMB Circular A-11, *Preparation, Submission and Execution of the Budget*, requires agencies to: (1) report security costs for all IT investments; (2) document adequate security controls and costs have been incorporated into the life cycle planning of each

investment; and (3) tie plan of action and milestones for a system directly to the funding request for the system. This information requested by OMB could help determine whether agencies' IT security funding needs are adequate.

Recommendation 8: *Reaffirm objective assessments of commercially available information technologies.*

GAO Response: FISMA requires that agencies assess the risks to systems and information, and implementing NIST guidance specifies that in so doing agencies should consider the use of emerging technologies in their strategy to mitigate emerging security threats. In addition, a stated purpose of FISMA is to acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector. Another stated purpose of FISMA is to recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products. Finally, FISMA requires NIST to evaluate commercially available information technologies to assess potential application by agencies to strengthen information security.

Question 2: You stated that there were opportunities to make FISMA more "clear" for agencies in complying with the law and security their information systems. (a) Can you tell the Subcommittee what parts of the law are unclear from an agency or inspectors' general perspective, and (b) do you have any recommendations for making FISMA more clear in its intent and implementation?

GAO response to Question 2: As we have previously reported, we believe that an opportunity exists to clarify the requirements in FISMA for agency security test and evaluation processes and independent IG evaluations.[2]

Clarify requirements for testing and evaluating security controls. Agencies are required to test and evaluate the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually, and that includes testing of management, operational, and technical controls. However, as we previously reported, federal agencies had not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. Clarifying or strengthening federal policies and requirements for determining the frequency, depth, and breadth of security control tests and evaluations could help agencies better assess the effectiveness of the controls protecting the information and systems supporting their programs, operations, and assets.

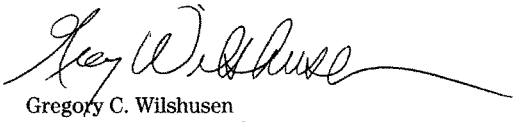
---

[2]GAO, *Information Security: Progress Reported, but Weaknesses at Federal Agencies Persist*, GAO-08-571T (Washington, D.C.: March 12, 2008).

Consider conducting FISMA-mandated annual independent evaluations in accordance with audit standards or a common approach and framework. As we previously reported, we found that the IGs lacked a common methodology, or framework, which culminated in disparities in type of work conducted, scope, methodology, and content of the IGs' annual independent evaluations. These inconsistencies could hamper the efforts of the collective IG community to perform their evaluations with optimal effectiveness and efficiency. Conducting the evaluations in accordance with generally accepted government auditing standards and/or a robust commonly used framework or methodology could provide improved effectiveness, increased efficiency, quality control, and consistency in assessing whether the agency has an effective information security program. IGs may be able to use the framework and methodology to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather sufficient, competent evidence efficiently. Having a documented methodology may also offer quality control by providing a standardized methodology, which can help the IG community obtain consistency of application.

In responding to these questions, we relied on previous audit work we preformed in developing prior reports and testimonies regarding federal agency implementation of the Federal Information Security Management Act. If you have any questions regarding this letter, please contact me at (202) 512-6244 or wilshuseng@gao.gov.

Sincerely yours,



Gregory C. Wilshusen
Director, Information Security Issues

[311009]

Questions and Responses for the Record for Mr. Howard

The Honorable Thomas R. Carper
Chairman
Federal Financial Management, Government Information, Federal Services, and International Security Subcommittee
Senate Homeland Security and Government Reform Committee

March 12, 2008

Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information

Question 1: Mr. Bennett's written testimony provided a number of recommendations concerning many of the topics that we have discussed today and some that we have not. I would ask that you evaluate each recommendation and tell the subcommittee which ones you agree with, which ones you would modify, and which ones you disagree with. Also, if you could, provide us a short explanation of why you chose what you did.

Mr Bennett's, President, Cyber Security Industry Alliance, Recommendations:

Response: The Department of Veterans Affairs (VA) has evaluated each of Mr. Bennett's recommendations and is providing our comments. It should be noted that while Mr. Bennett's recommendations are made on a government-wide basis, VA is responding only on behalf of the VA.

R commendation 1: *Align responsibilities and authorities to vest the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) with specific power over information security. The current authority of Agency CIOs to ensure should become the power to enforce cost effective measures of security. This must be accomplished by the CIOs of the organization's different units supporting the department-wide CIO.*

- *To effectively establish and maintain a comprehensive information security program for federal agencies, CIOs and CISOs need the enforcement authority, budget authority and personnel resources to carry out this essential mission. Funding needs to be allocated to those organizations and facilities that require the most support.*
- *The senior management of organizations that do not actively support the information security efforts must be held accountable for the failure of the organization to meet its FISMA responsibilities. Accountability at the individual level, not just agency level, is critical to obtaining improved security.*

R sponse: VA generally agrees with this recommendation as it applies to VA. In a large agency like VA, enforcement of security measures throughout the agency is not the sole responsibility of the CIO or CISO. Management and enforcement of security are everyone's responsibility at VA, requiring the support of executive managers, system administrators, and all users. A key element of the program is the clear assignment of responsibilities in all phases of the system life cycle. Another critical factor in successful security implementation is that information technology (IT) security

is a mandatory line item in VA's budget, which allows for more effective management and planning by giving the CIO control over security resource allocations.

Recommendation 2: *Require improvements to assessment, continuous monitoring, and remediation in order to develop a comprehensive approach to information systems security.*

- *Agencies need to implement strategies for security monitoring that assesses the health and resiliency of information systems on a regular, continuous basis.*
- *Although NIST issued base-line control updates in December 2006, additional emphasis on evaluation consistency for cyber security readiness among agencies is needed. This is complicated by differences in background and expertise at the Agency Inspector General level, and by staffing and budget short-falls in some IG offices.*
- *Congress should codify CIO/CISO responsibility and authority for testing and continuous monitoring as needed, but more than once a year.*

Response: VA agrees with this recommendation as it relates to VA. Last year, VA implemented a rigorous program of continuous monitoring testing. Testing is being completed this year via complete certification and accreditation (C&A) security controls assessment (SCA) testing for all operational IT systems in VA. In the out-years, systems not undergoing complete C&A SCA testing will conduct continuous monitoring testing on controls selected by the CISO. Also, VA now has an Office of Oversight and Compliance that reviews systems routinely – at least annually – and provides feedback on technical, managerial, and operational security controls. While continuous monitoring is necessary, codification of this concept is not required at this time. NIST is in the process of bolstering its guidance to address this how agencies should approach continuous monitoring and risk mitigation at the enterprise level. Upon finalization, its guidance will help VA implement more comprehensive continuous monitoring.

Recommendation 3: *Mandate preparation of a complete inventory of all federal agency IT assets by a certain date.*

- *The federal government is responsible for a massive amount of information technology assets that is expanded and maintained by a substantial IT budget. Those assets are located within the U.S. and abroad, within government owned buildings and leased buildings, in the homes of telecommuters and others, and can be stationary and mobile. It is a complicated task to complete a comprehensive inventory, but you can't protect what you don't know about even though an enemy might know about it. Control systems have been added to NIST guidance, but this needs to be incorporated into the law. Although this is presently a requirement, implementation of a complete inventory has yet to be achieved and must be made a priority.*

Response: VA agrees with the statement 'implementation of a complete inventory is needed for VA, however, a complete inventory is already required under FISMA. VA has already begun a wall-to-wall inventory and conducted a sensitive data inventory.

Recommendation 4: *Improve performance measurement and provide incentives to agencies that give information security a high priority.*

- *OMB should establish metrics and leading indictors on an annual basis that address agency performance on a 12 to 24 month timeframe. This would provide Agencies with some lead time to identify resources and implement controls to achieve some measure of performance with the identified metrics. Using a security maturity model such as NIST's Program Review for Information Security Management Assistance (PRISMA) would also accomplish the same objectives.*

- *The large federal agencies and departments are viewed monolithically from the outside. Organizations such as the Departments of Energy, the Interior, or Treasury are viewed as a single organization predicated on the assumption the CIOs have management control over the policies, procedures, and implementation requirements of FISMA. In reality, the operating units must each tailor the requirements and institutionalize good security practices within their organizations. Performance must be measured and collected at both the operating unit and the Agency level.*

- *With the many competing priorities federal agencies face to deliver mission success in a cost-constrained environment, cyber security is seldom a high priority. Agencies need to be incentivized to provide information security high visibility and a high priority. Incentives could address a broad range of rewards from public acknowledgement to additional funding or personnel bonuses.*

Response: VA agrees that performance measurement needs to be more effective, and metrics addressing VA's performance need to be established 12 to 24 months prior to using such metrics. An organization as large as VA cannot respond to changes in metrics without enough advanced notice to implement them throughout the entire infrastructure. We also agree that program review for information security management assistance (PRISMA) is a step in the right direction, but should not be the sole basis for evaluation of an IT security program as large and complex as the VA program. Instead, we suggest the use of a core set of performance metrics and a PRISMA type tool that accounts for differences between the VA IT security program, and that of other agencies with different business needs and risks associated with its mission. It should be noted that NIST is no longer conducting PRISMA reviews of other agencies. However, they have published a report on PRISMA and how agencies can conduct a review, and how the review results can be used. See http://csrc.nist.gov/groups/sma/prisma.

Recommendation 5: *Institutionalize security within federal agency culture.*

- *Training at all levels and functional responsibilities is critical to the success of agencies' information security program.*
- *OMB should establish a CISO Council to meet regularly and report to Congress on the effectiveness of sharing best practices, group purchases of automated tools and training courses, and development of a more effective common curriculum for training.*

Response: VA agrees with the need to provide both security awareness training and specialized security training for VA. Currently, general awareness training is provided to all system users. Specialized training is provided for IT staff and project managers. The training program is being expanded to include specialized security training for other job categories.

Recommendation 6: *Codify the OMB guideline regarding notification of individuals whose sensitive personal information held by government agencies has been compromised.*

- *Given the growing number of incidents where sensitive personal information held by government agencies has been compromised, agencies should be required to notify individuals of data security breaches involving sensitive personal information that pose a risk of identity theft or other harm to the individual. The policies and processes outlined in OMB's May 22, 2007 Guidance titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" should serve as the basis for language in legislation.*
- *Data breaches of information systems maintained by contractors or other sources working on federal projects should be promptly notified to the Secretary and CIO of the contracting agency. OMB's Fiscal Year 2007 Report to Congress on Implementation of FISMA (released on March 1, 2008) found a decreasing number of federal agencies could confirm that their agency ensures information systems used or operated by a contractor of the agency or other organization on behalf of the agency meets the requirements of FISMA, OMB policy, or NIST guidelines.*

Response: VA has an extensive program for data breach notification, as our Federal Information Security Management Assessment (FISMA) 2007 Report indicates. VA notifies the United States computer emergency readiness team (US Cert) when security incidents occur.

Recommendation 7: *Increase Federal Agency IT Security Funding.*

- *President Bush's proposed budget for fiscal 2009 includes $7.3 billion for cyber security efforts -- a 9.8 percent increase from last year. We urge Congress to meet and even exceed these proposed spending levels and help direct it to where it is most needed. In order to meet any new and enhanced FISMA requirements, agencies will continue to need sustained and increased IT security funding. Given the national security at stake, federal agencies should receive additional information security funds in FY2009 to manage the Administration's Trusted Internet Connections initiative and other priorities tied to the new Cyber Initiative. Federal agencies should not be expected to meet these requirements with current funding levels.*

Response: VA agrees that increase security funding is required for VA, which is why the FY 2009 Budget for VA includes $92.6 m for cyber security efforts. With those funds, VA will implement two major initiatives: the data security-assessment and strengthening of controls (DS-ASC) program and the personal identity verification (PIV) and identity and access management program. These programs will help us achieve the "Gold Standard" for data security to include: data encryption, IT equipment accountability, training and education, proactive inspection of compliance, promulgation of policies and procedures, data and information storage procedures and accessibility.

Recommendation 8: *Reaffirm objective assessments of commercially available information technologies.*

- *Given that new Internet technologies have the potential to dramatically enhance government performance at a substantially lower cost, FISMA should affirm that government agencies conduct an objective assessment of their security and not fall behind the curve by limiting their procurement options because preconceived compliance concerns prevent efforts to achieve greater efficiencies, better service, and improved security.*

R sponse: VA agrees with this recommendation. VA has established a group that conducts assessments of new technologies, and integrates these technologies into VA's approved procurement process.

Question 2: In the past year, the Administration has implemented a lot of initiatives to help secure our sensitive information and reduce costs. One of these initiatives is called the Information Systems Security Line of Business. I understand that this initiative will standardize information security education and reporting government-wide.

a. How is your agency taking advantage of these Lines of Business?
b. And do you think there are more opportunities for your agency, or others, to take advantage or improve these initiatives?
c. In addition, do you think there may be more ways we can standardize information security practices to reduce costs and increase security?

Response: VA believes that standardized information security practices are an effective way to reduce costs and ensure security for the VA. VA participates in the annual security awareness training lines of business activities through our learning management system, which is an enterprise-level software application designed to enable an organization to plan, deliver, and manage all learning events across the organization.

Throughout the VA, we use an automated tool with the Federal Information Security Management Act (FISMA) reporting system, which integrates the results of FISMA reporting into a risk assessment product to generate return on investment data, and estimate the costs to implement certain Health Insurance Portability and Accountability Act (HIPAA) security controls.

At this time, VA does not see opportunities for additional participation, as we already have security solutions that accomplish the same activities. These solutions are embedded in VA systems and infrastructure making transition to lines of business solutions impractical at this time. As a result, the CIO submitted a waiver to Office of Management and Budget (OMB) stating that VA could not participate in the security awareness training and FISMA reporting lines of business offerings..

Question 3: Also, I understand that there are some new cyber security initiatives that have deadlines soon or were recently supposed to be completed such as the Federal Desktop Core Configuration, Trusted Internet Connection, transition to LPv6, etcetera.

a. How are your specific agencies coping with these transitions?
b. And do you have comprehensive plans in place to be fully compliant with these initiatives when 0MB has asked?
c. Is your agency struggling with complying with any of these initiatives?
d. If so, what needs to happen before you are compliant with these transitions?

Response: VA is aggressively working to meet the deliverables of the Trusted Internet Connection (TIC) initiative, in order to identify and consolidate the existing external connections within our enterprise. Our plan is to have the connections migrated into the

Network Security Operations Center (NSOC) managed internet gateways by July 30, 2008. , NSOC is developing a plan to provide the necessary justification to OMB on the desired number of TICAPs and what VA needs to do in order to comply with the Statement of Capability (SOC) requirements.

Question 4: Ensuring appropriate executive level buy-in is critical to any mission critical area, especially information security. In your own agencies, have the roles of Chief Information Officers and Chief Information Security Officers been elevated to an effective level in the organization to put in place effective information security policies and procedures and enforce security?

a. In your opinion, what is an effective level of authority to place our CIOs and CISO's within a federal agency of your size and mission?

Response: Obtaining appropriate executive level buy-in is critical to ensuring that IT not only has a seat, but a voice at the executive table. At VA, we believe that the roles of CIO and CISO have been elevated to critical levels in the organization to put in place effective information security policies, procedures and enforcement. The CIO at VA is an Assistant Secretary, which means that the CIO is a "peer" with the other Assistant Secretaries in Human Resources, General Counsel, Finance and the other essential functional areas that support our mission. Also, because of the recent centralization of the Office of Information & Technology (OIT), it provides the IT department even greater leverage and efficiency in developing and implementing information security policies and procedures. A critical element of the centralization of OIT is the fact the OIT now manages the budget and money for all IT assets, allowing us to better manage the acquisition, development and execution of IT. In our opinion, the VA CIO and CISO are currently at effective levels of authority for an agency the size of VA to achieve our mission of serving the veteran.

Questions for the Record

The Honorable Norm Coleman
Senate Homeland Security & Government Reform Committee

March 12, 2008

Agencies in Peril: Are we Doing Enough to Protect Federal IT and Secure Sensitive Information

Question 1: A growing band of civilian units inside China is writing malicious code and training to launch cyber strikes into enemy systems. As for many of these units, the first enemy is the Department of Defense, the Department of Homeland Security and our nations' law enforcement agencies. Pentagon officials say there are more than three million daily scans of the Global Information Grid, the Defense Department's main network artery, and that the U.S. and China are the top two originating countries. I was disturbed by the March 7, 2008, CNN article entitled, *Chinese hackers: No site is safe,* which provided disconcerting insights into the People's Liberation Army's efforts to penetrate the Pentagon's IT network and other sensitive U.S. Government computer networks vowing that and I quote, "No Web site is one hundred percent safe". Right now China and more than 20 other nations possess dedicated cyber warfare computer attack programs – and that number doesn't include terrorist organizations. Can you please elaborate for me on exactly what your agency is pro-actively doing to prepare for the cyber warfare threat? Are you doing anything beyond the OMB memorandums to pro-actively address this challenge?

Response: The Department of Veterans Affairs (VA) network security operations center (NSOC) serves as the VA's security operations element. The NSOC manages, protects, and monitors the cyber security posture of the Department, coordinates externally with government incident response centers, performs threat and vulnerability analyses, reports cyber security vulnerabilities, develops concept of operations or guidelines relating to cyber security incidents, performs analyses of cyber security events, maintains detailed logs and databases of VA cyber security incidents and responses, and generally performs the full range of functions across the spectrum of activities relating to incident management and response, vulnerability scanning, event correlation and analysis, audit log analysis, patch distribution, and remediation planning. The spectrum of activities typically encompasses detection, pre-emption, prevention, reaction, response, and recovery.

Question 2: Some of the more notable breaches to personal identifying information maintained by the government have occurred away from the agency, usually while an employee is on travel or at home. Additionally, laptop computers are frequently used to conduct government business while traveling. Many of these computers contain sensitive agency or personal information. Thefts of laptops are very common, not to get the information but to get the device. What efforts have been taken through regulatory or policy guidance to limit the number of employees who have outside access to sensitive

sensitive information or to limit how much sensitive information they can have access to at a time? What efforts have been taken to make these computer system more secure, such as through the use of a boot-up password or token, or encryption of the data? Are there any requirements regarding the strength of the passwords or encryption used?

Response: To thoroughly protect VA sensitive information both in transmission and at rest (in storage), VA has developed VA Directive 6500 and VA Handbook 6500, which outline specific requirements for data encryption and protection of sensitive VA information. Moreover, each employee is required to sign a *Rules of Behavior* document that describes exactly how VA sensitive information is to be handled.

The technical solution to protecting VA sensitive data is VA's information protection project. The overarching goal of the information protection project is to safeguard VA information, ensuring the confidentiality, availability and integrity of information in transmission and at rest. The information protection project is an expansion of the device encryption project, and will address security of all VA information assets. In addition to employing encryption as a technical solution, the Department will be focusing on containing information and restricting access to information.

The information protection project is a collaborative effort among various components of the Office of Information and Technology to engineer and deploy technical controls, and to establish corresponding policy, procedures and guidance.

The encryption of over 15,000 laptops in September 2006 initiated the enterprise-wide effort to protect information. Since then, VA has established a two prong approach to deploying technology to ensure information is protected; 1.) to identify and leverage technologies that currently exist within the Department that will contribute to the Departments effort to protect information, and 2.) to develop a comprehensive strategy that will augment the existing technical solutions.

The comprehensive strategy entails identifying and codifying the Departmental requirements for all information that must be protected; this includes information that is stored and transmitted, both internally and externally. The purpose of gathering the requirements is to acquire solutions to rectify any vulnerability that exist where information resides or traverses the network.

In-Progress Information Protection Initiatives

- Laptop Encryption
- Enterprise Tape/Back-Up Encryption
- Secure File Transfer Protocol/Transmission Control Protocol
- Removable Storage Media Encryption (e.g., Universal serial bus (USB) thumb drives, external hard drives, compact discs)
- Port Security
- Mobile Device Encryption (e.g., Blackberry, smart phones, personal digital assistants)
- File/Document Security and Encryption
- Email Security and Encryption
- Remote Access Security

Questions for the Record Submitted to
Chief Information Officer Susan Swart by
Senator Thomas R. Carper (#1)
Senate Committee on Homeland Security,
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
March 12, 2008

Question:

Mr. Bennett's written testimony provided a number of recommendations concerning many of the topics that we have discussed today and some that we have not. I would ask that you evaluate each recommendation and tell the subcommittee which ones you agree with, which ones you would modify, and which ones you disagree with. Also, if you could, provide us a short explanation of why you chose what you did.

Answer:

Chief Information Officer and Chief Information Security Officer Recommendation

Partially Agree. The Department of State holds individuals responsible and accountable for failure to comply with information security requirements. The Department's Cyber Security Incident Program (CSIP) enhances the protection of Department of State's cyber infrastructure by identifying, evaluating, and assigning responsibility for breaches of cyber security. The CSIP focuses on accountability of personnel for actions leading to damage or risk to Department automated information systems and infrastructure, even when only unclassified material or information is involved. Valid cyber security incidents have the potential of resulting in disciplinary and personnel ramifications. Accordingly, while the recommendation may be of benefit to agencies lacking CIO and CISO

enforcement authority, the Department of State has already instituted such authorities of its own.

Improvements to Assessment and Continuous Monitoring Recommendation

Agree. The Department of State supports the addition of metrics that account for an agency's ability to detect, respond to and react to cyber security threats and manage vulnerabilities. For example, the Department's security services includes continuous network monitoring, technical countermeasures, counter intelligence services, threat analysis, and physical and technical security programs that should be measured on a continuous and quantifiable manner. If an agency's effectiveness in implementing FISMA were instead measured by the aforementioned continuous monitoring efforts, the Department of State and other similarly situated agencies would be better recognized. Prior GAO reports in April 2005 and June 2007 have likewise identified the lack of reporting on incident response metrics as a shortcoming in the FISMA evaluation process.

Preparation of Complete Inventory of All Federal Agency IT Assets by a Certain Date

Disagree. While a complete IT asset inventory is a worthwhile endeavor for an agency, the wide ranging characteristics of assets serving the agency community and the emphasis on a "date certain" inventory completion date is both unrealistic and impractical. As an example, the Department of State operates at over 300 posts world-wide as compared to other agencies that have only a domestic regional presence. The requirement is also unnecessary given the Chief Information Officer's associated

information resource management responsibilities pursuant to the Paperwork Reduction Act.

Improve Performance Measurement and Provide Incentives Recommendation

Agree. Some uncertainty exists whether the assignment of an annual FISMA grade will continue. The positive acknowledgment of an "A+" on an agency's annual FISMA grade fostered a type of competition between many in the agency community to be recognized as the leader in information security. Congress may wish to consider other incentives including limiting the scope of the annual OIG FISMA evaluation for higher performing federal agencies when measured against specific, federal-wide criteria.

Institutionalize Security Within Federal Agency Culture Recommendation

Agree. A Joint Department of State and USAID collaborative effort, known as JSAS, was selected by OMB as only one of three agencies to serve as a Shared Service Center for information security awareness training. The Department's annual awareness course requires all users to review applicable information security requirements and test one's understanding with evaluated answers to True/False questions. The Department of State's efforts enhance a thorough level of understanding and awareness by all Department employees and contractors. Furthermore, the Department's Foreign Affairs Manual codifies applicable information security requirements from a management, technical and operational level. Accordingly, the Department of State institutionalizes security at all levels and functional responsibilities.

Codify OMB Guideline Regarding Notification of PII Breach Recommendation

Agree. A codification of the applicable OMB guidelines would promote certainty by eliminating the potential for inconsistent interpretations across the agency community and formalize OMB's non-mandatory guidance.

Increase Federal Agency IT Security Funding Recommendation

The administration provides the Department of State with the appropriate level of resources and funding necessary to meet its requirements and mission. The Department of State also supports the OMB mandate that all programs assume security as a budgeted item with the overall cost of any particular initiative, rather than borrowing from unrelated information technology aspects of the federal budget.

Reaffirm Objective Assessments of Commercially Available IT Recommendation

Agree. The recommendation states that agencies should "conduct an objective assessment of their security and not fall behind the curve by their limiting their procurement options." The Department of State currently employs Security Assurance Services and Innovation (SASI) contract vehicle that competes every task among as many as seven highly pre-qualified vendors. SASI's overall objective is to provide for a safe and secure IT environment efficiently, effectively, and economically. Additionally, eight specific objectives were identified to potential contractors seeking to provide services under the comprehensive SASI umbrella:

- Provide innovative security and assurance services, under a performance-based arrangement, with maximum benefits to the agency's ability to perform its mission at a lower cost.
- Provide confidentiality, integrity and availability of information through an innovative and secure environment for the conduct of agency business and operations.
- Protect information and information technology resources from actual and potential security threats and sources.
- Anticipate and respond to challenges that threaten the confidentiality, integrity and availability of the agency's information.
- Conduct the management and implementation of security operations and information assurance programs in a way that complies with all applicable federal laws and regulations and customer agency(cies) policies, standards, processes, and procedures while maximizing benefit/cost ratios.

  Focus on performance and improve both quantitatively and qualitatively the value of security and assurance program and technology investments to the taxpayer and customer agencies over the life of the Blanket Purchase Agreement.
- Evaluate emerging technologies on a continuous basis and provide "forward thinking" and innovative recommendations to senior leadership.
- Utilize small, small disadvantage, women-owned, veteran-owned, Historically Underutilized Business Zone (HUBzone) and service-disable veteran businesses in a way that provides these businesses the maximum practicable opportunity to participate in the performance of federal contracts.

Questions for the Record Submitted to
Chief Information Officer Susan Swart by
Senator Thomas R. Carper (#2)
Senate Committee on Homeland Security,
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
March 12, 2008

Question:

In the past year, the Administration has implemented a lot of initiatives to help secure our sensitive information and reduce costs. One of these initiatives is called the Information Systems Security Line of Business. I understand that this initiative will standardize information security education and reporting government-wide.

a. How is your agency taking advantage of these Lines of Business?
b. And do you think there are more opportunities for your agency, or others, to take advantage or improve these initiatives?
c. In addition, do you think there may be more ways we can standardize information security practices to reduce costs and increase security?

Answer:

(a) The Department has been an ardent supporter of the federally-focused Information System Security Line of Business. From the onset, the Department dedicated staff and resources to the initial working group responsible for identifying the aspects of information security that would most readily lend themselves to a Shared Services model. A Shared Services model is where one agency is responsible for providing service to another agency. At the development stage, key Department of State personnel assisted by drafting requisite documents to ensure the most appropriate agency would be selected to serve as a Shared Service Center. During the selection stage, a Joint Department of State and USAID

collaborative effort, known as JSAS, was selected by OMB as only one of three agencies to serve as a Shared Service Center for information security awareness training. Presently, the Department of State and USAID information security awareness training solution is providing service to four other agencies totaling over 40,000 government employees and contractors in addition to their own employees and contractors. The Department of State continues to provide support to the Information Systems Security Line of Business through participation on half a dozen working groups.

(b) Yes. The Information System Security Line of Business benefits from active participation of officials from throughout the federal government. The federal government's executive agencies represent the entire spectrum of possibilities and complexities. From the micro agencies to the cabinet level agencies, from the agencies operating in one region of the United States to the agencies with an international charter, the information security issues remain constant. In order to adequately address the numerous instantiations and possibilities associated with this environment, the Information System Security Line of Business should continually strive to ensure participation is representative of the rich diversity of the agency community in all substantive discussions and decisions.

(c) One of the options to standardization of information security practices is through addressing the issues identified by the GAO with respect to FISMA implementation. Specifically, GAO reports in April 2005, July 2005, and June 2007 have all identified the lack of a common Inspector General reporting framework as a deficiency of the FISMA evaluation

process. In the GAO's own words, the "lack of a common methodology, or framework, has culminated in disparities in audit scope, methodology, and content. As a result, the collective IG community may be performing their evaluations without optimal effectiveness and efficiency." FISMA implementation could be improved through an agreement amongst IGs upon a common evaluation framework.

Questions for the Record Submitted to
Chief Information Officer Susan Swart by
Senator Thomas R. Carper (#3)
Senate Committee on Homeland Security,
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
March 12, 2008

Question:

Also, I understand that there are some new cyber security initiatives that have deadlines soon or were recently supposed to be completed such as the Federal Desktop Core Configuration, Trusted Internet Connection, transition to IPv6, etc.

a. How are your specific agencies coping with these transitions?

b. And do you have comprehensive plans in place to be fully compliant with these initiatives when OMB has asked?

c. Is your agency struggling with complying with any of these initiatives?

d. If so, what needs to happen before you are compliant with these transitions?

Answer:

(a) The Department of State is making all practical efforts to meet the requirements associated with the Federal Desktop Core Configuration, Trusted Internet Connection, and transition to IPv6.

(b) The Department has provided to OMB all of the requisite plans and other supporting documentation relating to the relevant initiatives on a timely basis.

(c) No, the Department is not struggling to meet these initiatives because of a sound and proven existing infrastructure that is being employed to implement them. The Department employs a strategic, layered approach to comprehensive risk management of our information and information assets. This security strategy, which we call "Defense in Depth,"

provides the Department multiple levels of defense and protection through a matrix of operational, technical, and managerial security controls. We focus on identifying and mitigating emerging threats because of our vast overseas exposure. Implementation and compliance with the relevant initiatives requires the Department to allocate the appropriate level of resources, while ensuring continued compliance with pre-existing requirements. Subject matter experts from the Department's Information Security Steering Committee are charged with tackling the complexities and subtleties many of the initiatives pose. In addition, the forum provides a high-level opportunity to ensure that the principles of sound information security management are instilled upon all Department employees as they fulfill their roles, regardless of geographic location. Accordingly, the Department is utilizing these processes to ensure timely and complete compliance of the aforementioned initiatives.

(d) No response necessary.

Questions for the Record Submitted to
Chief Information Officer Susan Swart by
Senator Thomas R. Carper (#4)
Senate Committee on Homeland Security,
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
March 12, 2008

Question:

Ensuring appropriate executive level buy-in is critical to any mission critical area, especially information security. In your own agencies, have the roles of Chief Information Officers and Chief Information Security Officers been elevated to an effective level in the organization to put in place effective information security policies and procedures and enforce security?

a) In your opinion, what is an effective level of authority to place our CIOs and CISO's within a federal agency of your size and mission?

Answer:

At the Department of State, the Chief Information Officer holds the title of an Assistant Secretary reporting directly to the Under Secretary for Management. At the Department of State, the Chief Information Security Officer holds the title of Deputy Chief Information Officer reporting to the Chief Information Officer. More important than their respective levels or titles, the effectiveness of both the Chief Information Officer and Chief Information Security Officer is driven largely by the visibility among all Department officials from the key decision makers to the system users. The Department's Information Security Steering Committee co-chaired by the Chief Information Security Officer Information utilizes Integrated Information Security Teams composed of subject matter experts from the different segments of the Department – policy specialists, operators, and

managers. The Integrated Information Security Teams are responsible for facilitating and coordinating Department-wide information security efforts, including the annual "90 Day Push" initiatives to improve security. The 90 Day Push initiatives are Department efforts on a quarterly timeframe that concentrate and leverage key resources to address previously identified deficiencies. Another example was the establishment of a team charged with developing a Department Information Security Program Plan. The Plan identifies the relevant laws, regulations, and policies; delineates responsibilities; describes the governance mechanism: and, catalogues the elements of the Department's operational, defense-in-depth cyber security strategy. While the Plan was fully approved by the members of the Information Security Steering Committee, it was done with the understanding that the Plan is a living document responding to changes in technology and the threat environment.

Questions for the Record Submitted to
Chief Information Officer Susan Swart by
Senator Norm Coleman (#1)
Senate Committee on Homeland Security,
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
March 12, 2008

Question:

At the end of February, Senator Collins and I sent a letter to 24 federal agencies highlighting the findings of the GAO on Protecting Sensitive Agency Information. We also requested a timeline in writing for when each agency expected to be in compliance with all the OMB Memoranda focused on protecting Personally Identifiable Information.

In your testimony you discussed how your agencies were complying with pieces of OMB Memoranda on protecting PII (see list below). Are your agencies fully compliant with all the OMB recommendations on protecting PII issued before the start of this year?

Date:	*Report*	*Title*
02/11/2005	*M-05-08*	*Designation of Senior Agency Officials for Privacy*
05/22/2006	*M-06-15*	*Safeguarding Personally Identifiable Information*
06/23/2006	*M-06-16*	*Protection of Sensitive Agency Information*
07/12/2006	*M-06-19*	*Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*
07/17/2006	*M-06-20*	*FY2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*
05/22/2007	*M-07-16*	*Safeguarding Against and Responding to the Breach of Personally Identifiable Information*

Answer:

The Department continues its commitment to comply with Privacy Act provisions, protecting the rights of American citizens and aliens admitted for permanent residence and safeguarding personal information regardless of physical format. More than a decade ago the Assistant Secretary for Administration was designated the Department's Senior Official for Privacy. More recently, the Department formed the Privacy Protection

Governance Board to heighten awareness and ensure the protection of personally identifiable information in all aspects of the Department's programs and activities. The Board brings together Assistant Secretaries from throughout the Department to address the interdependencies among the security, technology, and business aspects requisite to minimizing and reducing the collection, use, and dissemination of personal information -- and especially Social Security Numbers -- and to safeguarding this sensitive information in all its physical formats, particularly in today's dynamic electronic environment. The Department's accomplishments include the development of a Breach Notification Policy; Core Response Group procedures; reduction and elimination of the use or dissemination of Social Security Numbers; communication through websites, collectives, worldwide cables, and Department Notices; awareness building for the business owners of personal information; review of business practices and process; and enhanced attention to Privacy Impact Assessments in the Certification and Accreditation Process as reported in FISMA. While we have made considerable progress, we recognize that more work needs to be done to protect personal information within the Department.

Question:

If not, do you have a timeline for when you will be fully compliant? Do you know when your agencies will be sending us the status and timeline in writing for reaching compliance with all the OMB recommendations?

Answer:

The Department of State notified OMB it will meet the requirements of OMB memorandum 07-16 by December 2008.

Question:

Would you say that it is a high priority for all your agencies to be in compliance with the OMB memoranda on Personally Identifiable Information?

Answer:

The Department of State considers the OMB memoranda related to Personally Identifiable Information a high priority. Accordingly, the Department established an Assistant Secretary level board charged with addressing the requirements associated with the OMB memoranda and more generally, ensuring the protection of personally identifiable information in all aspects of the Department's programs and activities.

Question:

Is there anything Congress can do to help your agencies comply with the OMB guidance? Is it a matter of funding or is additional legislation needed?

Answer:

The Department of State supports the congressional oversight role as defined in FISMA and other applicable information security authorities. Congressional and Office of Inspector General oversight provides agencies with an objective and independent review of agency actions that are then utilized to enhance the agency-wide information security program.

Questions for the Record Submitted to
Chief Information Officer Susan Swart by
Senator Norm Coleman (#2)
Senate Committee on Homeland Security,
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
March 12, 2008

Question:

A growing band of civilian units inside China is writing malicious code and training to launch cyber strikes into enemy systems. As for many of these units, the first enemy is the Department of Defense, the Department of Homeland Security and our nations' law enforcement agencies. Pentagon officials say there are more than three million daily scans of the Global Information Grid, the Defense Department's main network artery, and that the U.S. and China are the top two originating countries. I was disturbed by the March 7, 2008, CNN article entitled, *Chinese hackers: No site is safe*, which provided disconcerting insights into the People's Liberation Army's efforts to penetrate the Pentagon's IT network and other sensitive U.S. Government computer networks vowing that and I quote, "No Web site is one hundred percent safe".

Right now China and more than 20 other nations possess dedicated cyber warfare computer attack programs – and that number doesn't include terrorist organizations. Can you please elaborate for me on exactly what your agency is pro-actively doing to prepare for the cyber warfare threat? Are you doing anything beyond the OMB memorandums to pro-actively address this challenge?

Answer:

Classified response provided via secure means.

Questions for the Record Submitted to
Chief Information Officer Susan Swart by
Senator Norm Coleman (#3)
Senate Committee on Homeland Security,
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
March 12, 2008

Question:

In 2006, media reports detailed a series of attacks perpetrated by hackers operating through Chinese Internet servers against our computer systems at the Departments of Commerce and State. Hackers were able to penetrate Federal systems and use "rootkits" – a form of software that allows hackers to mask their presence – to send information back out of our systems.

What have you learned from that attack? Do you know what information was relayed from the system at the Department of State? Have you determined how long these "root kits" were in place and what pre-cautions have you take since their discovery to ensure that the Department of State's computer system will not be compromised in the future?

Answer:

Classified response provided via secure means.

Questions for the Record Submitted to
Chief Information Officer Susan Swart by
Senator Norm Coleman (#4)
Senate Committee on Homeland Security,
Subcommittee on Federal Financial Management, Government Information, Federal Services and International Security
March 12, 2008

Question:

Some of the more notable breaches to personal identifying information maintained by the government have occurred away from the agency, usually while an employee is on travel or at home. Additionally, laptop computers are frequently used to conduct government business while traveling. Many of these computers contain sensitive agency or personal information. Thefts of laptops are very common, not to get the information but to get the device.

What efforts have been taken through regulatory or policy guidance to limit the number of employees who have outside access to sensitive information or to limit how much sensitive information they can have access to at a time?

Answer:

Prior to any user having access to a Department information system and subsequently on an annual basis, the user is responsible for undertaking a comprehensive information security awareness course. At the conclusion of the awareness course the user is tested on their level of understanding of the content. Failure to take the awareness course on a timely basis results in disconnection from the network. In the regards to policy, the Department of State has issued a number of Department Notices and cables outlining its policies concerning how employees are to access sensitive information. Several notices and cables were also issued specific to the handling of personally identifiable information. Authorized remote access to the Department systems may only be achieved through a two-factor authentication system that combines a hand-held random generating password device and a separate password authenticated by the Department's network. The Department's remote access solution also utilizes a "time-out" function requiring user re-authentication after 15 minutes of

inactivity, a standard exceeding the OMB requirement. Lastly, Department initiatives are currently underway to identify and reduce the use of Social Security Numbers in Department forms and information requests.

Question:

What efforts have been taken to make these computer system more secure, such as through the use of a boot-up password or token, or encryption of the data? Are there any requirements regarding the strength of the passwords or encryption used?

Answer:

The Department of State employs numerous means to ensure its computer systems are secure. The Department is compliant with the 12 character password requirement associated Federal Desktop Core Configuration requirements. Currently, the only means for a Department user to remotely access the Department's unclassified network is through a two-factor authentication system that combines a hand-held random generating password device and a separate password authenticated by the Department's network. The Department's remote access solution also utilizes a "time-out" function requiring user re-authentication after 15 minutes of inactivity, a standard exceeding the requirement. With regards to encryption, the Department is currently in the process of encrypting all of its mobile computing devices. The Department leveraged its PKI contract to provide encryption protection at no additional cost to the Department. The solution is fully compliant with applicable NIST standards and guidelines (FIPS 140-2). The Department has issued numerous Department notices and cables advising Department computer users of their responsibilities and appropriate rules of behavior with respect to securing their information and information systems.

Post-Hearing Questions for the Record
Submitted to Darren Ash
From Senator Norm Coleman

"Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?"
March 12, 2008

QUESTION 1: At the end of February, Senator Collins and I sent a letter to 24 federal agencies highlighting the findings of the GAO on Protecting Sensitive Agency Information. We also requested a timeline in writing for when the agency expected to be in compliance with all the OMB Memoranda focused on protecting Personally Identifiable Information.

(A) In your testimony you discussed how your agencies were complying with pieces of OMB Memoranda on protecting PII (see list below). Are your agencies fully compliant with all the OMB recommendations on protecting PII issued before the start of this year?

ANSWER

See the status of individual recommendations below

Date:	*Report*	*Title*
02/11/2005	***M-05-08***	***Designation of Senior Agency Officials for Privacy***

Status: Fully Compliant

The NRC designated the Deputy Chief Information Officer as the Senior Agency Official for Privacy in an email sent to the Office of Management and Budget (OMB) on March 18, 2005.

05/22/2006	***M-06-15***	***Safeguarding Personally Identifiable Information***

Status: Partially Compliant

The NRC reminded its employees and contractors of their specific responsibilities for safeguarding PII in a June 22, 2006 agency-wide announcement entitled "Safeguarding Personal Privacy Information." The NRC also reviewed its policies and processes and made appropriate modifications aimed at preventing misuse of, or unauthorized access to, PII. On October 6, 2006, in NRC's FY 2006 FISMA Report, which included the Privacy Management Report, the NRC notified the Director, OMB, that NRC had completed a review of NRC's physical and personnel security, and administrative and technical policies and processes related to the prevention of the intentional or negligent misuse of, or unauthorized access to, PII.

Although NRC has been reporting security incidents according to OMB memoranda M-06-15, NRC does not have a formal written policy that requires this reporting. NRC has drafted a new incident response policy that will be issued in the 3rd quarter of FY 2008 that will implement the OMB recommendation.

Date:	Report	Title
06/23/2006	***M-06-16***	***Protection of Sensitive Agency Information***

Status: Partially Compliant

In response to M-06-16, on September 19, 2006, the NRC issued its policy entitled "Protection of Personally Identifiable Information," that:

- Prohibits the removal of electronic PII from NRC-controlled space until all PII on mobile computers or devices is encrypted
- Prohibits staff from storing PII pertaining to NRC official business on personally-owned hard drives, removable media, and other stand-alone storage devices
- Prohibits staff from using personally-owned computers for processing or storing PII of individuals pertaining to NRC official business other than themselves
- Prohibits staff from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted
- Restricts remote access to PII information on NRC systems by requiring two-factor authentication and enforcing a 30-minute timeout
- Prohibits emailing of PII outside of NRC's infrastructure except where necessary to conduct agency business
- Requires identification of extracts or outputs that contain PII and deletion of those not necessary as well as logging and assessment of retention for future extracts/outputs.

This policy implements the NIST checklist for protection of PII that is either accessed remotely or physically transported outside of the NRC's secured, physical perimeter. This policy also implements the other recommendations contained in M-06-16 for protection of PII.

NRC adopted an additional policy on February 7, 2008 to further protect sensitive information. This policy prohibits employees from processing sensitive information on home personal computers unless the employee is using NRC's CITRIX Broadband Remote Access System. Employees are also prohibited from storing sensitive information on a home computer. Employees may process sensitive information at home on an NRC-issued laptop that is encrypted using NRC-approved encryption software.

Although NRC currently implements 30-minute or less timeouts for remote access sessions and mobile device access, NRC has not issued a formal written policy addressing this issue. The NRC will issue a written timeout policy in the 3rd quarter of FY 2008.

NRC is currently examining methods to enable encryption of sensitive information transmitted outside of NRC's infrastructure prior to transmission and decryption by the recipient to ensure adequate protection of sensitive information transmissions. NRC will develop a policy and implementation timeline after completion of the technology examination. The technology examination will be complete in the 3rd quarter of FY 2009.

NRC is developing a written policy requiring encryption of NRC sensitive information removed from NRC facilities and expects to implement this policy in the 1st quarter of FY 2009.

NRC is developing a written policy requiring logging all computer-readable data extracts from databases holding sensitive information and erasure of the information within 90 days or

documentation of the need to retain the data extract for a longer period of time. The policy is expected to be issued in the 4th quarter of FY 2008; however, full implementation will be delayed until October 2011 to enable implementation of technological aids to assist in complying with this requirement.

New systems that provide for remote access to information with a sensitivity of "high," such as the National Source Tracking System, are being deployed requiring that the user have an NRC issued digital certificate on a separate hard token to gain access to the system.

NRC is scheduled to fully implement HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, for physical access to NRC facilities in October 2010. Logical access to NRC systems and sensitive information will be incorporated into the identity cards by October 2011. Accordingly, NRC plans to require all remote access to NRC sensitive information employing two-factor authentication where one of the factors is a device separate from the computer gaining access by October 2011.

Date:	Report	Title
07/12/2006	***M-06-19***	***Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments***

Status: Partially Compliant

NRC has drafted a new incident response policy that will be issued in the 3rd quarter of FY 2008, which will codify our current practice and require the reporting of incidents (either electronic or physical form) involving PII to US-CERT within one hour of discovering the incident, regardless of whether or not the breach is suspected or confirmed.

NRC currently requires identification of security and privacy requirements as part of NRC's Capital Planning and Investment Control (CPIC) process. NRC will issue a written policy addressing this process in the 3rd quarter of FY 2008.

NRC is ensuring that operational systems meet applicable security requirements for security significant isolated or widespread weaknesses identified by the agency Inspector General or the Government Accountability Office. NRC will issue a written policy on these issues in the 3rd quarter of FY 2008.

Date:	Report	Title
07/17/2006	***M-06-20***	***FY2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management***

Status: Fully Compliant

The NRC's submission of the NRC FY 2006 annual FISMA report included this information with the exception of scorecard information. The NRC is not a scorecard agency and does not provide quarterly scorecard updates.

Date:	Report	Title
05/22/2007	***M-07-16***	***Safeguarding Against and Responding to the Breach of Personally Identifiable Information***

Status: Fully Compliant

The NRC issued on September 19, 2007, "U.S. Nuclear Regulatory Commission Personally Identifiable Information Breach Notification Policy," and the "U.S. Nuclear Regulatory Commission Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers." NRC employees were notified of these policies via an agency wide announcement on that date. These policies are publicly available on the NRC's Web site at: http://www.nrc.gov/site-help/privacy.html#ssn.

(B) If not, do you have a timeline for when you will be fully compliant? Do you know when your agencies will be sending us the status and timeline in writing for reaching compliance with all the OMB recommendations?

ANSWER

The status and timeline for reaching compliance with all referenced OMB recommendations is included in the preceding paragraphs. NRC is prepared to update you on the status of its implementation plans at any time.

(C) Would you say that it is a high priority for all your agencies to be in compliance with the OMB memoranda on Personally Identifiable Information?

ANSWER

Yes. Protection of personally identifiable information and compliance with the OMB memoranda are a high priority for the Nuclear Regulatory Commission. Prior to the Veterans Administration's loss of the computer containing the personally identifiable information of 26 million veterans, which brought the issue of personally identifiable information to the forefront of the federal government, the NRC had already begun efforts to identify and remove personally identifiable information from agency shared network drives, and now conducts annual searches of the shared drives for newly placed personally identifiable information. The issuance of the OMB memoranda on personally identifiable information reinforced to NRC the importance of protecting personally identifiable information. NRC placed a high priority on completing all initial recommendations and later the requirements of the OMB memoranda.

As reflected in the answers to other questions in this response, NRC has taken many actions to prevent the loss of personally identifiable information and to provide a framework for breach notification if a loss were to occur. Examples of NRC's high priority compliance with OMB requirements include prohibition on placing PII on any mobile information technology device that is not encrypted; prohibition on the use of personally identifiable information on home computers; and prohibition on the removal of paper copies of unredacted documents containing personally identifiable information from NRC-controlled space. Additionally, NRC diligently worked to develop its breach notification policy and its plan to eliminate the unnecessary collection and use of Social Security numbers and submitted them to OMB on time in compliance with OMB 07-16. The NRC plans to complete the plan's elements by November 2008.

(D) Is there anything Congress can do to help your agencies comply with the OMB guidance? Is it a matter of funding or is additional legislation needed?

ANSWER

Additional legislation does not appear to be necessary at this time to permit compliance with current OMB guidance. However, Congress can assist NRC by supporting proposed spending levels, which address known OMB requirements. Additionally, implementation of potential new or enhanced FISMA or OMB requirements will require increased IT security funding for which NRC will have to request funding once requirements are known and costs are quantified. Examples of this include implementation of the Administration's Trusted Internet Connections initiative and priorities tied to the new national Cyber Initiative. Also, because of the criticality of its mission, the NRC should receive sufficient funding in FY 2009 to support the regulation of cyber security programs of nuclear licensees.

QUESTION 2: A growing band of civilian units inside China is writing malicious code and training to launch cyber strikes into enemy systems. As for many of these units, the first enemy is the Department of Defense, the Department of Homeland Security and our nations' law enforcement agencies. Pentagon officials say there are more than three million daily scans of the Global Information Grid, the Defense Department's main network artery, and that the U.S. and China are the top two originating countries. I was disturbed by the March 7, 2008, CNN article entitled, *Chinese hackers: No site is safe,* which provided disconcerting insights into the People's Liberation Army's efforts to penetrate the Pentagon's IT network and other sensitive U.S. Government computer networks vowing that and I quote, "No Web site is one hundred percent safe."

(A) Right now China and more than 20 other nations possess dedicated cyber warfare computer attack programs – and that number doesn't include terrorist organizations. Can you please elaborate for me on exactly what your agency is pro-actively doing to prepare for the cyber warfare threat? Are you doing anything beyond the OMB memorandums to pro-actively address this challenge?

ANSWER

The NRC restricts a large volume of Internet traffic from China and other countries/sources at its perimeter firewalls. This is based on notifications received from U.S. Government sources such as US-CERT and IRS-CSIRT as well as other sources. In addition to blocking inbound and outbound traffic on the perimeter firewalls, the agency's proxy server restricts computer access to potentially malicious Internet web sites by using methods of category and domain name list filtering. The proxy server also restricts NRC computer access based on a site's content and is integrated with a security appliance that provides real-time scanning of active web content for malicious code. Other means of attack such as e-mail are blocked by multiple layers of Anti-Virus and Spam filtering to reduce scams and phishing that attempt to socially engineer users into loading malicious software or visiting sites that can load such software.

The NRC security team also monitors its firewall, proxy, intrusion detection system, and other system and security logs to detect security anomalies. Based on review of these logs,

additional IP and domain based restrictions are placed on the ingress and egress devices mentioned previously, such as the firewalls and proxy server. All of these actions have been taken apart from OMB mandated initiatives. However, NRC's compliance with the Trusted Internet Connection and Federal Desktop Core Configuration initiatives are part of its overarching strategy to address these types of threats.

QUESTION 3: Some of the more notable breaches to personal identifying information maintained by the government have occurred away from the agency, usually while an employee is on travel or at home. Additionally, laptop computers are frequently used to conduct government business while travelling. Many of these computers contain sensitive agency or personal information. Thefts of laptops are very common, not to get the information but to get the device.

(A) What efforts have been taken through regulatory or policy guidance to limit the number of employees who have outside access to sensitive information or to limit how much sensitive information they can have access to at a time?

ANSWER

The NRC reminded its employees and contractors of their specific responsibilities for safeguarding PII in a June 22, 2006 agency-wide announcement entitled "Safeguarding Personal Privacy Information." The NRC also reviewed its policies and processes and made appropriate modifications aimed at preventing misuse of, or unauthorized access to, PII. On October 6, 2006, in NRC's FY 2006 FISMA Report, which included the Privacy Management Report, the NRC notified the Director, OMB, that NRC had completed a review of NRC's physical and personnel security, and administrative and technical policies and processes related to the prevention of the intentional or negligent misuse of, or unauthorized access to PII.

In response to M-06-16, on September 19, 2006, the NRC issued its policy entitled "Protection of Personally Identifiable Information," that:

- Prohibits the removal of electronic PII from NRC-controlled space until all PII on mobile computers or devices is encrypted
- Prohibits staff from storing PII pertaining to NRC official business on personally-owned hard drives, removable media, and other stand-alone storage devices
- Prohibits staff from using personally-owned computers for processing or storing PII of individuals pertaining to NRC official business other than themselves
- Prohibits staff from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted
- Restricts remote access to PII information on NRC systems by requiring two-factor authentication and enforcing a 30-minute timeout
- Prohibits emailing of PII outside of NRC's infrastructure except where necessary to conduct agency business
- Requires identification of extracts or outputs that contain PII and deletion of those not necessary as well as logging and assessment of retention for future extracts/outputs.

NRC adopted an additional policy on February 7, 2008 to further protect sensitive information. This policy prohibits employees from processing sensitive information on home personal computers unless the employee is using NRC's CITRIX Broadband Remote Access System. Employees are also prohibited from storing sensitive information on a home computer. Employees may process sensitive information at home on an NRC-issued laptop that is encrypted using NRC-approved encryption software.

NRC is currently examining methods to enable encryption of sensitive information transmitted outside of NRC's infrastructure prior to transmission and decryption by the recipient to ensure adequate protection of sensitive information transmissions. NRC will develop a policy and implementation timeline after completion of the technology examination.

NRC is developing a written policy requiring encryption of all NRC sensitive information removed from NRC facilities and expects to implement this policy in the 1st quarter of FY 2009.

NRC is developing a written policy requiring logging all computer-readable data extracts from databases holding sensitive information and erasure of the information within 90 days or documentation of the need to retain the data extract for a longer period of time. The policy is expected to be issued in 4th quarter FY 2008; however, full implementation will be delayed until October 2011 to enable implementation of technological aids to assist in complying with this requirement.

New systems that provide for remote access to information with a sensitivity of "high," such as the National Source Tracking System, are being deployed requiring that the user have an NRC issued digital certificate on a separate hard token to gain access to the system.

(B) What efforts have been taken to make these computer systems more secure, such as through the use of a boot-up password or token, or encryption of the data? Are there any requirements regarding the strength of the passwords or encryption used?

ANSWER

On September 19, 2006, the NRC issued its policy entitled "Protection of Personally Identifiable Information," that addresses security of laptop computers among other topics. The policy:

- Prohibits the removal of electronic PII from NRC-controlled space until all PII on laptops is encrypted;
- Restricts remote access to PII information on NRC systems by means of a laptop or other mobile device by requiring two-factor authentication and enforcing a 30-minute inactivity timeout; and

Employees are permitted to process sensitive information outside of NRC on a government-issued laptop only if NRC-approved encryption software is used to protect data stored on the laptop.

NRC is currently examining methods to enable encryption of transmission of sensitive information outside of NRC's infrastructure prior to transmission and decryption by the recipient to ensure adequate protection of sensitive information while in motion. NRC will develop a policy and implementation timeline after completion of the technology evaluation. The technologies being assessed must meet FIPS 140-2 requirements.

Additionally, NRC has developed draft guidance documenting standard configuration requirements for laptop computers to include password composition and encryption standards, and is in the process of implementing the Federal Desktop Core Configuration for all laptops and desktops.

Post-Hearing Questions for the Record

Questions for the Record from Senator Thomas R. Carper

"Agencies in Peril: Are We Doing Enough to Protect IT and Secure Sensitive Information?"
March 12, 2008

QUESTION 1: Mr. Bennett's written testimony provided a number of recommendations concerning many of the topics that we have discussed today and some that we have not. I would ask that you evaluate each recommendation and tell the subcommittee which ones you agree with, which ones you would modify, and which ones you disagree with. Also, if you could, provide us a short explanation of why you chose what you did.

ANSWER

The NRC's response to each of Mr. Bennett's recommendations is contained in the enclosure.

QUESTION 2: In the past year, the Administration has implemented a lot of initiatives to help secure our sensitive information and reduce costs. One of these initiatives is called the Information Systems Security Line of Business. I understand that this initiative will standardize information security education and reporting government-wide.

(A) How is your agency taking advantage of these Lines of Business?

ANSWER

NRC has made use of the Information Systems Security Line of Business (ISS LOB) by purchasing and implementing the ASSERT tool offered by the Environmental Protection Agency for use in Federal Information Security Management Act (FISMA) reporting. NRC intends to use the tool to generate the Fiscal Year (FY) 2008 annual FISMA report. Additionally, NRC has made use of the security awareness course offered by the Department of Defense, and intends to make immediate use of it to meet FY 2008 security awareness requirements.

(B) And do you think there are more opportunities for your agency, or others, to take advantage or improve these initiatives?

ANSWER

Yes. NRC intends to evaluate future ISS LOB offerings for potential implementation to include SmartBuy products, Situational Awareness services, Tier II (Role Based Training) products, and Certification and Accreditation services.

(C) In addition, do you think there may be more ways we can standardize information security practices to reduce costs and increase security?

ANSWER

Yes. An additional opportunity for standardization that should be considered is a tool for development of security documentation that is consistent with National Institute of Standards and Technology (NIST) guidelines. Such a tool would fully integrate the development of security categorizations, system security plans, risk assessments, security tests and evaluations, and plans of action and milestones.

Also, standardization and cost efficiencies could be gained by encouraging agencies to identify and share best practices across the broad spectrum of FISMA compliance.

Finally, provision of a standardized solution to logging machine readable database extracts as required by Office of Management and Budget (OMB) Memo 06-16 could be very useful since little guidance has been provided to permit agencies to properly define the requirement.

QUESTION 3: Also, I understand that there are some new cyber security initiatives that have deadlines soon or were recently supposed to be completed such as the Federal Desktop Core Configuration (FDCC), Trusted Internet Connection (TIC), transition to IPv6, etcetera.

(A) How are your specific agencies coping with these transitions?

ANSWER

The NRC is coping with implementation of these initiatives within existing resource constraints. Compliance with these OMB mandates is being actively managed by the NRC Chief Information Officer (CIO). The NRC provides dedicated project management of each initiative that includes project planning, budgeting, oversight, and coordination. Implementation milestones have been established for each initiative and are integrated into overall plans for agency infrastructure modernization.

(B) And do you have comprehensive plans in place to be fully compliant with these initiatives when OMB has asked?

ANSWER

Yes. NRC has developed plans for complying with these OMB requirements. In the case of IPv6 implementation, NRC has complied with all OMB implementation milestones to date, and anticipates compliance with the near-term (June 30, 2008) target date. However, NRC is finding that target implementation dates may not be achievable for the FDCC and the TIC initiatives. For example, implementation of the FDCC will have a significant impact on application systems, and full implementation will be delayed until these applications can be individually modified to function with the FDCC. The NRC recent response to OMB regarding the TIC initiative advised OMB that the NRC is ready to comply with the initiative; however, the earliest the NRC would be compliant is approximately 120 days after a TIC portal service provider is able to receive agency orders.

(C) Is your agency struggling with complying with any of these initiatives?

ANSWER

Yes. As noted above, implementation of the FDCC is presenting a challenge because of impacts to custom applications. Testing of application with the new FDCC has shown that in some cases that functionality is adversely affected, thereby necessitating modification of the application. Such modifications are in many cases substantial and cannot be accomplished without additional resources. Implementation of the Trusted Internet Connection initiative has been hindered by the lack of clear and timely guidance from OMB and Department of Homeland Security (DHS), although we have received some guidance over the past few weeks. NRC has complied with all OMB IPv6 milestones, and has prepared its infrastructure for IPv6. However, IPv6 will not be fully implemented until an IPv6 business need is identified.

(D) If so, what needs to happen before you are compliant with these transitions?

ANSWER

Compliance with the Trusted Internet Connection initiative will require time to negotiate agreements with hosting service providers, and to develop processes to ensure internet access can be provided consistent with agency mission requirements. As noted above, additional time will be required to modify existing applications to function with the FDCC. Full transition to IPv6 will be dependent on the development of business demands for its use.

QUESTION 4: Ensuring appropriate executive level buy-in is critical to any mission critical area, especially information security. In your own agencies, have the roles of Chief Information Officers and Chief Information Security Officers been elevated to an effective level in the organization to put in place effective information security policies and procedures and enforce security?

(A) In your opinion, what is an effective level of authority to place our CIOs and CISO's within a federal agency of your size and mission?

ANSWER

The CIO should be a direct report to the head of the agency or the Chief Operating Officer, and the CISO should be a direct report to the CIO. The NRC CIO reports to the Executive Director of Operations, who is accountable directly to the Commission. The CISO directly reports to the CIO. This arrangement provides a very high degree of visibility for NRC's information security program, and provides sufficient means for enforcing IT security policies and procedures. This organizational placement has proven its effectiveness here at the NRC and is the optimal approach for any agency of this size (about 3,500 employees).

Enclosure

Mr. Timothy Bennett of the Cyber Security Industry Alliance (CSIA) offered the following recommendations in his submitted testimony for the record. The NRC evaluated each recommendation, and the response addresses which ones the agency agrees with, which ones should be modified, and which ones the agency disagrees with. A short explanation of rationale is also provided.

1. [Bennett] Align responsibilities and authorities to vest the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) with specific power over information security. The current authority of Agency CIOs to ensure should become the power to *enforce* cost effective measures of security. This must be accomplished by the CIOs of the organization's different units supporting the department-wide CIO.

   - [Bennett] To effectively establish and maintain a comprehensive information security program for federal agencies, CIOs and CISOs need the enforcement authority, budget authority and personnel resources to carry out this essential mission. Funding needs to be allocated to those organizations and facilities that require the most support.

     NRC Response: NRC concurs with this recommendation. Expanding the authority of the CIO and the CISO to enforce information security policy would lead to a significant improvement in the level of compliance with program requirements. Just as at most agencies, the NRC CIO and CISO do not currently have direct enforcement authority.

   - [Bennett] The senior management of organizations that do not actively support the information security efforts must be held accountable for the failure of the organization to meet its FISMA responsibilities. Accountability at the individual level, not just agency level, is critical to obtaining improved security.

     NRC Response: NRC concurs with this recommendation. Establishing accountability of individuals assigned roles and responsibilities for information security program implementation and maintenance is critical to the success of the program. NRC has taken action to include information security-related requirements performance measures into Senior Executive Service (SES) performance plans.

2. [Bennett] Require improvements to assessment, continuous monitoring, and remediation in order to develop a comprehensive approach to information systems security.

   - [Bennett] Agencies need to implement strategies for security monitoring that assesses the health and resiliency of information systems on a regular, *continuous* basis.

     NRC Response: NRC concurs with this recommendation. To date, NRC has focused its efforts on the certification and accreditation of information systems on a periodic basis. Plans for implementing continuous monitoring are now being developed to permit effective use of resources and automation to facilitate timely monitoring and maintenance of systems.

- [Bennett] Although NIST issued base-line control updates in December 2006, additional emphasis on evaluation consistency for cyber security readiness among agencies is needed. This is complicated by differences in background and expertise at the Agency Inspector General level, and by staffing and budget short-falls in some IG offices.

  NRC Response: The NRC concurs with this recommendation. Consistent use of assessment tools is needed. However, the tools used should measure effectiveness of controls, not simply documentation. Documentation of policies, procedures, configurations, etc. is very important, but effective implementation is more important.

- [Bennett] Congress should codify CIO/CISO responsibility and authority for testing and continuous monitoring as needed, but more than once a year.

  NRC Response: The NRC concurs with this recommendation. Annual self-assessment of security controls by system owners does not constitute adequate continuous monitoring. The intelligence community is currently providing an effective model for all systems with its classified systems, whereby system owners appropriately document, implement, and test IT security controls as part of certification and accreditation. After the initial certification and accreditation, a continuous monitoring process is employed to ensure the system remains secure.

3. [Bennett] Mandate preparation of a complete inventory of all federal agency IT assets by a certain date.

   - [Bennett] The federal government is responsible for a massive amount of information technology assets that is expanded and maintained by a substantial IT budget. Those assets are located within the U.S. and abroad, within government owned buildings and leased buildings, in the homes of telecommuters and others, and can be stationary and mobile. It is a complicated task to complete a comprehensive inventory, but you can't protect what you don't know about even though an enemy might know about it. Control systems have been added to NIST guidance, but this needs to be incorporated into the law. Although this is presently a requirement, implementation of a complete inventory has yet to be achieved and must be made a priority.

     NRC Response: NRC concurs with this recommendation. An inventory of information technology assets is essential to information security program success since one cannot protect that which one is not aware. The NRC has achieved a comprehensive inventory. The development of standardized definitions for various types of systems would be helpful in facilitating classification of items in the inventory (i.e., general support system, major application, minor application, standalone system, utility, etc.).

4. [Bennett] Improve performance measurement and provide incentives to agencies that give information security a high priority.

   - [Bennett] OMB should establish metrics and leading indictors on an annual basis that address agency performance on a 12 to 24 month timeframe. This would provide Agencies with some lead time to identify resources and implement controls to achieve some measure of performance with the identified metrics.

Using a security maturity model such as NIST's Program Review for Information Security Management Assistance (PRISMA) would also accomplish the same objectives.

NRC Response: The NRC concurs with this recommendation, particularly regarding provision of increased lead time. It is difficult for an agency to prove compliance without adequate preparation. However, it should be noted that PRISMA in large part measures what the annual FISMA report currently measures, and that is processes and documentation. Independent assessments that measure effectiveness, in addition to required documentation, are needed.

- [Bennett] The large federal agencies and departments are viewed monolithically from the outside. Organizations such as the Departments of Energy, the Interior, or Treasury are viewed as a single organization predicated on the assumption the CIOs have management control over the policies, procedures, and implementation requirements of FISMA. In reality, the operating units must each tailor the requirements and institutionalize good security practices within their organizations. Performance must be measured and collected at both the operating unit and the Agency level.

  NRC Response: As an agency having a single CIO, this recommendation has little practical impact on the NRC.

- [Bennett] With the many competing priorities federal agencies face to deliver mission success in a cost-constrained environment, cyber security is seldom a high priority. Agencies need to be incentivized to provide information security high visibility and a high priority. Incentives could address a broad range of rewards from public acknowledgement to additional funding or personnel bonuses.

  NRC Response: The NRC concurs with this recommendation. A broad range of incentives could result in the development and support of a positive security culture in the agency.

5. [Bennett] Institutionalize security within federal agency culture.

   - [Bennett] Training at all levels and functional responsibilities is critical to the success of agencies' information security program.

     NRC Response: NRC concurs with this recommendation. In order for individuals involved in making the information security program a success, they must be fully aware of what the program entails, their roles and responsibilities, threats to information assets. At the NRC, development and provision of training at all levels is currently underway.

   - [Bennett] OMB should establish a CISO Council to meet regularly and report to Congress on the effectiveness of sharing best practices, group purchases of automated tools and training courses, and development of a more effective common curriculum for training.

     NRC Response: NRC concurs with this recommendation, and considers a CISO Council as a means for sharing of best practices, and an effective forum for discussion of government-wide initiatives.

6. [Bennett] Codify the OMB guideline regarding notification of individuals whose sensitive personal information held by government agencies has been compromised.

   - [Bennett] Given the growing number of incidents where sensitive personal information held by government agencies has been compromised, agencies should be required to notify individuals of data security breaches involving sensitive personal information that pose a risk of identity theft or other harm to the individual. The policies and processes outlined in OMB's May 22, 2007 Guidance titled "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" should serve as the basis for language in legislation.

     NRC Response: The NRC concurs with this recommendation Customers, business partners, and employees of the government have a right to expect that their personal data is safeguarded from disclosure and have a corresponding right to be made aware of cases where the government has failed to do this. The NRC has developed and disseminated policies to its employees on breach notification.

   - [Bennett] Data breaches of information systems maintained by contractors or other sources working on federal projects should be promptly notified to the Secretary and CIO of the contracting agency. OMB's Fiscal Year 2007 Report to Congress on Implementation of FISMA (released on March 1, 2008) found a decreasing number of federal agencies could confirm that their agency ensures information systems used or operated by a contractor of the agency or other organization on behalf of the agency meets the requirements of FISMA, OMB policy, or NIST guidelines.

     NRC Response: NRC concurs with this recommendation. The Federal Acquisition Regulation should be revised to include specific contracting clauses for all government IT contracts. This would eliminate the need for each agency to develop and codify this guidance individually.

7. [Bennett] Increase Federal Agency IT Security Funding

   - [Bennett] President Bush's proposed budget for fiscal 2009 includes $7.3 billion for cyber security efforts -- a 9.8 percent increase from last year. We urge Congress to meet and even exceed these proposed spending levels and help direct it to where it is most needed. In order to meet any new and enhanced FISMA requirements, agencies will continue to need sustained and increased IT security funding. Given the national security at stake, federal agencies should receive additional information security funds in FY2009 to manage the Administration's Trusted Internet Connections initiative and other priorities tied to the new Cyber Initiative. Federal agencies should not be expected to meet these requirements with current funding levels.

     NRC Response: NRC concurs with this recommendation. Agencies have not yet been able to fully quantify the resource impact of the Trusted Internet Connections initiative and the national Cyber Initiative, and therefore resources to allow immediate implementation of related requirements should be readily available.

8. [Bennett] Reaffirm objective assessments of commercially available information technologies.

   - [Bennett] Given that new Internet technologies have the potential to dramatically enhance government performance at a substantially lower cost, FISMA should affirm that government agencies conduct an objective assessment of their security and not fall behind the curve by limiting their procurement options because preconceived compliance concerns prevent efforts to achieve greater efficiencies, better service, and improved security.

     NRC Response: The NRC concurs with this recommendation. The desire to achieve security compliance should not lead to a limitation on the employment of technologies that promise to enhance business delivery.

Questions for the Record to
USAID Chief Information Security Officer
Phil Heneghan by
Senator Norman Coleman (#1)
Senate Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
March 12, 2008

"Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?"

Question:

A growing band of civilian units inside China is writing malicious code and training to launch cyber strikes into enemy systems. As for many of these units, the first enemy is the Department of Defense, the Department of Homeland Security and our nations' law enforcement agencies. Pentagon officials say there are more than three million daily scans of the Global Information Grid, the Defense Department's main network artery, and that the U.S. and China are the top two originating countries. I was disturbed by the March 7, 2008, CNN article entitled, *Chinese hackers: No site is safe,* which provided disconcerting insights into the People's Liberation Army's efforts to penetrate the Pentagon's IT network and other sensitive U.S. Government computer networks vowing that and I quote, "No Web site is one hundred percent safe".

Right now China and more than 20 other nations possess dedicated cyber warfare computer attack programs – and that number doesn't include terrorist organizations. Can you please elaborate for me on exactly what your agency is pro-actively doing to prepare for the cyber warfare threat? Are you doing anything beyond the OMB memorandums to pro-actively address this challenge?

Answer:

While I do not want to comment on USAID's specific internal capabilities or technologies we are using, one of the most important aspects

of network monitoring and defense in the face of a cyber warfare threat is having comprehensive network visibility. Without that ability, it is difficult or impossible to detect, investigate, or respond to an attack. USAID has worked over the past several years to continually improve our network visibility, anomaly detection, and analytical capabilities to defend against a cyber attack. As a result, we feel that we are doing much more than the Office of Management and Budget (OMB) recommends in its memoranda. We are also leveraging external, government –wide relationships. For instance in 2006, USAID volunteered to participate in Department of Homeland Security's (DHS) Einstein pilot program. This program added another layer of defense by allowing review of our Internet traffic by individuals who have more immediate access to a broader amount of situational awareness information. DHS contacts us if they identify suspicious activity coming from USAID, augmenting our detection capabilities.

We are also active participants in the DHS-sponsored Government Forum of Incident Responders and Security Teams (GFIRST) that provides regular situational awareness information and opportunities to share best practices and collaborate. We regularly share intelligence gleaned from our investigations with US-CERT. This type of information sharing benefits all federal agencies and improves our ability to respond and work together in a crisis, such as a cyber warfare attack.

Questions for the Record to
USAID Chief Information Security Officer
Phil Heneghan by
Senator Norman Coleman (#2)
Senate Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
March 12, 2008

"Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?"

Question:

Some of the more notable breaches to personal identifying information maintained by the government have occurred away from the agency, usually while an employee is on travel or at home. Additionally, laptop computers are frequently used to conduct government business while traveling. Many of these computers contain sensitive agency or personal information. Thefts of laptops are very common, not to get the information but to get the device.

What efforts have been taken through regulatory or policy guidance to limit the number of employees who have outside access to sensitive information or to limit how much sensitive information they can have access to at a time?

Answer:

USAID implemented a global remote access technology in August of 2006, called Server-Based Computing (SBC), which allows users to securely access sensitive data remotely, without having to remove the data from the agency's security perimeter. Therefore, USAID users have the ability to conduct business from home or hotel rooms without needing to remove

personally identifiable information (PII) or other sensitive data. Remote users control a virtual desktop that resides logically inside the USAID network and receive only images of the activity occurring on the virtual desktop. This technology essentially turns the user's home computer or government-funded laptop into a dumb terminal that contains no agency data.

USAID government-funded laptops are for either internal or external use. A laptop designated as internal can only be connected to the agency network, and an external laptop can only be used outside the agency network. USAID policy prohibits removing PII from the internal network and storing it on external laptops. The agency's secure remote access solution, though, removes the need for users to take sensitive data from the internal network.

Question:

What efforts have been taken to make these computer system more secure, such as through the use of a boot-up password or token, or encryption of the data? Are there any requirements regarding the strength of the passwords or encryption used?

Answer:

USAID is working on a program to encrypt all laptops (both internal-only and external-only) to protect the data they contain, sensitive or not,

from unauthorized access. Encrypted laptops may have Sensitive But Unclassified (SBU) data on them but no PII. External laptop users gain access to agency data remotely using two-factor, token-based authentication and a web browser capable of supporting Federal Information Processing Standards- (FIPS)-compliant encryption, further reducing the risk of accidental loss of sensitive data. The USAID remote access technology, called Server-Based Computing (SBC), complies with the National Institute for Standards and Technology Special Publication 800-52 that defines the approved cryptographic cipher suites to transmit government SBU data across non-government networks. By deploying SBC, USAID has removed the need for users to store PII and other sensitive data on laptops. However, these laptops will also conform to the new security standards of the Federal Desktop Core Configuration (FDCC), one of which increases the minimum password length. The encryption that will be deployed on the laptops will comply with FIPS 140-2, "Security Requirements for Cryptographic Modules".

Questions for the Record to
USAID Chief Information Security Officer
Phil Heneghan by
Senator Thomas R. Carper (#1)
Senate Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
March 12, 2008

"Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?"

Question:

Mr. Bennett's written testimony provided a number of recommendations concerning many of the topics that we have discussed today and some that we have not. I would ask that you evaluate each recommendation and tell the subcommittee which ones you agree with, which ones you would modify, and which ones you disagree with. Also, if you could, provide us a short explanation of why you chose what you did.

Answer:

Although I generally agree that more weight should be given to the law, I disagree that it takes a change in the legislation to accomplish this. I believe that the Federal Information Security Management Act of 2002 (FISMA) provides the necessary framework for agencies to implement an effective information security program -- regardless of an agency's mission or size.

In its current form, FISMA maintains that an effective information security program is achievable if incorporated into the agency's business

decision-making process. I feel that one of the major shortcomings of FISMA is not with the law but rather a result of agencies viewing information security as a process unto itself instead of an integral part of conducting business. When this happens, agencies can easily fall into a compliance mode, merely trying to check boxes so they can return to their "real mission". When FISMA is the foundation of an information security program based on risk, the program becomes a component and stakeholder of the business, providing vital data that helps the business make appropriate decisions. By using the cyclical process of measuring, assessing, and reporting described in the law, agencies can create a culture of awareness that ultimately demands integrated risk metrics to operate successfully.

The metrics on the FISMA questionnaire shouldn't just measure whether an Agency completes specific actions; but how it completes those actions. For example, the training question on the Chief Information Officer (CIO) worksheet should not only ask how many people were trained, but also how they were trained as well. The Office of Management and Budget (OMB) should then ask the Inspector General to provide a qualitative assessment of the overall training process, including how it might be improved. Further, the questionnaire should also consider how agencies measure and manage other areas such as enterprise network vulnerabilities;

enterprise network exposure; inter-agency network intelligence sharing; and incident handling, verification, and reporting.

A major hurdle encountered by many agencies, and echoed in several of the hearing testimonies, is the lack of a standard measurement by which Inspectors General can assess and report on the quality of agency programs. Currently, agencies rightly believe that the Inspectors General (IG) reports submitted to OMB are uneven and can not truly be compared to one another. This perspective results from different agencies sizes, missions, and IG expertise. While each agency is unique in its mission, OMB could provide a standard attestation standard for the IG auditors to use to guide them in their evaluations. The agency IG could then formulate qualitative opinions on various aspects of the agency's program, thereby creating a system of checks and balances that prevents an agency from focusing on compliance and not risk.

FISMA currently covers all of the major components of a viable security program. The problems with the FISMA process seem to lie in how agencies view the law and implement its mandates rather than in the law itself. Fundamentally, the recommendations Mr. Bennett discussed in his eight points do not necessarily propose changes to FISMA itself but rather

describe potential refinements to the way agencies and OMB interact, these refinements are envisioned and allowed under the current law.

Specific comments to Mr. Bennett's recommendations follow:

Response to Recommendation #1:

Updating FISMA to grant an enforcement role of the CIO and Chief Information Security Officer (CISO) would have the opposite impact of the desired goal. FISMA mandates implementing a risk-based program and implies that the CIO and CISO support (or refute) security decisions by providing the business with accurate risk information. Therefore, the CIO and CISO are part of a deliberate and ongoing dialogue with agency business and system owners, not a "Thou shalt" approach. By codifying an enforcement role, FISMA would actually support and move toward a compliance-only model, working against the concept of appropriate risk-based security. The business owners need to be responsible for and engaged with the decisions and the trade-offs involved with running their business or program area.

Response to Recommendation #2

Effective security is an ever-evolving and never-ending pursuit; no agency will ever be "done" with security. Therefore, agencies should know that an effective information system security program is iterative and

requires continual improvements, assessments, ongoing monitoring, and risk mitigation activities. As technology changes, what we want to measure, and how frequently we want to measure it also changes, we don't want to have to change the law every time we change technology. The Office of Management and Budget and the National Institute for Standards and Technology (NIST) evaluate technology as it changes and update the technical standards as necessary. For instance, NIST Special Publication 800-40v2 "Creating a Patching and Vulnerability Management Program" already recommends continuous monitoring for vulnerabilities. When we define these types of recommendations in the law, the law itself will stagnate and become ineffective.

Response to Recommendation #3

FISMA requires an inventory of major systems and networks, termed General Support Systems (GSS). While this approach may appear to leave out a substantial number of IT assets at the device level, the law already provides the framework for device-level inventories that can be achieved without changing the law. For example, USAID performs continuous vulnerability scanning where each device on a USAID network may get scanned up to 10 times a month. This scanning ensures that we are measuring and monitoring the devices within all of our networks while

recording a device-level inventory at the same time. Modifying the law to mandate these inventories as a product, rather than as a by-product of a continuous business process, would only add another unwieldy and unhelpful task that would result in an inventory would have almost no value because it would be outdated.

Response to Recommendation #4

I support additional or improved performance measures from OMB, but the fact of the matter is that the law already allows for this. OMB changes what it measures every year, but could be more aggressive defining the things it wants measured. In addition, OMB could provide better auditing guidance to the agencies' Inspectors General through an audit attestation standard.

Regarding incentives, I am positive that FISMA would not have the visibility it has today if the House Committee on Oversight and Government Reform did not annually grade each agency's performance. From an incentive perspective, I feel this grading conveys the appropriate level of visibility to agency efforts and serves to appropriately motivate them.

Response to Recommendation #5

Without a doubt, better security training leads to a better security awareness, which leads to better security. Over the past four years, with the

help of the daily Tip of the Day security lesson, USAID network users have become more aware of the importance of and their responsibility for security. However, assigning responsibility is another powerful educator. USAID holds business owners responsible for their programs and systems (including their security). This ownership and responsibility drives the institutionalization of security awareness, from the top down. These business owners are senior agency executives, and they demand proper security practices from individuals in their chain of command.

Response to Recommendation #6

While not an unreasonable recommendation, OMB Memorandum M07-16 already requires each agency to have a defined breach notification process as well as a defined PII spillage incident response procedure. US-CERT has also provided a Personally Identifiable Information (PII) Spillage Incident Procedures document to federal agencies.

Response to Recommendation #7

I don't think any agency is going to argue with this recommendation.

Response to Recommendation #8

The federal government security needs are generally no different than companies in the private sector. As I mentioned in my comments during the hearing, USAID has deployed several technologies that are primarily used

within the banking industry. In fact, USAID was the first federal customer for many of these companies. I believe the cost benefit is clear. OMB also regularly performs assessments of commercial products to fill federal needs and makes them available through the GSA SmartBUY program.

Questions for the Record to
USAID Chief Information Security Officer
Phil Heneghan by
Senator Thomas R. Carper (#2)
Senate Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
March 12, 2008

"Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?"

Question:

In the past year, the Administration has implemented a lot of initiatives to help secure our sensitive information and reduce costs. One of these initiatives is called the Information Systems Security Line of Business. I understand that this initiative will standardize information security education and reporting government-wide.

How is your agency taking advantage of these Lines of Business?

Answer:

USAID, in a partnership with the Department of State, developed the Joint State/USAID Solution (JSAS) for security awareness training to deploy USAID's Tip of the Day program to other Federal agencies. USAID is also working with the Department of Justice to implement their Certification and Accreditation Line of Business tool CSAM.

Question:

And do you think there are more opportunities for your agency, or others, to take advantage or improve these initiatives?

Questions for the Record to
USAID Chief Information Security Officer
Phil Heneghan by
Senator Thomas R. Carper (#3)
Senate Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
March 12, 2008

"Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?"

Question:

Also, I understand that there are some new cyber security initiatives that have deadlines soon or were recently supposed to be completed such as the Federal Desktop Core Configuration, Trusted Internet Connection, transition to IPv6, etcetera.

How are your specific agencies coping with these transitions?

Answer:

USAID is working on these initiatives, and I support the ideas behind the cyber initiatives to improve security. I certainly understand the threat. However, like many agencies, we would like the deadlines for compliance with these initiatives to be more reasonable. What might help is to break up some of the larger initiatives into phases, with deadlines that take into account the size and mission of the agency. This prioritizes tasks and allows agencies to adjust resources between internal business and federal initiatives. Additionally, I think it would help to give consideration to the legacy

systems many agencies have in place that may prevent them from complying immediately.

Question:

And do you have comprehensive plans in place to be fully compliant with these initiatives when OMB has asked?

Answer:

Yes, USAID will be compliant within the mandated deadlines, with several exceptions. We are having difficulty with the Trusted Internet Connection (TIC) initiative and one of the actions listed in OMB Memorandum 06-16 to "Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required."

Question:

Is your agency struggling with complying with any of these initiatives?

Answer:

Yes, USAID is struggling with several initiatives. Specifically, we are struggling with the Trusted Internet Connection initiative for the following reasons:

- It is not clear how the TIC is planning to address overseas Internet gateways (gateways that allow local web browsing).

What consideration is given to organizations like USAID, which are in developing countries that cannot support the bandwidth requirements of a centralized Internet gateway approach?

- What changes would we need to make to our two CONUS Internet gateways that are currently covered by Einstein to make them TIC compliant?
- USAID has several dedicated connections to other agencies in the federal government that have been carefully crafted with protections including firewalls, detailed CONOPS, MOA's and constant monitoring. Information exchanged in this manner is often very sensitive and often involve life safety issues. What does the Agency need to do to get these connections categorized as "internal" so they don't have to be diverted through the TIC, which would needlessly expose the information beyond intended audience with no potential increase in security?
- If the USAID is granted authority to provide TIC services for its own community, what pressures will be exerted to provide similar services to other agencies? As a follow-up, when would there be a standardized cost model for charging external agencies that USAID

could review as part of the determination as to whether or not we could fiscally support the additional burden?

- Given that the USAID's missions are often located in remote and sometimes hostile regions of the world and the requirements for close interaction with the host country, dedicated connectivity, especially Internet back to Washington is often difficult to obtain and very expensive. That said; USAID has provided many missions the capability of obtaining Internet connectivity locally. These connections are centrally managed from Washington, DC, are fire-walled, have content filtering with the output sent back to Washington for analysis. With regards to internal Agency communications that come back to Washington, is this level of protection sufficient, or is there a need for additional monitoring/filtering?
- The TIC contemplates a simple change that should not require modifications to current infrastructures and the issue is as simple as a re-route of traffic to a different place. While this solution is one that is technically feasible, the reality is global networks such as USAID must make significant design decisions to applications in order to make the most efficient use of limited bandwidth in third-world

countries. Enterprise systems will suffer significantly if a network re-designing becomes necessary.

- Who ultimately has the authorization to provide and / or approve waivers and design decisions?
- The daily business of USAID missions includes interaction with various non-governmental organizations (NGO). Many USAID missions have web servers that allow NGOs to access. Will this practice be permitted when TIC is in place?

USAID is also struggling with a requirement in OMB Memorandum 06-16 to "Log all computer-readable data extracts from databases holding sensitive information and verify each extract including sensitive data has been erased within 90 days or its use is still required." We are struggling with identifying all databases, along with every instance where computer-readable data has been or can be extracted from the databases and saved into another computer-readable entity such as a spreadsheet or text file. Similarly, it is unclear how to successfully monitor the creation of extracts containing sensitive information to verify that the extracts have been removed after 90 days or that they are still needed. No automated solution is available that will fully complete this requirement.

Question:

If so, what needs to happen before you are compliant with these transitions?

Answers:

USAID is waiting on several factors before fully complying with the Trusted Internet Connection and OMB Memorandum 06-16. I am concerned about the Trusted Internet Connection initiative's potential financial impact to USAID and our ability to ensure our continued success in our overseas locations. So, we are waiting to see what, if any, adjustments or modifications OMB will allow based on our mission and in-place infrastructure. For OMB Memorandum 06-16, I'm not aware of a cost-effective, automated technology to ensure compliance with the mandate. Consequently, we are awaiting the identification of a technology and the appropriate funding to support its implementation.

Questions for the Record to
USAID Chief Information Security Officer
Phil Heneghan by
Senator Thomas R. Carper (#4)
Senate Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security
March 12, 2008

"Agencies in Peril: Are We Doing Enough to Protect Federal IT and Secure Sensitive Information?"

Question:

Ensuring appropriate executive level buy-in is critical to any mission critical area, especially information security. In your own agencies, have the roles of Chief Information Officers and Chief Information Security Officers been elevated to an effective level in the organization to put in place effective information security policies and procedures and enforce security?

Answer:

Yes, the CISO and CIO roles have been elevated to an effective level within USAID.

Question:

In your opinion, what is an effective level of authority to place our CIO's and CISO's within a federal agency of your size and mission?

Answer:

I feel that I have an effective level of authority where I can appropriately report to the CIO and also have access to the Administrator and other senior-level executives. USAID's structure mirrors the

organization described in GAO-08-34, "Implementing Chief Operating Officer/Chief Management Officer Positions in Federal Agencies". For instance, the CIO at USAID is part of the management team responsible for providing guidance and metrics to support long-term business transformation efforts. Through this interaction, I provide security information and metrics and support performance monitoring and information sharing with senior executives so that USAID is able to make informed risk-based decisions that are specific to its mission.

Answer:

I do believe that the Lines of Business initiative opens the door for broad technology sharing within the federal government. The USAID-developed Tip of the Day is an effective program that addresses an Agency's need for security awareness training. However, it may be difficult to translate the success that USAID has realized with this program to other agencies without additional financial support to ensure that the application scales and addresses the complexities of the largest department's network infrastructures. As the Lines of Business initiative broadens its offerings, I anticipate USAID will employ the technologies that solve problems for us.

Question:

In addition, do you think there may be more ways we can standardize information security practices to reduce costs and increase security?

Answer:

I feel that defining a standard of measurement across the federal government for areas of information security would provide a significant step towards standardizing federal security practices. These measurements should focus on risk management versus checklist compliance. If agencies understand what they should be measuring, they can assess if their programs are moving in the right direction from year to year.

○