S. Hrg. 111–662

MORE SECURITY, LESS WASTE: WHAT MAKES SENSE FOR OUR FEDERAL CYBER DEFENSE

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

OF THE

ONE HUNDRED ELEVENTH CONGRESS

FIRST SESSION

OCTOBER 29, 2009

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

53–852 PDF WASHINGTON : 2010

For sale by the Superintendent of Documents, U.S. Government Printing Office,
http://bookstore.gpo.gov. For more information, contact the GPO Customer Contact Center,
U.S. Government Printing Office. Phone 202–512–1800, or 866–512–1800 (toll-free). E-mail, gpo@custhelp.com.

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
THOMAS R. CARPER, Delaware
MARK PRYOR, Arkansas
MARY L. LANDRIEU, Louisiana
CLAIRE MCCASKILL, Missouri
JON TESTER, Montana
ROLAND W. BURRIS, Illinois
PAUL G. KIRK, JR., Massachusetts

SUSAN M. COLLINS, Maine
TOM COBURN, Oklahoma
JOHN MCCAIN, Arizona
GEORGE V. VOINOVICH, Ohio
JOHN ENSIGN, Nevada
LINDSEY GRAHAM, South Carolina
ROBERT F. BENNETT, Utah

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

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

THOMAS R. CARPER, Delaware, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
MARK L. PRYOR, Arkansas
CLAIRE MCCASKILL, Missouri
ROLAND W. BURRIS, Illinois

JOHN MCCAIN, Arizona
TOM COBURN, Oklahoma
GEORGE V. VOINOVICH, Ohio
JOHN ENSIGN, Nevada

JOHN KILVINGTON, *Staff Director*
ERIK HOPKINS, *Professional Staff Member*
BRYAN PARKER, *Staff Director and General Counsel to the Minority*
DEIRDRE G. ARMSTRONG, *Chief Clerk*

CONTENTS

WITNESSES

THURSDAY, OCTOBER 29, 2009

ALPHABETICAL LIST OF WITNESSES

APPENDIX

MORE SECURITY, LESS WASTE: WHAT MAKES SENSE FOR OUR FEDERAL CYBER DEFENSE

THURSDAY, OCTOBER 29, 2009

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 Subcommittee met, pursuant to notice, at 2:33 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Thomas R. Carper, Chairman of the Subcommittee, presiding.

Present: Senator Carper.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Good afternoon, everyone, and especially good afternoon, Congressman Tom Davis, whose sister, niece, and nephews live in the State of Delaware. We are grateful to you for coming today and sharing with us your advice and counsel.

The issue du jour is cyber warfare. It isn't science fiction. It is reality. Over the past few years, we have heard alarming reports that criminals, hackers, even foreign nations have deeply penetrated our government's most sensitive networks, including the offices of some of us right here in Congress.

In fact, just last week, the Congressionally-established U.S.-China Economic and Security Review Commission reported that China is strategically developing offensive capabilities that could be used against us in a future military conflict. Further, there have been reports that some of the previously successful cyber attacks against agency networks may have left behind what is commonly known as a back door, essentially a technological means for the bad guys to get back into our networks without anyone ever knowing about it.

These vulnerabilities could be used against us by those who might want to do us harm by stealing sensitive information stored on our military networks or by shutting down critical networks just when we need them the most. Imagine the terrifying scenario of a hacker creating uncertainty as to the validity of the data residing on the Federal Aviation Administration's (FAA) air traffic control systems. That is exactly the kind of scenario I hope our hearing today prevents.

But the threat of a cyber attack isn't something new. In fact, in 2002, Congress passed what is known as the Federal Information

Security Management Act (FISMA), to help prevent many of the problems that we are going to be discussing today. That legislation brought greater attention to the issue of cyber security and it helped to establish greater accountability within agencies. Overall, I think we would agree that it is a step in the right direction.

However, some 7 years after the passage of FISMA and approximately $40 billion later, I am troubled to learn that the Office of Management and Budget (OMB) does not track how much agencies spend on cyber security, nor does the agency measure those expenditures and whether those expenditures actually resulted in improved security. Even more troubling, agencies may be constrained from implementing the most basic cyber security best practice because of inflexible requirements.

Now, allow me to put this into perspective. Federal agencies have spent more on cyber security than the entire gross domestic product of North Korea, who some have speculated is maybe involved with some of those cyber attacks. That is unacceptable.

Some of the problems with FISMA implementation are a direct result of OMB's decisions over the years, while others are due to agency neglect. Still other problems lay at the feet of those of us here on Capitol Hill. In essence, there is blame enough to go around for all.

However, at today's hearing, we have an opportunity to discuss some concrete ways to correct some of those wrongs, and that is what we are going to do.

For example, one wasteful and ineffective area that OMB and agencies can target is what is known as the "certification and accreditation" process. The certification and accreditation process is essentially a process whereby agencies evaluate every 3 years what defense security protections are in place to prevent attacks on their systems. The process costs taxpayers about $1.3 billion—that is billion with a "b"—every year, and it produces a good deal of paperwork that ends up stored in binders in some clutter-filled rooms. In fact, those rooms look a lot like this one. In fact, that is one of them. There are, I think, others that look like it.

But we can see 3 years' worth of reports from the Department of State, just one department, which cost them a total of $38 million. These reports would be worth the price tag if the tactics that hackers used were as static as the words typed on a piece of paper. But hackers change how they attack us daily and their numbers, unfortunately, continue to grow.

And yet it seems like OMB thinks that a snapshot of agency preparedness every 3 years will somehow defend our critical networks. But instead, billions of dollars are spent every year on ineffective and useless reports, similar to the chart pictured here.[1] Meanwhile, we continue to get attacked.

However, testifying today will be a representative from the Department of State on our second panel who saw an opportunity to spend his agency's cyber security budget more wisely. Instead of spending money on ineffective paper-based reports, the State Department decided to focus on developing a system that monitored their global networks on a continuing basis.

[1] The chart referred to appears in the Appendix on page 99.

If you take a look at the second chart that has just been put up,[1] we can see the results of the hard work at the Department of State. According to that Department, they were able to reduce the amount of risk to their agency by 90 percent in a single year. I am told that this was achieved by developing a system that makes sense, uses effective metrics, and holds people accountable. In essence, the Department of State can prove that they have better security at a fraction of the cost that they were previously paying.

So as we progress through this hearing, I would like our witnesses to keep in mind that moving to a model more like the one at the Department of State requires no new legislation, costs less than or the same as the current paperwork-laden method, and will better protect our country. That is the kind of cyber security that makes sense to me, and I suspect that is the kind of cyber security that would make sense to most people in this country.

In fact, my colleagues and I introduced a bill last session, and we have introduced it again this year, which would require all agencies to move to a proactive approach like the one that the Department of State has taken.

In addition to requiring continuous monitoring of security controls and putting a strengthened Chief Information Security Officer in each agency, our bill would enhance the role of the Department of Homeland Security in cyber security. The Department would share information with agencies on where cyber attacks have been successful so that they can better prioritize their security enhancements.

Further, our bill would require agencies to use their enormous purchasing power to persuade vendors to develop and sell more secure IT products and services in the first place.

Again, our thanks to each of our witnesses. We certainly look forward to what you have to say, share with us, and to responding to our questions.

We will be joined as the afternoon goes on by others on our Subcommittee, but rather than sit here waiting for them for hours, we are going to dive right in with our first panel. As I telegraphed earlier, we will receive our testimony from former Congressman Tom Davis, who represented, I think, a Congressional district in the Northern part of Virginia, a State where I grew up. His service in the U.S. House of Representatives—how many terms did you serve there?

Mr. DAVIS. Seven.

Senator CARPER. Seven terms. Did it seem like eight?

Mr. DAVIS. It seemed like 20 at the end. [Laughter.]

Senator CARPER. Congressman Davis was the principal author of a number of pieces of legislation, but he was also the principal author of the Federal Information Security Management Act of 2002, lovingly called FISMA, which is the subject that we are going to be discussing here today.

He also held numerous oversight hearings on the implementation of FISMA and is considered an expert on the issue. I would like for the record to show that my name and the word "expert" have almost never been used in the same sentence. [Laughter.]

[1] The chart referred to appears in the Appendix on page 100.

We are pleased to have Mr. Davis with us, who is certainly an expert on this issue and very knowledgeable about a bunch of other things. It is a real pleasure to work with him. We are trying to make some progress on, among other issues, figuring out a path forward for the U.S. Postal Service.

But I understand that we will hear where you believe improvements can be made with the agency implementation and perhaps with the language itself, so we thank you for your previous service to our country and for your willingness to be of service again here today.

You are recognized to proceed for the next half hour—no, I will ask you to keep it fairly close to 5 minutes, but if you run a little over that, it is not going to trouble anybody too much. So thanks so much for coming, and your entire statement will be made part of the record.

TESTIMONY OF HON. TOM DAVIS,[1] FORMER U.S. REPRESENTATIVE FROM THE STATE OF VIRGINIA

Mr. DAVIS. Thank you, Chairman Carper. I really appreciate your efforts to improve information security and I am grateful for the opportunity to testify here today.

For 14 years, I represented the 11th District of Virginia, the home of the Internet. I would note for the record that I retired undefeated and unindicted.

Senator CARPER. That is quite an accomplishment. [Laughter.]

Mr. DAVIS. I was also honored to serve as a member of the House Committee on Oversight and Government Reform, first as the chairman of the District of Columbia Subcommittee, the least sought after Subcommittee chairmanship in the House, then as chairman of the Technology and Procurement Policy Subcommittee, then 4 years as chairman and my last 2 years as the ranking member. My Congressional service coincided with the proliferation of the Internet and the explosion of new capabilities that came along for both the public and the private sector.

It was clear the revolution in interconnectivity had the potential to fundamentally change governmental operations and service delivery. However, it also created a new form of vulnerability, one in which traditional protections of geographic distance and physical strength were irrelevant.

For these reasons, I made information technology management and security a focus of my work in Congress. Federal agencies needed to take this threat seriously and ensure proper procedures and tools were in place to protect information systems. Similarly, Congress needed a clear picture of the information security posture of the Federal Government in order to conduct effective oversight.

FISMA, which I championed in 2000 and 2002 and which had the concurrence from this Committee, was intended to help provide such a framework. FISMA required Federal agencies under the direction of the Office of Management and Budget to create a comprehensive risk-based approach to information security management. It further requires annual IT security reviews, reporting, and remediation planning at Federal agencies. These requirements

[1] The prepared statement of Mr. Davis appears in the Appendix on page 36.

were based on best practices, and in addition to safeguarding information were intended to make security management an integral part of an agency's operation.

At the time FISMA was enacted, no coordinated priority existed to address the threat of cyber attacks. Technology was evolving rapidly. Rather than taking a prescriptive approach, we believed agencies needed to walk before they could run, and putting procedures and protocols in place was an important first step in protecting government's critical infrastructure.

Since its enactment, FISMA has undoubtedly served to elevate the importance of information management and information security in government, and I am proud of the progress we have made. That said, there is room for updates and improvement, and your legislation, I think, is a very positive step in that direction. It is time to really take FISMA to the next level.

While I believe the requirements listed in FISMA would be components of any sound information security plan, the need at present is to operationalize its implementation. This would involve tools such as Red Team penetration tests. It would also require appropriate performance measures and, as the time between a penetration and detection, the time to deploy a security patch once it has been released, and the time to complete a root cause analysis when a security breach does occur, I am pleased your language references both penetration tests and performance measures.

Three other key ingredients: Responsibility, Authority, and Accountability.

Chief Information Security Officers (CISOs), may be responsible for overall information security planning, but they can't be just the bad men when things go wrong. Responsibility for an information security program permeates an organization, from the head of the agency to every employee. Most of the security breaches that have grabbed headlines in recent years aren't the result of some evil cyber genius but Federal employees failing to adhere to basic security protocols—a lost laptop, a stolen Blackberry, computers never returned when an employee leaves an agency. These can result in the personal information of untold thousands being put at risk.

CISOs might have to come up with the protocols, but the rank and file have to adhere to them. As Congress looks at information security issues, it might be wise to consider uniform procedures, training, and penalties to reduce theft, loss, or other adverse events. I might add, in the private sector, training is very critical in these areas and it is drummed into employees at every level.

Your language gives CISOs authority to development, implement, and enforce security measures. That is important. There also have to be consequences, good and bad, for failures and successes. That is one aspect of the accountability component. The private sector provides some models. For example, the payment card industry mandates compliance with standards set by the PCI Security Standards Council. Failure to adhere to these standards results in a business losing the ability to conduct transactions with payment cards. Now, that exact example isn't going to fit the Federal system, but we need carrots and we need sticks that promote compliance and punish negligence.

Another aspect of accountability deals with funding. Federal Government spending has risen sharply in recent years, but to what end? We have to link performance in this specific instance, performance of information security products and services, with spending decisions. Simply asking for more or providing more isn't going to fix the problem, nor is it going to serve the interest of the American people.

In closing, I would like to reiterate my appreciation for the work you are doing on information security. The information age is indeed a strange new world in which a mischievous teenager could be just as dangerous as a terrorist organization or malevolent government. I am committed to helping however I can to make sure our Federal systems are up to the task and that our oversight mechanisms are commensurate to the need, and I think your legislation is a good step forward. Thank you.

Senator CARPER. Thank you very much, Congressman.

I don't know if you have ever done this, but one of the things I have done for a number of years as a new Senator here, whenever it is one of my colleagues' birthdays, I actually call them on the phone if we are not in session and just wish them a happy birthday, track them down wherever they are, around the country or really around the world. Those are calls that I enjoy, and I think my colleagues do. I do the same thing with members of my staff, former members of my staff and just family and friends.

I don't know if this is true, but it is in my briefing notes so it must be true—but I am told that today happens to be the birthday of the Internet, and I was thinking about maybe just sending an e-mail out and seeing how well it can get around and cover as much of the Internet as we could—— [Laughter.]

But I understand that 40 years ago, I'm told, in 1969, the first message was sent out on the Internet, and I understand that the message also ended up crashing the Internet. [Laughter.]

So today's hearing is timely.

I would just ask, Congressman Davis, as one of the principal authors and Congressional overseers of the FISMA legislation, you know all too well that there have been some successes and some challenges since its adoption. For example, it seems that OMB has historically focused on agency compliance rather than on agency outcomes. And I must say, we are real good at focusing on process and compliance rather than outcomes.

Arne Duncan was just in Delaware, the Secretary of Education, and he spent a fair amount of time at the University of Delaware 2 days ago talking about the need for us in education to focus not on process, but on outcomes. It turns out that is not just in education, but it is in this regard, as well.

Could you take a few minutes maybe and explain to us where you think there are opportunities to improve agency cyber security? It seems like the sophistication of the attacks dramatically evolves every year. We just met with an agency head in the current Administration who shared with us just how many cyber attacks are occurring every day on his agency, on the agency that he leads. It is alarming. But this training has led to a huge increase in the number of reported breaches by agencies.

As you know, I have been trying to lead the effort to reform FISMA and really strengthen it to make it the legislation that I think you, as its principal author, hoped it would be so that agencies focus their limited resources on improving security rather than just producing the kind of paperwork that we see over here to my right.

Some of the improvements that we have been suggesting, such as continuous monitoring, seem like they make a lot of sense, and the best part of this idea is that it doesn't require a bill to be passed by Congress. However, the previous Administration didn't seem all that interested in making any changes to the current reporting structure, at least not during their final year. I think they just said, we will let the new folks take care of that.

So that is a big way of leading me to this question, and I would just ask, Congressman Davis, what are your thoughts on this idea, and are there other opportunities that either us on this Committee, Subcommittee, or the Administration should be looking into?

Mr. DAVIS. Well, thank you. That is a pretty broad range, but let me take a stab. Let me note first that in your second panel, you look at the State Department and what they have done. This is an agency that has paid careful attention to not just compliance, but also operationally what to do, and I think you are going to get some glimpse of some of the things that can be done across other agencies when they give it the appropriate attention.

You know, it is hard to legislate priorities. It has really got to come from the Executive Branch, because our managers have so many different things to do, so many boxes to check, that at the end of the day, they make everything a priority and nothing becomes a priority. And that is one of the difficulties. This legislation will help, but if an administration or an agency head doesn't buy into this, it is difficult to make it really as operational as we would like it. Anybody can check a box. That is not hard to do. But making this a priority—and you will hear in the next panel, I think, some good ideas on this.

You can't just involve the heads of the agencies or the CISOs, as I have noted before. You need to get a buy-in at all levels. This has to be part of what every employee does. It has to be drilled into them through training. They have to understand, anybody that deals with any entry point, any secure network, that they have to really be on top of that 24 hours a day.

A lot of our problems result from just plain negligence, people that didn't take this seriously. It wasn't drilled into them as part of their jobs. It means everybody has to be trained, that really, our whole systems are vulnerable at our weakest point, and our weakest point is any entry point, and frankly, any employee.

I like the certification process you talk about in this bill. I like the idea that using the purchasing power of the government to not just drive down costs, but you can get a congruity of products that way. One of the difficulties in government is we are so stovepiped. We have agencies even within agencies that aren't talking with each other. I think using that purchasing power, maybe allowing the Group 70 Schedule in GSA to be utilized by States and locals—well, not just Group 70, the schedules for any cyber products to be included in that could be helpful in getting the same kind of prod-

ucts that everybody is using appropriately certified. There is just a lot of room here if we will make it a priority, and I think you have included some of those in the bill.

Finally, the carrots and sticks are tough in government. How do you reward? How do you punish the people that aren't doing this? You can always do it through bonuses and you can do it through promotions and those kind of things, but that has to come from management. It has to come from a buy-in from the top.

And you are right. We banged our head in the previous Administration trying to take this to a different level and get their interest in it. But what so often happens with administrations, they have so many different things to do and different agency heads, that without a lot of additional money, this doesn't become the priority. They want to make sure that they are advancing their mission and they will take a chance of a cyber attack hoping it doesn't occur on their watch and spend the money in other areas.

Senator CARPER. I appreciate the kind words you have had to say about the legislation we have reintroduced this year. If you were on this side of the dais, where you sat for many years, and had an opportunity to contribute to the legislation, to amend it, to make better what we have introduced, any thoughts of what you would do, or what you would have us do, to strengthen it further?

Mr. DAVIS. I alluded to one part in my testimony and that is the fact that we are losing a lot of information and a lot of secure information just by employees and contractors mishandling this information, taking computers home. In the case of the Veterans Administration, the employee that took this home that had his computer stolen, it wasn't even encrypted. We have now changed that through protocols.

But we are still—we have lost Census information, we have lost hand-helds. We have people leaving with their computers from government and sensitive information and nobody has bothered to get it back. I think writing that into law would be very helpful in terms of those kind of protections and making sure that at least we are not being careless about this. If we are going to get penetrated and hit, make them earn it. Don't make it easy. And I think sometimes, as I said, any careless employee can lose confidential information if it is not handled right. I think that ought to be written into this.

Senator CARPER. Alright. Thank you.

I suspect you have been following the current debate about whether there ought to be a cyber coordinator, which is supposed to help prioritizing and align agency efforts. As you know, FISMA clearly gives the responsibility for coordinating the Federal Government's cyber security to OMB's Administrator for E–Government. However, I am concerned that the people who work in that office may not have the cyber security qualifications that are needed or necessary to make sure that agencies are cost-effectively securing their networks. In fact, I am even more troubled that OMB has never asked, apparently, how much money they spend on cyber security.

What are your thoughts on the role of the E–Government office in the larger cyber security discussion, and what do you believe

should be the role of that office in overseeing agency cyber security?

Mr. DAVIS. Well, you are going to hear from Vivek Kundra, who is very able. He will have a perspective on that now, having come to the Federal Government. He used to be with the Commonwealth of Virginia, where he did an outstanding job. I am glad the Administration has recognized his capability. So he may have a little bit different perspective.

But coming from the legislative perspective on this, I think you are spot on. The E–Government is the head of that area. It may not have expertise in this particular area. Even more important, I think, is navigating the land mines of getting a consistency across government in terms of how this is going to be implemented.

OMB, Homeland Security, I don't know how you want to pick this. A Cyber Czar, though, or someone who has that particular expertise and can navigate this so the Administration can get everybody kind of marching to the same protocols, using the same systems, instead of having it so stovepiped and factionalized as it is now, is just a very important part of solving this problem.

Senator CARPER. Alright. Thanks.

Let me just follow up on that with another question that relates to this. I understand that you have been briefed on some of the benefits that the State Department has been able to achieve with their new system. I was just wondering if there were any risks associated with following that model. Sometimes, as a recovering governor, we used to say that what would work in Delaware may not work in Virginia. It may not work in Missouri. It may work in Texas, but it works in Delaware. But in some cases, there is one model that will serve in a variety of different States, and in this case, agencies. But I wonder if there are any risks with following the model that they have pursued at the State Department? What do you see are some——

Mr. DAVIS. Well, I am not sure—first, I think State has done just an outstanding job, and what they have done is they have paid attention. They have taken the legislation seriously and you have a dedicated cadre up there at the top that have driven this.

What works at State may not work at Commerce. It may not work in intelligence. I am not probably smart enough to know that. But the one thing State has shown us is that when you get agency officials that take this seriously, they can make a huge difference. And, of course, State has been vulnerable to a number of attacks, which I think has heightened their awareness of this. I hope it doesn't take cyber attacks in some of these other agencies to get them to up their awareness—but it is just a good model of how you have people sitting around a room thinking about what are their possible vulnerabilities and coming up with a program to combat that.

Again, I don't know if I am qualified to talk about what would work at different agencies and what the vulnerabilities are, but that is just a good example. Their FISMA grade has been excellent, not just because they checked the right boxes, but because they have been operational in what they have done, as well.

Senator CARPER. OK. One of the things we are trying to encourage agencies to do more of is this notion of continuous monitoring,

rather than just taking a snapshot every 3 years, but to focus on this and monitor every day. Are there any pitfalls with that that come to mind?

Mr. DAVIS. Well, the one pitfall when you are not just monitoring it but when you are testing these is you run into the Freedom of Information Act (FOIA) situation. You don't want everybody to know what your vulnerabilities are. I think you need to keep a cap on that so that you can make the appropriate corrections.

The other thing I would add is there is a lot we can learn from the private sector. The private sector has had to deal with these issues even more than government, the banking system, in particular, with the kind of penetrations that they are getting, the hits they are getting. Opening up that dialogue with the private sector is important to understand what they have gone through and some of the innovations that they have made. The difficulty comes in the FOIA laws. It comes with antitrust. It comes from tort law and their ability to share that information with us, and that is a dialogue, I think, that needs to continue. But they can be a part. There is a lot of expertise out there in the private sector we want to harness and bring into government.

Senator CARPER. Two more questions and I am all done. In the Federal Information Security Management Act (FISMA) bill that you helped to create, the Inspectors General are required, I believe it is annually, to evaluate whether agencies are doing the kind of security that they say they are doing in this regard. For example, the Inspectors General use paperwork from the certification and accreditation process to evaluate whether agency security is really effective.

I understand that if all the agencies moved to an approach like the one they have over at State, not much paperwork is going to be produced. In fact, it seems to me that an Inspector General could come at any time during the year, see whether the agency's security is actually effective. I don't know if this is a question you would be prepared to answer, but do you think that is true, and what should be the role of the IGs in this?

Mr. DAVIS. Well, the IGs are independent. I mean, that is the one reason that I think they are equipped to do this as opposed to someone else who could be under the thumb of the agency. You really want an independent to look at that. Now, the IGs operate differently in different departments. They have different burdens that they have to meet. But they bring an independence to this which I think is critically important.

Senator CARPER. And finally, you served on the House Committee on Oversight and Government Reform for, I think you said, maybe 14 years, as Chairman for 6 years, as Ranking Member for another 2 years, and during that time, you and I were able to work together to identify a couple of potentially wasteful practices in the Federal Government, and I think in one or two cases, we actually made some positive changes.

What do you see as the greatest opportunity for improving the efficiency of cyber security spending in the Federal Government?

Mr. DAVIS. Well, I think contracting. All this really comes down to contracting, and when it is done ad hoc in stovepipes by different agencies, not sharing information, not building it together, you get

a lot of systems that, at the end of the day, some are better than others. They don't talk to each other. It has to get coordinated.

One of the things I like about this bill is you use our purchasing power together to drive those products and I think that will bring it together much better than we have today. We spend a lot of money. We don't always get what we want in government contracting across the board. But in this particular case, I think—I like your concepts that you have in this bill, government using its power. I think that will drive a congruity of products that is absolutely necessary in this case to get this solved.

Senator CARPER. Alright. Well, those are my questions. Some of my colleagues who are waiting back in the anteroom until you leave—no, they are not, but when some of my colleagues show up, whether they show up or not, some of them are going to have some questions that they would like to send along——

Mr. DAVIS. You can always get them to me. We are happy to respond. You have a great second panel, as well, and thanks for allowing me to share my views.

Senator CARPER. It is great to see you. Thanks so much for your previous service to our country, and not just for the folks in Virginia, but also in Delaware and the other 48 States.

Mr. DAVIS. Thank you.

Senator CARPER. Good luck. Take care.

The second panel is welcome to approach the table and take your seats. Gentlemen, welcome. It is good to see you all, and thank you for taking the time to be with us today.

I understand from Erik Hopkins, who has worked on this legislation for a couple of years now, that we have on a dolly up here some of the paperwork that kind of flows from—is it just one agency? Not just from one agency, but from one system, is that right, one system within one agency, their paperwork from their certification and accreditations. If that is just one system and one agency, I hate to think what would be the case for the whole government.

Be careful, Mr. Streufert. You are not going to have a place to sit here very soon. Well, that gives us some idea. That is a fair amount of paperwork. And again, that is one system and one agency. We wouldn't be able to see you guys—you probably wouldn't be able to get in the room—if we had all of them gathered here today.

Let me make some introductions to kick off our second panel. We are going to hear from Vivek Kundra, who was appointed Federal Chief Information Officer of the United States by President Obama in March of this year. We are glad to see you are still able to sit up and take nourishment and to be here with us today. You look none the worse for wear.

As Congressman Davis mentioned earlier, prior to his taking his current position, Mr. Kundra served in Mayor Fenty's cabinet as the Chief Technology Officer for the District of Columbia and in Governor Kaine's cabinet as Assistant Secretary of Commerce and Technology for the Commonwealth of Virginia. You are great to be here and we appreciate your service and thank you for your presence.

Our next witness is no stranger before our Subcommittee. Mr. Wilshusen. He is the Director of Information Security Issues at the

Government Accountability Office. We are told today by our chaplain, Chaplain Barry Black, Chaplain for the U.S. Senate, he said the words that people most enjoy hearing in their lives is the sound of their own name. Among the words that they least like to hear are their own name mispronounced, so we will try to get your names right. But I will say, none of your parents made this easy for a guy like me. [Laughter.]

So please bear with me. But I am told you have over 28 years of auditing, financial management, information systems experience starting at the age of 12, and you have been at it for quite a while. Before joining GAO in 1997, Mr. Wilshusen held a variety of public and private sector positions, so we thank you for coming back today.

Our last witness is John Streufert. Your name doesn't look like "Stroy-fert," but it is, isn't it? I bet it has been mispronounced once or twice, hasn't it?

Mr. STREUFERT. Yes. Every day.

Senator CARPER. You are the Chief Information Security Officer at the Department of State. You are like our hero here today, and we are here to celebrate what you have done and to try to find out if it is something we can replicate in other agencies.

I am told that since starting your current job, you have been recognized for outstanding leadership and improving cyber security at both the Department of State and the U.S. Agency for International Development (USAID). In fact, Mr. Streufert was a recipient of the Distinguished Presidential Rank Award in 2004 for his work at USAID, and I understand that you will show us once again how we can improve cyber security, so good for you.

With that having been said, we will turn to Mr. Kundra as our first witness and ask you to proceed. Your statements will be made part of the record, so feel free to summarize as you wish. But you are recognized. Thank you.

TESTIMONY OF VIVEK KUNDRA,[1] FEDERAL CHIEF INFORMATION OFFICER, ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, U.S. OFFICE OF MANAGEMENT AND BUDGET

Mr. KUNDRA. Good afternoon, Chairman Carper. Thank you for the opportunity to testify on the Federal Information Security Management Act and information security posture of the U.S. Government.

Our Nation's security and economic prosperity depend on our digital infrastructure. The President's Cyberspace Policy Review stated that cyber security threats are some of the most significant economic and national security challenges of the 21st Century.

The groups of State and non-State actors that target U.S. citizens, businesses, and Federal agencies is growing exponentially. Daily, there are millions of attempts to attack open ports and vulnerable applications across our government.

The Federal Government's current security posture does not adequately confront the real-time threat factors that we face on a daily basis. Hiring challenges, a focus on compliance, and cumbersome

[1] The prepared statement of Mr. Kundra appears in the Appendix on page 39.

reporting have inhibited effective cyber security management. The Federal Information Security Management Act of 2002 raised awareness across the Federal Government regarding information security, yet significant progress is essential when it comes to execution.

To advance the Federal Government's security posture, the Administration is taking steps in key areas, such as human capital management, performance management, cost analysis, and risk management. For example, in the area of human capital management, we expedited the hiring authority for up to 1,000 cyber security professionals across the Department of Homeland Security. This will enable DHS to recruit skilled cyber analysts, developers, and engineers to secure our country by securing our Nation against cyber attacks.

To enhance the performance monitoring, last week, we actually launched CyberScope, an online platform for agencies to submit security information that will allow us to analyze and monitor the Federal Government's security posture in a comprehensive manner. Prior to 2009, it took three full-time employees to compile hundreds of spreadsheets that were e-mailed to OMB by agencies in response to FISMA reporting requirements. This laborious, unsecure process inhibited insight into the security posture of the government. The threats we face change daily, yet our legacy reporting processes have been tied to manual, annual, and quarterly processes to evaluate how secure we are.

The CyberScope platform will be leveraged to develop a cyber security dashboard that will unlock the value of agencies' submissions when it comes to FISMA reporting and also the real-time posture across the Federal Government. Just as the IT dashboard took us from a static, paper-based environment to a dynamic, digital environment, the new cyber security dashboard will provide the government with a real-time view of threats facing us and our vulnerabilities.

For example, the State Department is supplementing its FISMA reporting with a risk-scoring program that you alluded to that scans every computer and server connected to its network at least 36 hours on multiple security factors. Rather than just conducting certifications and accreditations every 3 years, continued monitoring must be the norm across the government.

To enable effective security cost analysis, we are asking agencies for detailed security cost information for the first time. We recognize that the best security is baked into the systems and the architecture and investments that agencies are making. Therefore, we see this as the beginning of the process of obtaining relevant data. In the coming years, detailed cost data combined with performance-based metrics will allow OMB and agencies to effectively manage and make informed decisions when it comes to risk.

To better manage risk, OMB has established a task force that was launched last month to develop forward-leaning metrics and making sure that those metrics are actually focused on outcomes rather than process. To solicit the best ideas, we have reached out across the Federal community as well as the private sector. OMB plans to release the metrics for fiscal year 2010 along with a road map of how we are going to move from a culture of compliance to

a culture of outcomes in the first quarter of 2010. What gets measured gets done.

The threats we face are numerous, evolving faster than our cyber defenses, and they have the potential to do great harm to our cyber infrastructure. From the launch of CyberScope to the hiring of up to 1,000 new DHS cyber security experts, the Administration is committed to strengthening our cyber defense. A secure, trusted computing environment in the Federal Government is the responsibility of everyone involved, from agency heads to those charged with oversight. It entails employees, contractors, and the American people all working together.

This will not be easy, nor will it occur overnight. Our current actions represent important steps toward a strong cyber defense and begin the shift from a culture of compliance to one focused on real security to protect the digital infrastructure that is so vital to our economic prosperity and national security.

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

Senator CARPER. You bet. It is I who thank you.

Mr. Wilshusen, please proceed. Thank you, and welcome back.

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

Mr. WILSHUSEN. Mr. Chairman, thank you for the opportunity to participate in today's hearing on how agencies can establish cost effective cyber defense.

FISMA, which was enacted in 2002, was intended to provide a comprehensive framework for ensuring the effectiveness of security controls over information resources that support Federal operations and assets. It also requires agencies and OMB to annually report on the adequacy and effectiveness of agency information security programs and compliance with the provisions of the Act. To help meet these requirements, OMB established a uniform set of information security measures that all Federal agencies report on annually.

Mr. Chairman, in light of questions about whether agencies are measuring the right things in securing their systems, you requested that GAO examine how organizations develop and use metrics to assess the performance and effectiveness of their information security activities. In a report being released today, we describe the key types and attributes of information security performance measures and the practices of leading organizations in developing and using them, and compare those measures and practices with those used by 24 major Federal agencies and OMB.

Leading organizations and experts identified measures that generally fell into three major types: Compliance, control effectiveness, and program impact. They stressed the importance of developing and using different types of measures to ensure the measurement process is comprehensive and useful in achieving their information security goals. They also reported that all such measures generally

[1] The prepared statement of Mr. Wilshusen appears in the Appendix on page 45.

have certain characteristics or attributes. These attributes include being measurable, meaningful, repeatable, and actionable.

Further, these organizations and experts indicated that the successful development of measures depends on adherence to a number of key practices, including focusing on risks, involving stakeholders, assigning accountability for measures, and linking them to business goals.

Mr. Chairman, we have determined that Federal agencies have not always followed these key practices. While agencies have developed measures that generally fall into each of the three major types, on balance, they rely primarily on compliance measures, which have a limited ability to gauge program effectiveness. Agencies stated that, for the most part, they predominately collected measures on compliance because they were focused on measures associated with OMB's FISMA reporting requirements.

In addition, while most agencies have developed some measures that include the four key attributes identified by leading organizations, these attributes were not always present in all agency measures. Further, agencies have not consistently followed key practices in developing measures, such as focusing on risks.

Last, the measures established by OMB for FISMA reporting purposes are primarily compliance-based. They focus on whether control activity was implemented, not how well or how effectively that control was implemented. Consequently, OMB's report to Congress provides limited information about the effectiveness of agencies' information security programs and the security posture of the Federal Government.

In our report, we recommended that OMB provide direction and guidance to agencies in developing and using measures that better address the effectiveness of their information security programs. We also recommended that OMB revise its annual FISMA reporting guidance to require reporting on a balanced set of performance measures, including measures that focus on effectiveness of control activities and program impact, and to revise its annual report to Congress to better provide information on the effectiveness of agency security programs, the extent to which major risks are being addressed, and progress that has been made in improving the security posture of the Federal Government.

OMB has generally agreed with our recommendations. Implementing these recommendations will help to focus attention on activities that will enhance the effectiveness of security controls and improve the cyber defense of Federal computer systems and information.

Mr. Chairman, this concludes my statement. I would be happy to respond to any questions that you may have.

Senator CARPER. Good. Thank you so much. Mr. Streufert, you are number four.

TESTIMONY OF JOHN STREUFERT,[1] CHIEF INFORMATION SECURITY OFFICER AND DEPUTY CHIEF INFORMATION OFFICER FOR INFORMATION SECURITY, BUREAU OF INFORMATION RESOURCE MANAGEMENT, U.S. DEPARTMENT OF STATE

Mr. STREUFERT. Good afternoon, Chairman Carper. I am pleased to have this opportunity to testify before the Subcommittee regarding the Department of State's capabilities for securing its global information and technology infrastructure.

The Department serves as the diplomatic front line in over 270 overseas posts by serving its 70,000 users with the Worldwide Network and mission essential software applications. The foreign policy mission makes an inviting target for attack by highly-skilled cyber adversaries. However, the Department's layered approach to risk management allows multiple levels of protection.

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

The passage of FISMA served as a game-changing event for the Federal agency community. FISMA applies to all information used on behalf of Federal departments and agencies on behalf of American citizens. It established a holistic information security program and also the responsibility of accounting to oversight entities, including Congress. Together, these served as valuable checks in determining the health of an agency's information security program.

However, the Federal cyber landscape has changed in the past 5 years. The implementation of Federal cyber security has been typically undertaken through manual processes and compliance checks, like in conducting an annual inventory of systems, testing security not less than annually, reporting quarterly on weaknesses to OMB and performing certification and accreditation studies every 3 years.

Our cyber problems, though, have dramatically escalated in severity and frequency. In a typical week, the Department of State blocks 3.5 million spam e-mail and intercepts 4,500 viruses and detects over a million external probes to our network. Of that number, in the past 2 years, the percentage of malicious code attacks recorded at the Department of State on trouble tickets has jumped from 38 percent in the year ending August 2008 to 79 percent just 12 months later for that same period. The volatility of changes to security-sensitive changes has been equally problematic.

Ongoing demands for certification and accreditation studies similar to this single system that I have shown the documentation for here, amounted over 6 years to the expenditure of $133 million, amassing a total of 50 shelf feet, or 95,000 pages for just the 150 major information systems that we were monitoring to this degree. This does not include the databases for tracking system inventory or tracking the plans of action and milestones to resolve the pending weaknesses. This equates to the cost of the CSA report, not in-

[1] The prepared statement of Mr. Streufert appears in the Appendix on page 51.

cluding the related products, like the security plans, of roughly $1,400 per page.

And indeed, if there is any particular problem with this, it is not the content of the report, it is the fact that you could get a false sense of security that these snapshots produce results on paper that are extraordinarily accurate but out of date within days of being published, in fact, perhaps out of date even in the time that it took to print these 2,000 pages.

In contrast, this month, the Office of Management and Budget launched CyberScope, a secure streamlined interactive data collection platform far more efficient in allowing and also allowing research and analysis across Federal agencies. The U.S. Chief Information Officer has similarly and in support of this formed an interagency task force charged with developing outcome-focused metrics for information security performance by all Federal agencies and departments, including the Department of State. Final metrics based on this work are expected to be released later this fiscal year.

For its part, the Department began supplementing its FISMA compliance reports and studies with a risk scoring program that scanned every computer and server connected to its network not less than every 36 hours on eight factors and twice a month for safe configurations with software. This risk scoring program utilizes best practices, such as the Consensus Audit Guidelines, which was a collaborative effort between government and industry.

To assess the vulnerabilities, we use the Common Vulnerability Scoring System of the National Institute of Standards and Technology and the Department of Homeland Security, where scanning tools tag specific risks with point values between zero and 10, with 10 being the highest vulnerability. When the problem is resolved in this method, risk points are deducted and a better score comes to the technical team and organizations. This computation occurs no matter where they are located across the world.

Since mid-July, overall risk on the Department's key unclassified network, measured by the Risk Scoring Program, has been reduced by 90 percent in overseas sites and 89 percent at domestic sites, as the chart indicates.[1] These methods have allowed one critical piece of the Department's information security program to move from snapshots in time to a program that scans for weaknesses continually, identifies weak configurations each 15 days, recalculates the most important problems to fix in priority order on a daily basis, and issues letter grades of A-plus through F monthly to managers so that accountability for progress can be taken for every organization as experience has indicated for them over the past 30 days. The various score reports tabulate risk scores by region, compare progress overseas to our domestic sites, and creates enterprise-wide summaries for senior management.

In short, these details empower administrators with targeted daily attention to conduct remediation and offer summaries to empower experts to our executives to oversee the most serious problems.

[1] The chart referred to appears in the Appendix on page 100.

Mr. Chairman, I want to conclude by emphasizing that the Department's policies, technologies, business processes, and partnerships in place continue to evolve and continue to meet the challenges as the threats change in the cyberspace environment. I thank you and the Subcommittee for this opportunity to speak before you today and would be pleased to respond to any of your questions.

Senator CARPER. Thanks, Mr. Streufert, for that testimony. Thanks for being a good role model over at the State Department and USAID for the rest of us.

I just want to start with this chart,[1] and it looks like a reduced risk of cyber vulnerabilities, about 89 percent at the State Department headquarters from July 2008 to July 2009, and 90 percent abroad. Did you anticipate this kind of progress in a year when you were getting into this? Did you anticipate this kind of a record of achievement?

Mr. STREUFERT. At the Agency for International Development (AID), we had a similar progress, a two-thirds reduction in a 6-month period, so we had a feeling that it was possible but had not yet tested this on the scale of an organization the size of the State Department. We were certainly very pleased, and at that point, we began discussing what had been found with our colleagues.

Senator CARPER. You mentioned this in your testimony. I want you to go back. Kind of walk us through again why were you so successful at the State Department and at AID before that? What were the key elements again, please?

Mr. STREUFERT. This is an instance where support beneficially comes from many parts of the organization. It begins, as Congressman Davis indicated, with strong support at the top, and I am pleased to say that the senior leadership of the State Department has been very supportive at each step on the way.

Senator CARPER. When you say senior, how senior? What are we talking about?

Mr. STREUFERT. Under Secretary for Management Patrick Kennedy, and he has assembled an E–Government Oversight Board for the Department of State. I have been able to speak on progress before this group twice in the last year. So there has been strong involvement from the top of the organization.

The next beneficial thing that one needs is the coordination and——

Senator CARPER. Why do you suppose the folks at the top were so supportive?

Mr. STREUFERT. Well, we understand that strong information security is essential for our mission. We are spread in 24 time zones. The ability to send and receive information in support of American citizens services, and in support of the passport and visa process are vital to our mission. We understand that we depend on the information systems, and therefore the security related to them.

Senator CARPER. OK. Other than support at the top, what were the other key elements in your success?

Mr. STREUFERT. We brought together a coalition of 11 different organizations inside the State Department that worked on tech-

[1] The chart referred to appears in the Appendix on page 100.

nology matters, and that set the template where we could begin our regular scanning. And after that point, when we deployed the system, the fact that the individuals at each of the embassies and consulates and headquarters organizations could understand exactly what they needed to fix, it was of substantial benefit to them to get some of the positive reductions in risk points that the chart and our experience indicates.

Senator CARPER. Now, talk to us about other agencies being able to replicate the success that you enjoyed at the State Department. Other than cloning you, moving the agency heads from State over to—cloning them and moving them into the other agencies, how transferrable is this to other agencies? What do you think might transfer and what might not?

Mr. STREUFERT. One item that we always mention in discussion with other cabinet departments is that we used information that was already being collected in our organization for other purposes, including producing the certification and accreditation reports. Eighty percent of the information, as an example, was an outgrowth of what we needed to manage our servers and personal computers already. So it was simply a question of lifting that data up and out of where it was at the local level and then putting it in the security warehouse. Once there, our dashboard calculates grades and shows the most serious problems that need to be worked on.

Since many of the other parts of the Federal Government have this software, the primary things to work on are assuring that all of the networks are connected and that they have the support structures in place in order to put the security information out to the managers who want to make the changes. And I should hasten to add, the progress at the State Department came from thousands of individuals that were working every day on their most serious problems, and that is where the progress indeed came from.

Senator CARPER. Let me ask, first, Mr. Kundra, and then Mr. Wilshusen about replicating this kind of success. How do we go about doing that? In fact, it may be something you have already begun. I don't know.

Mr. KUNDRA. Yes. We started talking about this back in April, and within the Federal CIO Council, Susan Swart, who is the CIO at the State Department, has been sharing this approach with our colleagues. But if you look at what we are doing across the Federal Government, CyberScope is the first step in that direction in terms of if you looked at the previous approach, it was manual, it was based on a lot of paperwork and didn't really produce meaningful insight where we could slice and dice information across the Federal Government so we could compare what was happening at Health and Human Services versus State versus DOD versus Department of Energy. The first step is to make sure that we are getting data and information so we could get meaningful insight.

The second part of that, which is the task force that we are spending a lot of energy and we would love to share the metrics with you and get feedback from the Congress at the end of November, and these metrics are essentially going to be focused on game changing ways where we can address real security. So not necessarily asking the question, do you have a patch management pro-

gram, but getting to the point which is how long does it take you to actually patch those systems.

And thinking about the Red Teams, it is not enough to just say we have this file room that you pointed to. I talk about how the files you see in that room are actually far more secure than the very systems they are supposed to protect. So how do we get Red Teams to validate that the information that is out there, we are testing it against what we know in terms of agencies and it makes it really difficult right now across the Federal Government to spot patterns. So if we see a threat vector that may start at the State Department, how do we know we don't have the same threat vector at Health and Human Services?

So we are in the early phases in terms of deploying a Federal Government-wide approach. But the key here, as Congressman Davis said, is to move away from this culture of compliance and really move towards execution. How do we get these things done and how do we apply some of these methodologies? And I know that DHS and the National Institute of Standards and Technology (NIST) are actually working with the State Department to think through how this can be scaled across other Federal agencies.

Senator CARPER. Mr. Wilshusen, same question in terms of replicability. What do you think we ought to be able to replicate and why not?

Mr. WILSHUSEN. Well, I had the privilege of Mr. Streufert giving me a presentation of his system last week, and so I can't really attest to the accuracy of the data that he presents, but a couple of things——

Senator CARPER. Would you say that the accuracy is probably pretty skeptical?

Mr. WILSHUSEN. Well, I just don't have data or evidence to show that it is accurate. I can't say one way or the other. We just haven't done the tests on that.

But what his system shows is a lot of promise. With regard to replicability, one of the key aspects that it relies upon is the ability to have automated tools in place that have the capability to reach, touch, and then scan each of the devices that are covered under this particular system. Now, the Department of State has, according to their system, about 30,000 devices that are covered by this particular system.

It does at the present, as I understand it, cover Windows workstations and servers. And so presumably, it might be able to be replicated at other agencies to address those particular servers if those other agencies allow a central point to be able to go out and reach all those devices throughout the entire organization, and that may or may not be the case. I just don't know.

Senator CARPER. Erik Hopkins, sitting right behind me, just handed me a note that says, "Agencies are making the decision right now to spend another $1.3 billion to produce the paperwork we see here. Is there anything we can do about that?" It is a pretty good question.

Mr. WILSHUSEN. It is, indeed. Certainly, as you know, FISMA requires that agencies implement cost-effective solutions to mitigate their risks, and one has to make the assessment, is spending this

amount of money on preparing presumably the certification and accreditation documents appropriate?

If it is just to prepare paperwork, that is not really cost-effective—the agency would not be receiving the true value of the execution of the underlying processes that are represented by that paperwork. Primarily, are they assessing the risks? Are they developing and documenting controls that mitigate those risks? And then are they providing the training to staff, to implement those controls, testing and evaluating those controls to make sure that they are operating as intended and are effective? And then remediating deficiencies as those become known?

Those are all activities that are required under FISMA with regard to agencies' information security programs and some of the activities that are required in order to go through the certification and accreditation process. So if the process is just to check off boxes on paperwork, then that is not very useful. The important part is that the agencies are effectively performing these processes in order to implement controls that effectively protect their systems.

Senator CARPER. Mr. Kundra.

Mr. KUNDRA. If I can add to that, I want to make sure as we look at the paperwork that we are seeing here in systems that the State Department is talking about and other agencies, I agree in terms of the fact that the pendulum has definitely swung too much towards a paperwork exercise. But I also want to caution that some of these systems have very sensitive information regarding the personal information of the American people, Social Security numbers, and the processes conducted on these systems are also very sensitive.

So although I recognize that there is a lot of paperwork here, it is very important to make sure that this is also a process that ensures accountability for the business owners in terms of making sure that before a system goes online, have they done a risk assessment? Have they thought about all the risks? Do they have the right controls in place in terms of running the system? Have they made sure that they have back-ups and thought through the processes required to connect this to other systems?

But what has happened, unfortunately, is a lot of agencies are also treating this as a paperwork exercise rather than saying, look, just like if an airplane were to take off, the first flight, you would go through a number of checks, but after it takes off, you need to make sure that you are monitoring all the dials and the gauges to understand where you are in the air. What has happened is, unfortunately, a lot of agencies are substituting and are looking at these processes as a 3-year exercise rather than saying, what do we do on an ongoing basis after the system goes live? What do we do to make sure that we are monitoring risk on a real-time basis?

Senator CARPER. Alright. Mr. Wilshusen, did you want to add anything else?

Mr. WILSHUSEN. Yes, I did. I would just echo what Mr. Kundra mentioned is the fact that it is critical that agencies provide a monitoring capability and test and evaluates the effectiveness of their controls on a regular, current basis, because the threats change, the vulnerabilities change daily. Waiting every 3 years at specific

points in time is not adequately addressing those risks and threats. That is one of the benefits of what Mr. Streufert has done at the Department of State. As he mentioned, he is scanning his systems every 2 weeks to look for certain weaknesses and configuration changes and that is an important control.

Senator CARPER. When there is a penetration, sometimes whoever the penetrator is leaves a back door to allow somebody to come back in later on and create mischief. In a case where that has happened, they have left a back door open. How would your continuous monitoring and updating at the State Department solve that problem, Mr. Streufert?

Mr. STREUFERT. This is a very critical question in Congressman Davis's testimony as well as your own. The problem is that there are back doors and then the action step of deploying the Red Teams that do penetration tests trying to break into the systems. We believe this concern and the practice of penetration tests is so good and worth continuing all across the government and expanding it, as your bill indicates, is that when we did this at the State Department, we found that 80 percent of the successful attacks which were modeled in the penetration test were ethical hacking, as it is called. We invite people to break in, though a surprise to us, but with our understanding that it would be done. Eighty percent of the successful attacks were based on known vulnerabilities.

Senator CARPER. Known to whom?

Mr. STREUFERT. Known to the National Institute of Standards in this National Vulnerability Database that we use for scoring. And so we know those problems are there. I would liken it unto a burglar that can kick through a screen door to get into a system and cause mischief, and once inside, what the penetration tests show is that known vulnerabilities and weak configurations, both referenced by Mr. Wilshusen in his remarks, can allow lateral movement inside the networks.

So it is not that we will be able to prevent every attack. It is that the higher that the risk score is by these methods the National Institute of Standards and DHS have provided to us, the more likely that we will be exposed to a very easy attack. If it is within our control to change, and, in fact, we prove that it is possible at the Department of State over a period of just 12 months to have a significant effect, we should do it as part of our responsibilities of protecting the systems of the government.

Senator CARPER. Alright. Thank you.

Mr. WILSHUSEN. This is consistent with the results of our audits that we conduct at various different Federal agencies in that we often find deficiencies that are related to unpatched systems and other known vulnerabilities that have not been corrected by the agencies. There have been a number of other reports by private organizations that have consistently reported that many successful attacks are based upon known vulnerabilities for which patches have been available, some for 6 months or more. And so it is imperative that agencies take appropriate steps to immediately address those vulnerabilities and mitigate them before they can be exploited.

Senator CARPER. Alright. Thank you.

I should have asked this question sooner, but I didn't. I will go back to it now. Something that you said, Mr. Streufert, kind of triggered this for me. When you look back to Congressman Davis's presentation, some of the comments that he made, is there anything there that you would want to go back and kind of underline as especially important and noteworthy, or something maybe you disagreed with?

Mr. KUNDRA. I think the approach of Red Teams, essentially making sure that the government is focused on constantly trying to find and penetrating our national infrastructure so that we can get ahead of some of these threats, recognizing that if we take an offense when it comes to our defense, we will be in a much better situation than just having a strategy that focuses on defense.

Senator CARPER. OK. Mr. Wilshusen.

Mr. WILSHUSEN. I would agree with Mr. Kundra's remarks. I would also agree with Mr. Davis's remarks related to having an independent evaluation of agencies' information security programs and that it is essential to have IGs be able to examine and review the controls in the programs at their particular agency. Having an independent evaluation is critical, and in my mind, there are opportunities to improve the effectiveness of those evaluations by assuring that they are being performed in accordance with Generally Accepted Government Auditing Standards and that they do, in fact, include testing of the systems on a regular, frequent basis.

Senator CARPER. OK. In other discussions we have had on the issue of cyber security attacks and being ready for them and being able to deter them or turn them back, some of the experts we talk with have suggested that we simply need to do a better job in contracting to make sure that the systems that we are buying as a government, whether it is by agency or Federal Government-wide, that they are better technology, just better able by virtue of the way they are made and provided to the agency to turn back attacks. I wonder to what extent did that play a role in the State Department in terms of replicating, if there are any lessons that we can take from that for the rest of our government.

Mr. STREUFERT. I think that there are many ways that the acquisition process could support this effort, and as we are just in the beginning of the continuous monitoring phase of our security programs in the government, we would want to take note and try to get it right the first time.

One thing that the Department of State has already begun implementing is the idea of associate contractor agreements when we go out and compete our technical services work. This idea was first employed in the Department of Defense with the B–1B bomber, and the idea was that it was functionally necessary for that airplane to hire many different contractors that did the different parts of the airplane. But the question was, would they be invited to work together, and so a clause with associate contractor agreements was placed in the overall contract and all of the subcontractors that they would work together. We believe that this is one of the factors at the State Department that, over time, we will be able to improve by making awards and asking the contractors to work together.

The second element under acquisition, the 20 most important controls or consensus audit guidelines, is a view that many key government and industry professionals in the security field believe that we need tools around each of the 15 of the 20 categories that are susceptible to automated verification at the State Department. Our programs currently only implement about four or five of the 15 areas that are under the continuous evaluation and grading program. So if we awarded a contract that had multiple providers for those 15 tools, then the most compelling and innovative ways that industry would give to the government would be regularly refreshed. So I think a multiple-award contract would be very helpful.

Senator CARPER. Mr. Kundra.

Mr. KUNDRA. The other area I would like to add is as we think about the public-private partnership, it is very important to recognize that we need to approach cyber security from an ecosystem perspective, thinking about what technologies are we buying, how are we buying them, and what are the default settings in a lot of the software and hardware that we procure.

An example would be what we are doing with Microsoft in terms of an operating system strategy, which is that if you look at a Federal desktop core configuration, by fundamentally changing the default settings, because most software companies are going to design software and operating systems and have the default settings so they are extremely easy to use, yet from a public sector perspective, there are a lot of things that we need to change to make sure that we are leaning towards greater security to protect the privacy and security of the American people.

So through this strategy, we have partnered with Microsoft and we actually create a model configuration that prevents a majority of the attack vectors that are out there. And especially as we move towards a new platform with Windows 7, we are working closely with Microsoft through NIST and DOD to make sure that their core configuration is a secure one before we even deploy it across the Federal Government.

Senator CARPER. Alright. Thank you. Mr. Wilshusen.

Mr. WILSHUSEN. I would just like to add that the U.S. Government spends about $70 billion a year on IT products and services. I think that is the correct number. So there is a certain leverage that the Federal Government has when it procures these products and services to require certain minimum security requirements. Certainly that will help potentially enhance the security features on products that it buys and that could also apply to other marketplaces, as well.

Having standard settings and standard requirements can also potentially lead to cost savings, as well. One of the benefits that we looked at when we had our review on Federal encryption efforts was the Smart Buy program over at GSA in which agencies were able to buy cost-effective encryption technologies at almost pennies on the dollar, not quite, but at a huge cost savings because they were able to take advantage of volume discounts. So there are advantages to leveraging the Federal procurement dollar and its acquisition policies.

Senator CARPER. In a day and age when we have seen in the first 8 years of this decade, we literally doubled our Nation's debt, we ran it up by another $1.4 trillion last year, and likely even more this year, every time we can save some pennies on the dollar, that is good. It sounds like in this case it is quarters on the dollar, which is even better.

A couple more questions and then we will wrap it up. This would be a question really for the entire panel. In the current FISMA legislation that we have drafted, Inspectors General must evaluate whether agencies are securing their systems like they say that they are securing them. That means that agencies are spending $1.3 billion to produce the paperwork that the IGs use to evaluate agency effectiveness. IGs then must spend even more time and more money, perhaps another $1 billion or so, to see whether the paperwork was accurate. So the government ends up spending maybe over $2 billion, maybe it is $2.3 billion or so, on a process that is basically flawed. It doesn't make a lot of sense to me, and I don't think to others, as well.

Could each of you just take a couple of moments and tell us what you think the role of the IG should be in cyber security? And maybe better yet, how do we make the partnership between an agency and that agency's IG more proactive, more collaborative, so that we aren't wasting or they aren't wasting so much money? Do you want to go first, Mr. Streufert?

Mr. STREUFERT. Yes, Senator Carper. This is a key question. The first thing we might say is that these products in the three-ring binders here, a systems security plan, a contingency plan, testing plans, test results, these are all important things to do. What the finding of the State Department is, that with the modern tools that are increasingly available since FISMA was put into law, we can do that 72 times more frequently than the 3-year standard of producing these binders.

So the first thing to say is that as we look at the possibility for continuous monitoring, the discussions between the departments and the OIGs could be on data that was as fresh as 15 days old, as opposed to what I will have to do unless there is an adjustment. It will take me a full 8 months to produce these 2,000 pages for the third time when I know that many elements of that data I am already collecting every 2 to 15 days.

I would say that our conversations with the OIG would be stronger if we had common measuring sticks for security, not just in the vulnerability area, which we have already done very well, but many other parts of our security program. And if we had an agreement between the parties that managed the security program of what were the criteria for evaluation in advance, not just within an individual cabinet department but across the entire government, we would be able to compare the relative security between one cabinet department or agency and another.

I think the worst mistake of all we could make, even though the dramatic nature of some of our expenditures of C&As, is to make the mistake of doing less than we are currently doing. So notwithstanding, I would be the first person to say that we should try to use automated means rather than paper. We want to make sure before we set aside the paper methods that we would do our very

best to make sure we have a stronger system than the one that we just left behind.

Senator CARPER. Mr. Wilshusen.

Mr. WILSHUSEN. And I would also agree to a large extent with what Mr. Streufert said, in that many of these documents that are being prepared are not being prepared just for the benefit of the auditor, but, in fact, are being prepared in order to adequately protect the systems that are being covered by those documents.

Now, having said that, certainly auditors have a responsibility to review the effectiveness of security controls, and that includes testing a subset of systems. In our examinations, while we do look at certain documents that are the products or byproducts and artifacts of agency processes, we are also looking at how systems are actually configured and testing the effectiveness of those controls. So it is more than just reviewing documents. It is actually doing a more in-depth review, and that is what IGs are doing and should be doing, as well, in addition to reviewing some of the artifacts that are generated from agency security processes.

Senator CARPER. Alright. Mr. Kundra, you get the last word on this question, and then I have one more separate question for you and we will call it a day.

Mr. KUNDRA. I think it is impossible to confront a real-time threat, such as cyber warfare or adversaries and State actors and organized crime that are actively trying to hack into our systems, with a process that is built around annual reporting, quarterly reporting, or whether you do it on a monthly basis. What needs to happen in terms of the relationship between the IGs and the CIOs is that they need to have greater transparency into the same data and moving toward a real-time platform so they could both see what is happening on a real-time basis and constructively move the security posture of the U.S. Government rather than relying on reports that are created.

By the time that report is printed and handed over to the IG, there is already a new threat factor that is created on a real-time basis. The velocity at which these threats come and the frequency cannot be addressed with a filing cabinet like this.

Senator CARPER. Good point. Thank you.

And the last question, I think I will direct it just to Mr. Kundra unless other panelists think he mis-answers the question, then you can correct him. In your current position, how do you like what you are doing? Are you enjoying it? Is it challenging? Do you ever get to go home at night?

Mr. KUNDRA. It is great. Very little sleep, but it is an enormous opportunity to serve the country and to advance the President's technology agenda.

Senator CARPER. Alright. Good. In your current position, I think you are maybe the person responsible for overseeing the effectiveness of our Federal Government's cyber defense, and that is a government, as we know, that is composed of hundreds, maybe thousands of different systems. I am told that you have relatively few, if any, cyber security experts that work for you and I find that of concern, maybe even troubling.

But I find it even more troubling that OMB, which is known for their budget prowess, has never asked for a detailed accounting of

what an agency spends on cyber security. I don't know if that is true, but if it is true, why do you think it has been the case? Why hasn't OMB, as far as I know, ever said, well, what are you all spending for cyber security? And to follow up, if that is true, are you going to do anything to correct that situation?

Mr. KUNDRA. Sure. So that was actually one of the most shocking things when we tried to do analysis as far as cyber security was concerned. One was that the information that was being submitted to OMB was being submitted in these spreadsheets, hundreds of spreadsheets that were being mailed in.

Two was, from a cost perspective, what was being collected was aggregate security information. So what we did immediately is for the 2009 report, we are getting to the detailed cost allocation when it comes to information security, so we know where is the government spending when it comes to products, human capital, and specifically computer network attacks (CNAs). And unfortunately, with a lack of that information, what we aren't able to do is effective comparative analysis between one agency and another, and more importantly, a deeper understanding of how do our investments line up with our vulnerabilities and where do we need to make those appropriate investments.

But we are working very closely with DHS and the U.S. Computer Emergency Readiness Team (US-CERT) specifically, and as part of the FISMA reporting requirements in CyberScope, we are going to be collecting all that data.

Senator CARPER. If you will all just bear with me for one moment, please.

[Pause.]

Senator CARPER. I know I said the last question was the last question. I am going to try to squeeze one more in here before we let you go. Again, this is for Mr. Kundra, and if others want to chime in, go ahead.

I think OMB has the ability to ask agencies if they would follow a model similar to that of the Department of State. Do you think that conducting a pilot, or maybe having a number of agencies basically say, we want you to follow something similar, do you think that is a good idea? Maybe it is something you have given some thought to, or maybe you are planning on doing it, or maybe you don't think it is a good idea, but would you just think out loud for us on that?

Mr. KUNDRA. Sure. I actually think it is a great idea. That is one of the reasons the State Department is actually talking to the Veterans Administration. It is making the tool, the software actually available to NIST and DHS, also, to figure out how can that be scaled, recognizing that across Federal agencies, HHS is going to have a very different environment. But what is going to be common is they all have desktops, certain network infrastructure, from routers to switches, and figuring out how can we make sure that we are not duplicatively spending money and creating new tools if we can leverage best practices across a Federal Government.

From an OMB perspective, it is very important for us to get the threat matrix across the entire Federal Government. So how do we roll up this information at a DHS level so we get a real-time posture from a security perspective?

Senator CARPER. OK. Do you all want to comment at all on what Mr. Kundra said? You don't have to, but if you would like to, you are welcome to do so. Did he do OK?

Mr. STREUFERT. Yes. We very much appreciate the leadership of Mr. Kundra and OMB on the issues of CyberScope to make our reporting more efficient, and his very early willingness to look at issues like dashboards. I think that our collective commitment should be to one of continuous improvement. The State Department has some ideas on this and we have worked on it some. We want to share that with others. But I believe what will happen is Vivek invites, and he already has done so, conversations more widely in government that good ideas will come from all of the cabinet departments that we will be well served to fold in and come up with the strongest possible product as a government together.

Senator CARPER. OK. I think we will wrap it up at this point. I have another hearing that started at 9:30 this morning that is still going on on climate change legislation. It will be a full day.

A couple of thank yous. One to Mr. Streufert, to you and your colleagues. I know you said it is not just you, there are a lot of people involved at the State Department that are responsible for the progress that is being made there and for the example that you are able to provide for other Federal agencies. But thank you for your leadership, and our commendation is to you and to your colleagues. As we used to say in the Navy, Bravo Zulu.

I want to thank Mr. Wilshusen for the report that we received from you and your colleagues on cyber security metrics. It is one I requested, I believe last year, but thanks for that report.

And Mr. Kundra, thank you for taking on this responsibility and giving it 110 percent, maybe more than that.

We are going to stay on this. We are going to push forward on the legislation and get it enacted if we can. I know the Chairman and Ranking Member of the full Committee on Homeland Security and Governmental Affairs are interested in passing even more comprehensive legislation on cyber security, and there is some discussion of folding our piece into that, or maybe moving what we are doing on its own if we want to try to get it out there and moving along.

But thank you for helping inform our legislative path just a little bit better today. I would encourage, Mr. Kundra, for you and our friends at OMB to use this model that works and other models that work and to replicate that success.

But maybe one or two points that I will make, and maybe I am being redundant, but I will go ahead and make them anyway. I think repetition can be helpful.

But the first point is we are spending way too much money on a process that is flawed from the beginning. That is not to take anything away from Congressman Davis and others who were involved in the FISMA legislation from 2002, but it is a process that is flawed. Writing a report about security is not the same as investing in security, and with so much at stake, we should be doing a much better job.

The irony of it is, we had a luncheon speaker at our weekly caucus luncheon today who runs a big Federal agency and he shared with us just some up-to-date information about the kind of attacks

that are underway every day, every hour, every minute. It really puts this in real time and with a real sense of urgency.

My next point is the fact that OMB is, I think, the only one who really can make this happen absent Congress passing a bill. I would again say, Mr. Kundra, actually take a hard look at what you can do, and I sense that you are already doing that, to make sure that we don't waste another year, another $1 billion, if not more, to do something that doesn't work very well.

My last point is the fact that, obviously, that we all need to work together. I am pleased to see with the three of you here before us, it is a pretty good model of how we can cooperate and I hope that we are part of that, as well. But technology changes so fast that without a partnership between—not just among agencies, but also between the Legislative Branch and the Executive Branch, Americans, unfortunately, are going to end up on the losing end, and we don't want that to happen.

I am going to ask, I think, for you all to come back to me, I will put this in writing, but to come back to us in maybe 2 weeks with opportunities that you believe will lead to efficiencies in defending our networks. If you do that, I would be grateful. If you get any other questions from my colleagues, then if you would respond to those within 2 weeks, that would be terrific.

Thank you all very much for coming today, for your testimony, and for the work that you are doing. I would encourage you to continue on and we will do our best to have you back. Thank you.

And with that having been said, this hearing is adjourned.

[Whereupon, at 4:07 p.m., the Subcommittee was adjourned.]

APPENDIX

FOR IMMEDIATE RELEASE

TOM CARPER

UNITED STATES SENATOR · DELAWARE

FOR IMMEDIATE RELEASE: Oct. 29, 2009
CONTACT: Katinka Podmaniczky (202) 224-2441

Statement of Senator Thomas R. Carper, Chairman

Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security

Committee on Homeland Security and Governmental Affairs

"More Security, Less Waste: What Makes Sense for our Federal Cyber Defense"

The issue of "Cyber Warfare" isn't science fiction anymore. It's reality. Over the past few years we have heard alarming reports that criminals, hackers and even foreign nations have deeply penetrated our government's most sensitive networks, including the offices of some of us right here in Congress. In fact, just last week the congressionally established U.S.-China Economic and Security Review Commission reported that China is strategically developing offensive capabilities that could be used against us in a future military conflict.

Further, there have been reports that some of the previously successful cyber attacks against agency networks may have left behind what's known as a "backdoor," essentially a technological means for the bad guys to get back into our networks without anyone knowing.

These vulnerabilities could be used against us by those who might want to do us harm by stealing sensitive information stored on military networks or shutting down critical networks when we need them the most. Imagine the terrifying scenario of a hacker creating uncertainty as to the validity of the data residing on the Federal Aviation Administration's Air Traffic Control systems.

That is exactly the kind of scenario I hope our hearing today helps prevent.

But, the threat of a cyber attack isn't something new. In fact, in 2002 Congress passed what is known as the "Federal Information Security Management Act" – or FISMA for short – to help prevent many of the problems we will be discussing today. FISMA brought greater attention to the issue of cyber security and helped establish greater accountability within agencies. Overall, it was a step in the right direction.

However, seven years after the passage of FISMA and approximately $40 billion later, I am troubled to learn that the Office of Management and Budget does not track how much agencies spend on cyber security or measure whether those expenditures actually resulted in improved security.

And even more troubling, agencies may be constrained from implementing the most basic of cyber security best practices because of inflexible requirements. Allow me to put that into perspective, federal agencies have spent more on cyber security than the entire Gross Domestic Product of North Korea, who some have speculated is to be involved with some of these cyber attacks.

That is simply unacceptable.

Some of the problems with FISMA implementation are a direct result of OMB's decisions over the years, while others are due to agency neglect. Still other problems lay at the feet of those of us here on Capitol Hill. In essence, we all share in the blame. However, at today's hearing we have an opportunity to discuss some concrete ways to correct some of those wrongs.

For example, one wasteful and ineffective area that OMB and agencies can target is what is known as the "Certification and Accreditation" process. A Certification and Accreditation is essentially a process whereby agencies evaluate every three years what defensive security protections are in place to prevent attacks on their key systems. The process costs taxpayers about $1.3 billion every year and it produces a good deal of paperwork that ends up stored in binders in some clutter-filled room.

If we look at the chart to my right, we can see three years worth of reports from the Department of State, which cost a total of $38 million dollars. These reports would be worth the price tag if the tactics that hackers used were as static as words typed on a piece of paper.

But hackers change how they attack us daily and their numbers continue to grow.

And yet it seems like OMB thinks that a snapshot of agency preparedness every three years will defend our critical networks. But instead, billions of dollars are spent every year on ineffective and useless reports, similar to the ones pictured here. Meanwhile, we continue to get attacked. However, testifying today will be a representative from the Department of State who saw an opportunity to spend his agency's cyber security budget more wisely.

Instead of spending money on ineffective paper-based reports, the State Department decided to focus on developing a system that monitored their global networks on a continual basis. If we take a look at the second chart on my right, we can see the results of their hard work. According to the State Department, they were able to reduce the amount of risk to their agency by 90 percent in a single year. I'm told that this was achieved by developing a system that makes sense, uses effective metrics, and holds people accountable. In essence, the Department of State can prove they have better security at a fraction of the cost.

So as we progress through the hearing, I would like our witnesses to keep in mind that moving to a model like the one at State Department requires no new legislation, cost less than or the same as the current paperwork-laden method, and will better protect our country. That's the kind of cyber security that makes sense.

In fact, my colleagues and I introduced a bill last session, and again this year, which would require all agencies to move to a proactive approach like the one the State Department has taken. In addition to requiring continuous monitoring of security controls and putting a strengthened Chief Information Security Officer in each agency, my bill would enhance the role of the Department of Homeland Security in cyber security. The department would share information with agencies on where cyber attacks have been successful so that they can better prioritize their security enhancements. Further, my bill would require agencies to use their enormous purchasing power to persuade vendors to develop and sell more secure IT products and services in the first place.

###

STATEMENT OF SENATOR JOHN MCCAIN, RANKING MEMBER

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

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

Hearing on "More Security, Less Waste: What Makes Sense for Our Federal Cyber Defense"

October 29, 2009

Senator Carper, thank you for holding this hearing today. As the sixth annual Cybersecurity Awareness Month comes to a close, it is an appropriate time for this subcommittee to examine how we measure the effectiveness of cybersecurity policies and procedures at our federal agencies.

The federal government relies heavily on complicated information systems for day-to-day operations. The risks posed to those systems have never been higher. Cybercrime and cyber espionage are on the rise. Indeed, nation-states seek to exploit our government networks, to steal sensitive intelligence or intellectual property for military and industrial advantage. A report prepared just this month for the bi-partisan US Chinese Economic and Security Review Commission concludes that the Chinese have made it a military priority to target the US Government and industry as part of a "long term, sophisticated, computer network exploitation campaign."

Recognizing these threats, the federal government is spending billions of dollars on information technology security each year. OMB estimates $6.2 billion was spent in fiscal year 2008 alone, nearly 10% of the entire cost of the federal IT investment portfolio.

Agencies spend a large percentage of their security budget and manpower on collecting data on compliance. Compliance with security standards and training mandates are necessary and can be useful for providing accountability and oversight.

Many experts, however, argue that these polices simply require that agencies have a security plan but do not measure that plan's effectiveness. This process has been described as a multi-million dollar paperwork exercise that certifies only that appropriate security measures are in place at a fixed point in time. In other words, a closet full of reports about the security of IT systems yesterday does not necessarily tell us how secure those same systems are today.

As we keep reading in media reports, the sophistication, frequency, and speed at which new cyber threats emerge have increased exponentially in just the last five years. To combat emerging cyber threats requires a continuous reevaluation of security priorities based on current risk. Agencies should not spend finite resources on reports that are outdated as soon as they are published. Most experts agree that only the continuous monitoring of security controls will both ensure compliance with federal policy and also achieve the accountability and real-time situational awareness that is critical for protecting our government networks.

I look forward to an informative discussion with our witnesses on new approaches that may accomplish that goal cost effectively.

Thank you Mr. Chairman.

More Security, Less Waste: What Makes Sense for our Federal Cyber Defense

Statement of Former Representative Tom Davis before the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security

October 28, 2009

Chairman Carper, Ranking Member McCain, I appreciate your efforts to improve information security and am grateful for the opportunity to testify here today.

For 14 years I represented the 11th District of Virginia; I was also honored to serve as a member of the House Committee on Oversight and Government Reform, first as chair of the District of Columbia subcommittee, then as chair of the Technology and Procurement Policy Subcommittee, and finally as chairman and ranking member of the full committee.

My congressional service coincided with the proliferation of the Internet and the explosion of new capabilities that came along, for both the public and private sector. It was clear the revolution in interconnectivity had the potential to fundamentally change governmental operations and service delivery; however, it also created a new form of vulnerability, one in which traditional protections of geographic distance and physical strength were irrelevant. For these reasons, I made information technology, management and security a focus of my work in Congress.

Federal agencies needed to take this threat seriously and ensure proper procedures and tools were in place to protect information systems. Similarly, Congress needed a clear picture of the information security posture of the federal government in order to conduct effective oversight. The Federal Information Security Management Act (FISMA), which I championed in 2001 and 2002, was intended to help provide such a framework.

FISMA requires federal agencies, under the direction of the Office of Management and Budget, to create a comprehensive, risk-based approach to information security management. It further requires annual IT security reviews, reporting and remediation planning at federal agencies. These requirements were based on best

practices and, in addition to safeguarding information, were intended to make security management an integral part of an agency's operations.

At the time FISMA was enacted, no coordinated priority existed to address the threat of cyber attacks. Technology was evolving rapidly. Rather than taking a prescriptive approach, we believed agencies needed to walk before they could run, and putting procedures and protocols in place was an important first step in protecting government's critical infrastructure.

Since its enactment, FISMA has undoubtedly served to elevate the importance of information management and information security in government, and I am proud of the progress the federal government has made through FISMA implementation. That said, there is room for updates and improvement. It is time to take FISMA to the next level.

While I believe the requirements FISMA enumerated would be components of any sound information security plan, the need at present is to "operationalize" its implementation. This would involve tools such as "red team" penetration tests. It would also require appropriate performance measures, such as the time between a penetration and detection; the time to deploy a security patch once it has been released; and the time to complete a root cause analysis when a security breach does occur.

I am pleased your language references both penetration tests and performance measures.

Three other key ingredients: Responsibility, Authority and Accountability.

Chief Information Security Officers (CISOs) may be responsible for overall information security planning, but they cannot just be the bag men when things go wrong. Responsibility for an information security program permeates an organization, from the head of the agency to every employee. Most of the security breaches that have grabbed headlines in recent years aren't the result of some evil cyber genius, but federal employees failing to adhere to basic security protocols. A lost laptop, a stolen Blackberry, computers never returned when an employee leaves an agency – these can result in the personal information of untold thousands being put at risk. CISOs might have to come up with the protocols, but the rank

and file have to adhere to them. As Congress looks at information security issues, it might be wise to consider uniform procedures, training and penalties to reduce theft, loss or other adverse events.

Your language gives CISOs authority to develop, implement and enforce security measures. That's important. There also have to be consequences, good and bad, for failures and successes -- that's one aspect of the accountability component. The private sector provides some models. For example, the payment card industry mandates compliance with standards set by the PCI Security Standards Council. Failure to adhere to these standards results in a business losing the ability to conduct transactions with payment cards. That exact example isn't going to fit the federal system, but we need a system of carrots and sticks that promotes compliance and punishes negligence.

Another aspect of accountability deals with funding. Federal government spending has risen sharply in recent years, but to what end? We have to link performance, in this specific instance performance of information security products and services, with spending decisions. Simply asking for more, or providing more, isn't going to fix the problem, nor is it serving the interests of the American people.

In closing, I would like to reiterate my appreciation for the work you are doing on information security. The Information Age is indeed a strange new world in which a mischievous teenager could be as dangerous as a terrorist organization or malevolent government. I am committed to helping however I can to make sure our federal systems are up to the task and that our oversight mechanisms are commensurate to the need.

STATEMENT OF VIVEK KUNDRA
FEDERAL CHIEF INFORMATION OFFICER,
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

October 29, 2009

More Security, Less Waste: What Makes Sense for Our Federal Cyber Defense

Good afternoon Chairman Carper, Ranking Member McCain, and members of the Subcommittee. Thank you for the opportunity to testify on the state of Federal information security.

Our Nation's security and economic prosperity depend on the stability and integrity of our Federal communications and information infrastructure. As stated in *The Cyberspace Policy Review*, the 60-day clean slate look at cyber activities ordered by the President, threats to cyberspace pose some of the most serious economic and national security challenges of the 21st century for the United States. The group of State and non-state actors who target U.S. citizens, businesses, and Federal agencies is growing. US-CERT, the computer response center for civilian agencies, sees millions of attempts daily to access open ports and vulnerable applications on Federal networks.

Historically, the Federal Government has not been as effective as necessary in its cyber defense. An inadequate cyber security workforce, a focus on compliance rather than outcomes, and a cumbersome and time-consuming process for collecting information regarding agency security postures have hindered our cyber security management capabilities.

To address these issues, OMB has taken the following actions:

- Expedited hiring authority for 1,000 cyber security positions at the Department of Homeland Security;
- Launched CyberScope, an automated, streamlined platform for secure reporting to replace the old, less secure manual process for the collection of agency cyber security information;
- Created a taskforce comprised of representatives of the Federal CIO Council, which includes the CIOs of civilian agencies, the Department of Defense, and National Intelligence Community; the Council of Inspectors General on Integrity and Efficiency; the National Institute of Standards and Technology; the Department of Homeland

Security; and the Information Security and Privacy Advisory Board to develop new reporting metrics that focus on outcomes not processes; and

- Required agencies to report detailed cost information on security spending beginning with FY 2010.

The Road to FISMA

The cyber security environment in the Federal Government has been in constant evolution, due to the ever-changing nature of technology as well as the need to meet the increasingly complex threats we face. Over the past twenty years, Congress has enacted legislation to address these complex issues.

The Computer Security Act of 1987 sought to improve the security and privacy of sensitive information in Federal computer systems and to establish acceptable security practices for such systems. However, information technology was not considered a critical part of the management agenda for Federal agencies. It was not until 1996, with the passage of the Clinger Cohen Act, that the position of the Chief Information Officer (CIO) was created across Federal agencies, recognizing the need for a single executive to lead information technology at each agency.

In 1999, Y2K highlighted our reliance on the information technology that powers our digital economy. The Government Information Security Reform Act (GISRA) of 2001 established information security program evaluation, and reporting requirements for Federal agencies yet sunset by 2002. Recognizing the Nation's continued dependence on IT, Congress passed the Federal Information Security Management Act (FISMA) in 2002.

The Current State of FISMA Implementation

In the seven years it has been in place, FISMA has raised the level of awareness of the critical importance of information security in the agencies and in the country at large. It has also strengthened agency reporting requirements and established mechanisms for the collection of agency information. For example, based on agency FISMA submissions, security awareness training has become prevalent across the Federal Government for employees and contractors. Agencies and departments are now reporting inventory numbers for their systems, and CIOs play a critical role in managing information security in the agencies. However, continued progress must be made to realize FISMA's full vision of a secure and vigilant Federal Government.

When FISMA was first enacted, OMB approached the question of metrics by concentrating on compliance. During the first few years of FISMA reporting, the required metrics evolved as initial benchmarks were met.

These metrics were lagging indicators focused on compliance rather than outcomes. Agencies reported infrequently and, in many cases, only annually. This occurred in an environment where threat vectors change daily. Moreover, the information collected does not reflect the readiness of the agencies to deal with the reality of modern threats. Even information

as basic as the cost of compliance or the number of days to apply a critical patch is not readily available.

The economic prosperity of our Nation relies upon, and is powered by, the digital infrastructure. Yet, security in the Federal Government is not where it needs to be. The Nation's approach to cyber security over the past 15 years has failed to keep pace with mounting threats. We are taking actions to improve the situation but are only at the beginning of what needs to be done. The Federal Government must remain committed to protecting the digital infrastructure upon which we so heavily depend.

I) EXPANDING THE WORKFORCE

As the Department of Homeland Security (DHS) grows into its role of protecting the homeland in cyberspace, it must have a skilled workforce capable of securing networks, understanding the threats we face, and assisting Federal agencies in defending their networks. Recently, OMB worked closely with the Office of Personnel Management to extend special hiring authority to DHS to meet its growing needs.

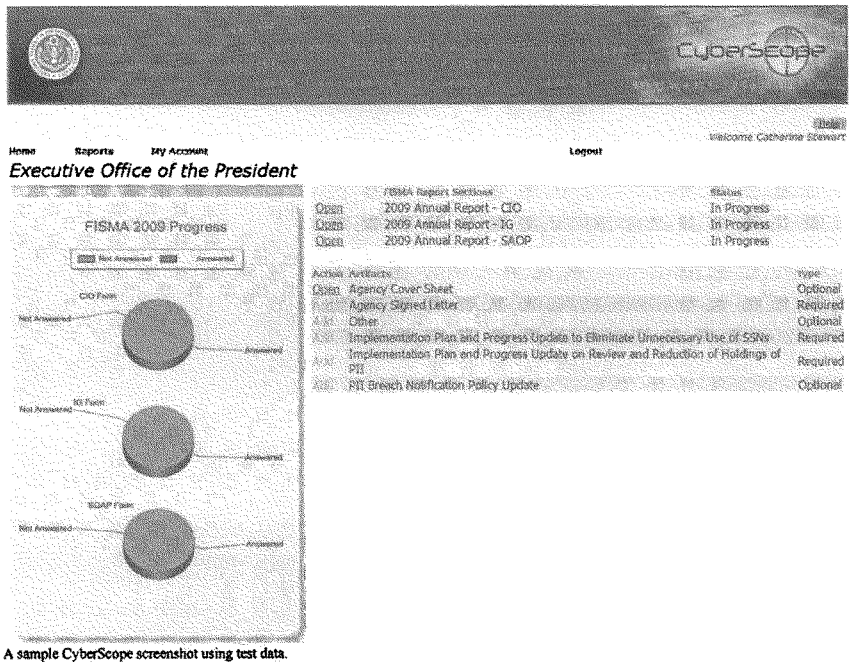
On October 1, 2009, DHS Secretary Janet Napolitano announced that DHS has the authority to hire up to 1,000 new cyber security professionals over the next three years to fill staffing gaps at various DHS agencies. DHS will look to fill critical cyber security roles including: cyber risk and strategic analysis; cyber incident response; vulnerability detection and assessment; intelligence and investigation; and network and systems engineering. This new hiring authority will enable DHS to recruit skilled cyber analysts, developers and engineers to serve their country by helping to secure the nation against cyber threats.

II) CYBERSCOPE: A MODERN PLATFORM FOR FISMA REPORTING

Prior to the 2009 reporting cycle, OMB received via email over 100 individual spreadsheets from agencies and paper copies of the Inspector General reports in response to FISMA reporting requirements. It took three FTEs working for a full month to compile and analyze the data submissions. This manual spreadsheet process was laborious, time consuming, and unsecure. Furthermore, the lack of meaningful analysis, the vulnerable reporting methodology, and the manual nature of the process inhibited clear, timely, and comprehensive insight into the security posture of the Federal Government's information technology systems.

On October 19, 2009,O MB launched an interactive data collection tool—CyberScope—enabling agencies to fulfill their FISMA reporting requirements through a modern digital platform.The broad range of meaningful information collected, the use of secure two-factor authentication, and the online access to data provides for a more efficient and effective reporting process.

In spring of next year, OMB will unveil a cyber security dashboard, unlocking the value of agency FISMA submissions in a timely, comprehensive, and secure manner. The streamlined collection format allows for better research and reporting across Federal agencies, OMB, and GAO.



A sample CyberScope screenshot using test data.

Rather than relying on unencrypted emails and unprotected spreadsheets, CyberScope requires users to login via a secure identity card and an accompanying unique PIN number.[1] The use of the PIV card for logging into CyberScope is the first time this credential has been used for a Government-wide system.

CyberScope empowers its 600 estimated agency users to manage their internal reporting and information collection processes as best suits their individual needs. OMB conducted training sessions prior to the launch of CyberScope and utilized much of the feedback to improve the system. Going forward, CyberScope's extensible platform is the performance-based solution to years of inefficient and unsecure collection of agency security data.

Although the agency focus to-date has been on compliance, some agencies have adopted a performance-based approach. For example, the Department of State (DoS) is one such agency. DoS faces unique security challenges as it serves both domestic employees and U.S. officials at embassies and consulates worldwide. The DoS network supports 285 foreign posts and consists

[1] The Personal Identity Verification (PIV) card was mandated for use by all Federal employees by Homeland Security Presidential Directive 12 (HSPD-12).

of 5,000 routers and 40,000 hosts. Although ultimate responsibility and accountability resides with the CIO, individual posts have a degree of responsibility for management of the network.

To provide better insight into its security posture, DoS has moved to a security dashboard. Cyber security information is gathered through automated processes and is integrated into a central database. In some cases, data are accessed on-demand directly from source systems. DoS also uses a scoring process based on a set of ten groups of criteria spanning from scans to security settings to the vulnerability of a host. Because scores are visible to other system managers across the agency, the system fosters an atmosphere of peer-based competition.

DoS' use of a security dashboard provides its CIO and other senior managers secure access to meaningful, dynamic data, ultimately yielding better insight into its security posture and enhanced protection for its networks.

III) PERFORMANCE-BASED METRICS

What gets measured gets done; metrics are policy statements. As long as OMB metrics continue to measure compliance, agencies and departments will continue to march toward that goal. However, we can never get to security through compliance alone.

In September 2009, OMB established a task force to develop new, outcome-focused metrics for information security performance for Federal agencies. To solicit the best ideas, OMB has reached out across the Federal community, as well as to the private sector. This task force is concentrating on developing metrics that will advance the security posture of agencies and departments. Understanding that metrics are a policy statement about what Federal entities should concentrate resources on, the task force is developing metrics that push agencies to examine their risks and make substantial improvements in their security.

Participants in the task force include: the Federal CIO Council, which includes the CIOs of civilian agencies, the Department of Defense,a nd Office of the Director of National Intelligence; the Council of Inspectors General on Integrity and Efficiency; the National Institute of Standards and Technology; the Department of Homeland Security; and the Information Security and Privacy Advisory Board. In addition, the Government Accountability Office (GAO) serves as an observer to this taskforce.

The task force is currently developing forward-looking metrics focused on improving security at agencies rather than merely demonstrating compliance. Additionally, the task force is working with OMB to develop a roadmap for future reporting under FISMA which will incorporate real-time metrics and enhance Government-wide situational awareness.

OMB plans to release for public comment the draft metrics for FY 2010 reporting later this fall. Upon receipt and analysis of comments, OMB will release the final metrics for FY 2010 reporting and the roadmap for future reporting efforts in the first quarter of 2010. Agencies will report on performance-oriented metrics in the fall of 2010.

As part of this effort, OMB is also working on a roadmap for the future. As other cyber security activities progress, such as the Comprehensive National Cybersecurity Initiative

(CNCI), OMB is considering the role and participants of security information collection. For example, more frequent reporting of outcome based metrics, near or at real-time, is imperative for developing situational awareness across the Federal enterprise.

IV) IMPROVED INSIGHT INTO THE COST OF SECURITY

In FY 2010, for the first time, we are asking agencies for detailed cost estimates and the actual amounts spent on security. Historically, as part of the annual budget process, agencies reported only the percentage of spending related to cyber security for each IT investment. However, this was not broken down into distinct categories, such as personnel costs, reporting costs, certification & accreditation (C&A) costs, and security management costs. The only other cyber security-related cost data point collected was the amount spent for training by the agencies. This lack of detailed information precludes the level of meaningful analysis needed to assess the efficiency and effectiveness of Federal information security spending.

Recognizing that the best security is "baked in" to information technology investments and not added in separately, we know that this is the beginning of the process of obtaining relevant cost data. Analysis of the preliminary cost data will be provided in the FY 2009 FISMA Report to Congress, to be delivered in March 2010.

In the coming years, access to this data will allow OMB to evaluate the efficiency of the Federal expenditure on security. Right now, we cannot answer key questions such as: "Are we spending too much on certification and accreditation, considering its benefits?" Even basic questions, such as, "How many cyber security employees are there across the Federal Government?" are unknown. Collection of detailed information, especially when combined with the performance-based metrics, will allow both OMB and agency management to make informed, risk-based decisions on where to allocate scarce resources.

Closing

From the launch of CyberScope to the hiring of up to 1,000 new DHS cyber security experts, the Administration is committed to strengthening our Federal cyber defense. The actions we are taking will both enable critical insight into agency security postures and help enhance protection of our nation's systems. Ultimately, this will lead to more effective, efficient, and secure IT across all Federal agencies.

The threats we face are numerous, evolving faster than our cyber defense, and have the potential to do great harm. A secure, trusted computing environment in the Federal Government is the responsibility of everyone involved from the agency heads to those charged with oversight. It entails employees, contractors, and the American people working together to create a culture of vigilance and security to enable us to continue to efficiently leverage the power of technology. This will not be easy nor will it take place overnight. Our current actions represent important steps towards a stronger Federal cyber defense, but we must remain ever-vigilant.

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
Thursday, October 29, 2009

INFORMATION SECURITY

Concerted Effort Needed to Improve Federal Performance Measures

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-10-159T

Mr. Chairman and Members of the Subcommittee:

Thank you for the opportunity to participate in today's hearing on how agencies can establish cost-effective cyber defense. My statement today is based on our report titled *Information Security: Concerted Effort Needed to Improve Federal Performance Measures*, which is being released at this hearing.[1]

Cyber security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. Organizations are faced with a variety of information security threats, such as fraudulent activity from cyber criminals, unauthorized access by disgruntled or dishonest employees, and denial-of-service attacks and other disruptions. The recent dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology all contribute to the urgency of ensuring that adequate steps are taken to protect the federal government's information and the systems that contain and process it.

The Federal Information Security Management Act (FISMA), which was enacted in 2002, sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. The act assigns specific responsibilities to federal agencies, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). It also requires agencies and OMB to annually report on the adequacy and effectiveness of agency information security programs and compliance with the provisions of the act. To help meet these requirements, OMB established a uniform set of information security measures that all federal agencies report on annually.

Mr. Chairman, in light of questions about whether or not agencies are measuring the right things in securing their systems, you requested that GAO examine how organizations develop and use

[1]GAO-09-617 (Washington, D.C.: Sept. 14, 2009).

metrics to assess the performance and effectiveness of information security activities. In response to your request, our report and my statement provide (1) a description of key types and attributes of performance measures; (2) information about the practices of leading organizations for developing and using measures to guide and monitor information security control activities;[1] (3) information on the measures used by federal agencies to guide and monitor information security control activities and how they are developed; and (4) an assessment of the effectiveness of the measures-reporting practices that the federal government uses to inform Congress on the effectiveness of information security programs. In conducting this work, we collected and analyzed information from leading organizations, security experts, NIST, 24 major federal agencies, and OMB.[2] Our work for this report was performed in accordance with generally accepted government auditing standards.

In brief, Mr. Chairman, leading organizations and experts have identified different types of measures that are useful in helping to achieve information security goals. While officials categorized these types using varying terminology, we concluded that they generally fell into three types: (1) compliance, (2) control effectiveness, and (3) program impact. These types are consistent with those laid out by NIST in its information security performance measurement guide.[4] In addition, while information security measures can be grouped into these three major types, organizations and experts reported that all such measures generally have certain key characteristics, or attributes. These attributes include being (1)

[1]For the purposes of this report, "leading organizations" refers to prominent, nationally known organizations, academic institutions, and state agencies that have implemented comprehensive enterprisewide information security programs.

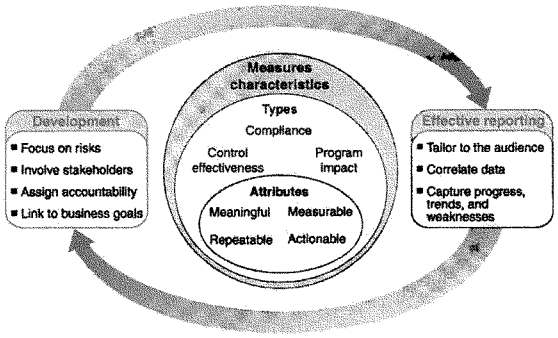
[2]The 24 major federal agencies are the Agency for International Development; the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans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

[4] National Institute of Standards and Technology, *Performance Measurement Guide for Information Security*, NIST Special Pub. 800-55 Revision 1 (Gaithersburg, Md.: July 2008).

measurable, (2) meaningful, (3) repeatable and consistent, and (4) actionable.[6]

Further, these organizations and experts indicated that the successful development of information security measures depends on adherence to a number of key practices, including focusing on risks, involving stakeholders, assigning accountability, and linking to business goals. Additional practices are critical to ensuring that the measures are useful in effectively conveying information to operational managers, executives, and oversight officials. These include tailoring measures to the audience; correlating data; and capturing progress, trends, and weaknesses. Figure 1 illustrates the interrelationship of these key practices with the key characteristics.

Figure1: Measures Development and Use Cycle



Source: GAO.

[6] Although we focused on identifying attributes and practices for measuring the performance of information security programs, our findings conformed closely to our prior work on effective performance measurement and reporting practices for the federal government in general. See, for example, GAO, *Managing for Results: Enhancing Agency Use of Performance Information for Management Decision Making*, GAO-05-927 (Washington, D.C.: Sept. 9, 2005).

We determined that federal agencies have not always followed key practices identified by leading organizations for developing information security performance measures. While agencies have developed measures that fall into each of the three major types (i.e. compliance, control effectiveness, and program impact), on balance they have relied primarily on compliance measures, which have a limited ability to gauge program effectiveness. Agencies stated that, for the most part, they predominantly collected measures of compliance because they were focused on measures associated with OMB's FISMA reporting requirements. In addition, while most agencies have developed some measures that include the four key attributes identified by leading organizations and experts, these attributes were not always present in all agency measures. Further, agencies have not always followed key practices in developing measures, such as focusing on risks.

Lastly, we determined that OMB's measures did not address the effectiveness of several key areas of information security controls, including, for example, agency security control testing and evaluation processes. There is no measure of the quality of agencies' test and evaluation processes or results that demonstrate the effectiveness of the controls that were evaluated.[4] In addition, OMB's report to Congress does not fully employ key practices for reporting and thus provides limited information about the effectiveness of agency information security programs.

We made five recommendations to OMB to assist federal agencies in developing and using measures that better address the effectiveness of their information security programs:

- issue revised guidance to chief information officers for developing measures;

[4] OMB does require agency inspectors general to assess agencies' certification and accreditation process; however, the assessment may or may not include an assessment of security control testing and evaluation processes. Further, OMB does not provide a transparent depiction of how an assessment of an agency's security control testing and evaluation process contributes to the overall certification and accreditation quality rating.

- direct chief information officers to ensure that measures exhibit key attributes;
- direct chief information officers to employ the key practices for developing a measure as identified by leading organizations;
- revise annual FISMA reporting guidance to agencies; and
- revise the annual FISMA report to Congress to provide better status information on the security posture of the federal government.

Implementing these recommendations will help to focus attention on activities that will enhance the effectiveness of agency information security controls and improve the cyber defense of federal computer systems and information. In providing oral comments on a draft of the report, representatives of OMB's Office of E-Government and Information Technology stated that they generally agreed with the contents and recommendations of the report.

Mr. Chairman, this concludes my prepared statement. I would be pleased to respond to any questions that you or other members of the subcommittee may have.

For questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Individuals making key contributors to this testimony include Ashley Brooks, John de Ferrari, Season Dietrich, Neil Doherty, Ronalynn Espedido, Min Hyun, Anjalique Lawrence, Joshua Leiling, Lee McCracken, and David Plocher.

Statement of John Streufert

Chief Information Security Officer /
Deputy Chief Information Officer for Information Security

Bureau of Information Resource Management
United States Department of State

Senate Subcommittee on Federal Financial Management, Government Information,
Federal Services, and International Security,

Committee on Homeland Security and Governmental Affairs

More Security, Less Waste:
What Makes Sense for Our Federal Cyber Defense

342 Dirksen Senate Office Building
October 29, 2009
2:00 p.m.

VerDate Nov 24 2008 11:34 Oct 25, 2010 Jkt 053852 PO 00000 Frm 00055 Fmt 6601 Sfmt 6601 P:\DOCS\53852.TXT SAFFAIRS PsN: PAT

Good afternoon Chairman Carper, Ranking Member McCain, and distinguished Members of the Subcommittee:

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

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

The Current Landscape from the Perspective From a Civilian Department

FISMA Benefits. The passage of the Federal Information Security Management Act in 2002 served as a game-changing event for the federal agency community. Whereas, the Health Information Portability and Accountability Act applies to medical information and the Privacy Act of 1974 applies to personal information, FISMA applies to all information used by or on behalf of the federal department and agency. The establishment of a holistic information security program and the responsibility of accounting to oversight entities, including Congress, served as a valuable check in determining the health of an agency's information security program.

Challenges Faced. The federal cyber landscape has changed the past five years. The implementation of federal cyber security has typically been implemented through manual

processes and compliance checks like: (1) conducting an "annual" inventory of systems; (2) testing security controls not less than "annually" , (3) reporting "quarterly" reports of weaknesses to OMB, (4) conducting awareness training "once a year" and (5) performing Certification and Accreditation (C&A) studies every "three" years.

Meanwhile our cyber problems have dramatically escalated in severity and frequency. In a typical week, the Department blocks 3.5 million spam e-mails, intercepts 4,500 viruses and detects over a million external probes to our network. Of that number in the past two years the percentage of malicious code attacks recorded at the State Department in trouble tickets jumped from 38% in the year ending in September 2008 to 79% twelve months later. Comparing monthly totals of trouble tickets for the same two periods, the number of cyber incidents doubled. The volatility of changes to security sensitive settings has been equally problematic.

Ongoing demands for Certification and Accreditations (C&A) studies every three years are the most problematic for our goals. The Department spent $133M over the last six years amassing a total of 50 shelf feet, or 95,000 pages, of final C&A documentation for about 150 major information systems. The electronic working files that support this process over the same period contain 18 Giga-bites of documents with over 33,000 working files. This does not include data bases for tracking system inventory, and tracking Plans of Action and Milestones to resolve pending weaknesses. This equates to cost of the C&A report, which does not include other related products (e.g., system security plans), roughly $1,400 per page. Most compliance driven "snapshots" produce results on paper which are often extraordinarily accurate but out of date within days of being published and are only indirectly connected to the new threats heading toward the Department minute to minute.

Promising Opportunities. In contrast, this month the Office of Management and Budget launched CyberScope, a secure, streamlined, interactive data collection platform for more efficient reporting that also allows research and analysis across Federal agencies.

Additionally, the U.S. Chief Information Officer has formed an interagency task force charged with developing outcome-focused metrics for information security performance by Federal

agencies. Final metrics based on the work of this task force are expected to be released this fiscal year. The National Institute of Standards and Technology (NIST) is revising its current C&A, Special Publication 800-37, by changing the focus of security protection to "continuous monitoring." For its part, the Department began supplementing its FISMA compliance reports and studies with a risk scoring program scanning every computer and server connected to its network not less than every 36 hours on 8 security factors and twice a month for safe configurations of software.

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

Since mid-July, overall risk on the Department's key unclassified network measured by the Risk Scoring program has been reduced by nearly 90% in overseas sites and 89% in domestic sites. These methods have allowed one critical piece of the Department's information security program to move from the snapshot in time previously available under FISMA to a program that scans for weaknesses – continuously; identifies weak configurations – each 15 days; recalculates the most important problems to fix in priority order – daily; and issues letter grades (A+ to F) monthly to senior managers tracking progress for their organization the last 30 days.

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

Conversations I have had with other federal and private chief information security officers encourages me to believe that the State Department experience is both scalable and adaptable to other parts of government and private industry.

Other Elements of Cyber Security Defense in Depth at State

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

Network Monitoring & Incident Response

The Department maintains a 24/7 network watch program that guards against the external penetration, compromise, or misuse of the Department's cyber assets. Analysts stationed at our Network Monitoring Center serve as continuous sentries for inappropriate network activity based on intrusion detection system signatures, reports from the Firewall Team and other sources. The analysts perform preliminary assessments to confirm the nature and source of suspicious network security events. Those matters deemed significant are escalated to the Computer Incident Response Team (CIRT) for in-depth analysis and corrective action.

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

Threat Detection

To combat increasingly sophisticated cyber attacks, the Department's Cyber Threat Analysis Program provides overseas posts and Department management with indicators and early warnings about potential cyber incidents. This team of technical analysts performs essential in-depth assessments of network intrusions and helps coordinate the Department's response to sophisticated cyber attacks. They also work closely with the law enforcement and network defense communities to develop both a comprehensive threat picture and possible remediation

measures. In addition, they perform proactive penetration testing and network forensic analysis to detect and resolve significant threat issues.

Global Security Scanning

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

Consequences for Cyber Misuse or Abuse

The Department's Cyber Security Incident Program was formed to address consequences for acts of cyber misuse or abuse by individuals. The program enhances the protection of the Department's cyber infrastructure by raising overall cyber security awareness and providing managers with the ability to hold individual users accountable for acts of cyber misuse or abuse. The Department like all parts of the federal government needs to balance the benefits of cyber space for mission effectiveness, with the personal responsibility every employee is asked to demonstrate when using government cyber resources.

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

In addition to the types of incidents that lend themselves to detection, the Department's network monitoring and inspections alert key Department officials to risks when they occur. Upon notification of an incident, an investigation is undertaken incorporating several Department

organizations charged with gathering the information necessary to ensure a prompt and appropriate response to the cyber event, while protecting the rights of the accused.

Since the Cyber Security Incident Program was established in 2007 a total of 82 users have been cited for infractions and 14 users have been cited for violations. For those found to have committed an infraction or violation, the consequences available to the Department range from a letter of warning, suspension of network access or further disciplinary action.

Other Federal Activity

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

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

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503
www.whitehouse.gov/OMB

Post-Hearing Questions for the Record
Submitted to Mr. Vivek Kundra
Federal Chief Information Officer,
Administrator for Electronic Government and Information Technology
Office of Management and Budget

Senate Homeland Security and Governmental Affairs
Subcommittee on Federal Financial Management,
Government Information, Federal Services, and International Security
"More Security, Less Waste: What Makes Sense for our Federal Cyber Defense"
October 29, 2009
Questions for the Record from Senator Thomas R. Carper to Mr. Vivek Kundra

1. **I think everyone can agree that during a time when the federal government is racking up record-high deficits, we need cut out as much waste as possible. At the hearing, we discussed whether the current paper-work laden method of conducting certification and accreditation is a wise investment of our tax dollars. It doesn't make sense to me that agencies will spend $1.3 billion to produce paperwork that, in the end, is quickly out-dated and doesn't help secure our networks. But I doubt that this is the only area where the federal government may not be spending its money wisely defending the networks. What are one or two other opportunities that we didn't discuss at the hearing that we can pursue together and will lead to greater efficiencies?**

The ongoing automation of the collection of metrics is allowing us to analyze the software and services that agencies are currently using to defend and secure their networks. We can use that information to strategically negotiate "Smartbuy" government-wide contracts that leverage the government's purchasing power and provide consistent solutions for the most widely used. A further advantage of the Smartbuy program is that state and local governments can also take advantage of these savings. Many state and local governments have already participated in earlier Smartbuys for encryption tools.

Another area that promises greater efficiencies is the use of cloud-based resources. The cloud uses a shared infrastructure that can be secured once for all applications running. We have taken a step towards this promising future with the launch of *Apps.gov*, a GSA site that offers one-stop shopping and resources for agencies looking for cloud services.

Finally, OMB is committed to consolidating data centers across the Federal government. Currently, there are nearly 1,000 datacenters in existence. By consolidating and reducing the number, the Federal government will save money by reducing energy consumption, personnel and maintenance costs.

2. As the saying goes, "what gets measured gets done." It strikes me that for the past few years agencies have spent billions of dollars and seen little to no improvement in their security. For example, it seems every year OMB tells Congress in their annual FISMA report that agencies are making progress, yet we continue to hear of massive intrusions into our government networks. Fortunately, it seems that the State Department has developed a system that measures the right things, holds people accountable, and reduces the department's risks. What specific performance based measures and tools would you recommend agencies employ that are likely to make the government more secure? Further, what do you recommend would be the appropriate way for OMB to effectively monitor whether agencies are making progress and securing their systems?

We agree that the current implementation of FISMA measures does not adequately meet all of our current security management needs. We have pulled together a task force that represent diverse viewpoints. This task force, composed of representation from the CIO Council, NIST, DHS, the IG Council, and the ISPAB, has assisted us in developing a set of draft metrics that are forward-looking and will move the agencies towards real security improvement. These metrics are currently out for public comment and we plan to issue the final set in winter 2010. The metrics cover areas OMB has never measured before but that constitute significant attack vectors for the federal agencies, such as remote access and data level protection controls. In addition, the metrics are designed to push the agencies to adopt automated and continuous monitoring by asking more directly about their abilities to monitor their network activity.

3. I was in disbelief at a hearing I chaired last year on this issue to learn that many of the people that are responsible for securing our networks aren't allowed to know how the bad guys are getting into our systems because they don't have clearances. However as you know, we can't spend unlimited resources on cyber security. So that means we need to be wise with our money and prioritize our risks so that our defenses are strongest where the attackers are nailing us. It struck me that all of the witnesses agree that penetration testing, essentially good guys breaking into our systems to see where our weaknesses are, is something that all agencies should be doing. Please explain to me how you think agencies currently prioritize their risks and whether the money we spend on our defenses is actually stopping the attackers. Further, provide me with some possible improvements to the current system so that if new sophisticated threats arise, the American people can have confidence that agencies will protect their systems in a timely manner.

OMB agrees that penetration testing is an essential diagnostic and management tool for agencies to understand their vulnerabilities to specific attacks. This can be used as one measure to test their security. In addition to diagnosing network defenses, it is one of the best ways to raise management awareness of deficiencies and test an agency's incident response capability. We are working with Executive departments to develop operational procedures to support penetration testing so that agencies can get the most value from these services. In addition, in

our draft performance metrics, we push agencies to procure these services by asking them directly about results.. However, our adversaries are very agile. Penetration testing reveals some, but not all of the weaknesses of and poor security practices employed in systems. If we focus our priorities only on flaws revealed by penetration testing, we are likely to miss undiscovered flaws and leave ourselves vulnerable to changes in our adversaries' attack strategies. Penetration testing does have real value as a diagnostic tool, but it may be even more useful as a means for encouraging very senior management to focus on and reduce their systems' security vulnerabilities. The Department of Commerce is working on relevant security standards, as well as the Departments of Defense and Homeland Security.

Over the last decade, agencies have increased their awareness of cybersecurity risks and under the guidance of OMB they have invested in a variety of security risk prevention, detection, and mitigation capabilities. The funds spent on these capabilities are a worthwhile investment and they provide protections against a certain set of known cybersecurity risks. However, security threats change continuously and rapidly. In their concentration on completing their missions and serving the citizens, agencies sometimes lose sight of the risk of cybersecurity attacks or do not prepare to defend themselves against new, emerging threats quickly enough. Additional layers of protection, known as a "Defense-in-Depth" strategy are still needed to improve the Federal government's cybersecurity protections to an acceptable level. Concern about attacks directed against Federal networks is the main driver behind the development and implementation of the Comprehensive National Cybersecurity Initiative (CNCI) and the implementation of the Trusted Internet Connection (TIC) Initiative as part of the CNCI. By insisting that agencies reduce their external connections into fewer more heavily secured portals, we are reducing their visibility as a target. The TIC initiative will also provide detection of the most dangerous attacks against the agencies. Another part of the CNCI involves increasing the sharing of information among the various incident centers in the Federal Government to provide strong cybersecurity awareness.

4. I want to commend you for tackling such a complex and difficult issue. You are in a unique position to make positive change in the federal government and save money while you are at it. The model the State Department is using may not work in every agency, but there is a lot that I believe other agencies can take away and implement in their own agency. Mr. Kundra, in the following months, what will you be doing to refocus the money agencies spend on paperwork compliance, which is not mandated by law but by OMB, and shifting that money to invest in a system like the one used by the State Department. Further, should Congress and the American people expect to pay another $1.3 billion next year on a process that doesn't seem to be paying off?

As was mentioned above, we are drafting new metrics that will change the agencies' perspective from compliance to improvement of their security. Part of those metrics is encouraging agencies to adopt scanning and monitoring tools that give them real time information on their security posture. Those are the types of tools that underlie the vulnerability remediation and reporting system demonstrated by State. For example, the draft metrics include queries about whether agencies have the ability to determine all the devices connected to their network at any time and whether they can determine the configuration of those devices. These

types of questions are combined with questions on areas of security programs that represent major vulnerabilities for agencies but were not covered in previous years, such as data level protections and remote access.

In addition to changing the metrics, we have changed the method of collection to an automated platform. On October 18, 2009, OMB released CyberScope, a platform that allowed metrics to be collected into a web-based, database, rather than as separate spread sheets. The development and implementation of CyberScope was designed to allow the automated collection of metrics from the agency. This may not seem like a major change, but only with the elimination of the cumbersome manual collection process, can we move from a static annual or even quarterly reporting system to one that is on-demand and in real time. Over the next few years, we, in cooperation with the Department of Homeland Security, to build out a platform that will permit the secure collection of information that is needed at the time it is needed, for security response as well as oversight.

5. I find that sometimes after a hearing, there are certain points that I wish had made or questions I wanted to explore further. That is the case with me and maybe with you too. If you have anything else on this topic that you would like to bring to my attention, please do so now and I look forward to working with you going forward.

We look forward to working with you in the future and to receiving your comments on the draft proposed security metrics. (NOTE: copy of proposed metrics are attached)

Proposed FY 2010 FISMA Performance Metrics

Please send comments to:

OMB-Metrics@nist.gov

By January 4, 2010

System Inventory

- Please provide the number of agency-owned and contractor systems by component with the following information
  - FIPS 199 risk category
  - Certification and accreditation status
  - Whether annual testing occurred
  - Whether a tested contingency plan exists
  - The number of systems assessed at E-Authentication levels 3 or 4

Hardware Inventory

- Can the agency provide a real-time data feed of its asset inventory of all devices connected to its network?

Hardware Inventory

Sub questions:

- How frequently updated is the D/A's asset inventory of all devices connected to the network and the network devices themselves, recording at least the network address, device name(s), purpose of each system, and an asset owner responsible for each device?
- Is this capability manual, partially automated or fully automated for all D/A devices?
- Does the D/A have the technical ability to block introduction of unauthorized hardware to any device connected to the network? Is there a process to respond if detected?
- Does the D/A regularly test this capability by attaching devices not already in the inventory to the network?
- Does the D/A technically scan and discover/inventory all devices connected to the enterprise network?
- If the D/A does not currently maintain such an inventory, what are its plans to do so and by when?

Software Inventory

- Can the agency provide a real-time data feed of its asset inventory of all software installed on all devices connected to its networks?

Software Inventory

Sub-questions:

- How frequently updated is the D/A's asset inventory of all software installed on devices connected to the network, recording at least the operating system, version number, patch level, and the applications installed on it?
- Is this capability manual, partially automated or fully automated for all D/A devices?
- Does the D/A technically scan and discover/inventory all software on devices connected to the enterprise network?
- If the D/A does not currently maintain such an inventory, what are its plans to do so and by when?
- Does the D/A have the technical ability to block introduction of unauthorized software to any device connected to the network? Is there a process to respond if detected?
- Does the D/A regularly test this capability by attempting to install unapproved software on D/A devices?

Connections Inventory

- Can the agency provide a real-time data feed of all of its external connections as defined in the TIC architecture?

Connections Inventory

Sub-questions:

- How frequently updated is the D/A's inventory of all external connections as defined in the TIC architecture?
- Is this capability manual, partially automated or fully automated for all D/A connections?
- Does the D/A technically block connections of unauthorized devices to the network?
- Does the D/A employ technical means to scan and map all IPs on each enclave?
- If the D/A does not currently maintain a connections inventory, what are its plans to do so and by when?

Configuration Management

For various hardware and software, agencies will be asked the following questions:

- Standard baseline configuration defined
- Checklist Used
- Number of instances that can be and the number that are technically scanned for compliance with standard baseline
- Frequency of scanning of all instances (Average number of days)
- Number of instances with settings found to be compliant with standard baseline
- Average time to apply high security criticality patch to 95% of machines
- What technology is used for scanning?

Integration of Security into SDLC

- What number of new systems (by 199 level) went live during the reporting period?
- What number of new systems used 800-53 controls as system design requirements?
- What number of new systems used 800-53A in the process of system acceptance testing?
- What number of contract systems have the FISMA requirements in the contract or equivalent language?

Remote Access Management

- Can the agency provide a real-time data feed of all of its external connections?

Remote Access Management

Sub-questions:

- For GFE, do you automatically mitigate deviations from the minimum D/A configurations before allowing connection to proceed?
- For personally-owned equipment (if permitted for use), do you require the user's system to meet minimum D/A configurations before allowing the connection to proceed?
    - If you are unable to prohibit connections when minimum D/A configuration standards are not met, when do you plan to have that functionality in place?
    - If you are unable to actively validate that remotely connected devices meet D/A configuration standards upon connection, when do you plan to have that functionality in place?
- What percentage of remote access connections to the D/A network do you monitor?
- Does your D/A monitor for: (a) intrusions, (b) malware, (c) data loss, (d) data flows (e.g., source/destination IP), (e) authorized user information (e.g., user ID), (f) resource(s) accessed, (g) other

Remote Access Management, cont.

- Does the D/A's remote access policy require two-factor authentication for remote access (including VPN, dial-up, and other forms)?
    - If the agency does not have a remote access policy, what are the plans to develop and implement one and by when, respectively?
- What number of users have remote access to the D/A networks?
    - What number of those use two-factor authentication for remote access?
    - What number of those use HSPD-12 cards?
- What percentage of connections prohibit split tunneling (as defined by NIST)?
- Is D/A information permitted to be stored on the local device?
- What percentage of remote access solutions (e.g., the cryptographic portions, if any) use FIPS 140-2 validated cryptographic modules?
- Does your D/A use a "time-out" function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity?

Incident Management

- **During the D/A's controlled network penetration testing, what percentage of incidents were detected by NOC/SOC?**
  - For detected incidents, what is the mean-time to incident recovery?
  - What tools, techniques, technologies, does the Agency use for incident detection?
  - How many systems (or networks of systems) are protected using the tools, techniques, and technologies listed above?
  - If the agency has not performed controlled network penetration testing, when will it have the capability to do so?

Incident Management cont.

- Does your D/A have an Incident Response Capability (whether in-house or as part of managed security services contract)?
    - If not, does the D/A have a Security Operations Center operating as the incident response center?
- Does your D/A participate in US-CERT threat briefings? (E.g., JACKE)
    - If not, why and what are the D/A's plans to participate?
- Does your D/A have access to GFIRST information?
    - If not, why and what are the D/A's plans to obtain access?
- Does your D/A have access to US-CERT publications? (E.g., SARS)
    - If not, why and what are the D/A's plans to obtain access?

Training

Can the agency provide a real-time data feed with the information in the chart below?

# of employees and contractors with log-in privileges	# of employees and contractors given annual security awareness training	# of employees and contractors with significant security responsibilities	# of employees with significant security responsibilities provided specialized security training	Cost of providing security awareness training	Cost of providing specialized security training

Does the D/A security awareness training:

- Address phishing?
- Cover the subject of remote access?
- Cover the subject of Web 2.0 technologies?
- Cover the subject of Peer-to-Peer technologies?

Training, cont.

- Is the training automated or in person? Or both?
- How many employees/contractors have security related certifications?
- How many employees/contractors with significant security responsibilities have security-related certifications?
- Please identify the types of security-related certifications for each.
- List the titles of Agency official(s) that determine the employees with SISR.
- Provide the criteria to determine who has SISR. (E.g., privileged access, data focused, decision-making/managerial focused, OPM job descriptions, etc.)
- Provide the number of employees and contractors with system privileges.
  - Provide the number of these that were given appropriate security and privacy awareness training during the reporting year.

Identity & Access Management

- **What is the percentage of employees and contractors with valid HSPD-12 credentials?**
  - Please upload a progress update for your HSPD-12 logical access plan.
- How many systems in your reported system inventory use two-factor authentication?
  - How many of these systems are enabled to use Personal Identity Verification (PIV) credentials for user authentication?
- Of the systems assessed at E-authentication levels 3 or 4, what percentage of those require two-factor or multi-factor authentication for non-Federal users (e.g. citizens, business partners)?
- What is the D/A number of privileged users (e.g. system administrators)?
- What percentage of privileged users are required to use two-factor authentication for all privileged authentications?

Data Leakage Prevention

- **What products/technologies does the D/A use for Data Leakage Prevention (DLP) or equivalent on its network to technically prevent the sending of unencrypted sensitive information outside the perimeter?**
    - If the D/A does not have any products/technologies in use, when will these be in place?
- What products/technologies does the D/A use for DLP or equivalent on its network to technically prevent the sending of unencrypted sensitive information to mobile media and USB devices?
    - If the D/A does not have any products/technologies in use, when will these be in place?

Data Leakage Prevention

- Does the D/A have the following in place:
  - data sensitivity based labeling scheme
  - a technical based labeling scheme
  - security controls invoked based on sensitivity based labeling
  - the capability to disable compromised mobile devices (i.e. lost or stolen devices)
- What is the percentage of portable computers (laptops) which have all user data encrypted with FIPS validated encryption?
- What is the percentage of Personal Digital Assistants which have all user data encrypted with FIPS validated encryption?

Real-Time Security Status & Management

- **Does the D/A have an automated capability (e.g. via a SIM or SIEM tool) to provide real to near real time enterprise-wise cybersecurity situational awareness?**
  - Does it integrate the following:
  - Note: If your answer is no to any of the following, please provide the date by which your agency will have this capability in place.
    - Intrusion Detection/Prevention Sensor Data
    - Anti-Virus/Anti-Malware/Anti-Spyware
    - System Log Data
    - Application Log Data
    - Patch Status
    - Vulnerability Scans
    - Security Configuration Management Scans of:
      - » Operating Systems
      - » Databases
      - » Servers
      - » Network Devices (firewalls, routers, switches)

Real-Time Security Status & Management

- If your agency does not have the automated capability to provide real to near real-time enterprise-wide cybersecurity situational awareness, please provide the date by which your agency will have this capability in place.

GAO
Accountability * Integrity * Reliability
United States Government Accountability Office
Washington, DC 20548

December 18, 2009

The Honorable Thomas R. Carper
Chairman
Subcommittee on Federal Financial Management, Government
Information, Federal Services, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

Subject: *Review of Actions for Securing Federal Networks*

Dear Senator Carper:

This letter responds to your request to elaborate on issues discussed at the October 29, 2009, hearing on cost-effective cyber defense practices. Your post-hearing questions for the record provided by your staff via e-mail and our responses follow.

1. I think everyone can agree that during a time when the federal government is racking up record-high deficits, we need to cut out as much waste as possible. At the hearing, we discussed whether the current paperwork-laden method of conducting certification and accreditation is a wise investment of our tax dollars. It doesn't make sense to me that agencies will spend $1.3 billion to produce paperwork that, in the end, is quickly out-dated and doesn't help secure our networks. But I doubt that this is the only area where the federal government may not be spending its money wisely defending the networks. What are one or two other opportunities that we didn't discuss at the hearing that we can pursue together and will lead to greater efficiencies?

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

Another opportunity to increase efficiencies is to leverage the federal government's purchasing power to promote the offering of more secure products and to save costs on the acquisition of security software products and services. For example, the SmartBUY program, currently led by the General Services Administration, assists agencies in acquiring commercial off-the-shelf encryption software at discounted prices. According to the General Services Administration (GSA), SmartBUY is a federal government procurement vehicle designed to promote effective enterprise-level software management. By leveraging the government's immense buying power, SmartBUY could save taxpayers millions of dollars through governmentwide aggregate buying of commercial off-the-shelf software products.[1] This program could possibly be expanded to include acquisition of automated tools such as the ones discussed above.

2. As the saying goes, "what gets measured gets done." It strikes me that for the past few years agencies have spent billions of dollars and seen little to no improvement in their security. For example, it seems every year that the Office of Management and Budget (OMB) tells Congress in their annual FISMA report that agencies are making progress, yet we continue to hear of massive intrusions into our government networks. Fortunately, it seems that the State Department has developed a system that measures the right things, holds people accountable, and reduces the department's risks. What specific performance-based measures and tools would you recommend agencies employ that are likely to make the government more secure? Further, what do you recommend would be the appropriate way for OMB to effectively monitor whether agencies are making progress and securing their systems? Lastly, what are the three most notable metrics that agencies should be focused on to see immediate success?

While federal agencies have made progress toward fulfilling their statutory responsibilities under the Federal Information Security Management Act of 2002 (FISMA), the current reporting process does not produce information to accurately gauge the effectiveness of federal information security activities.[2] A key reason for this is that federal agencies have tended to rely on compliance metrics that measure whether or not a control activity was performed and not on metrics that measure how well or effectively the control was implemented. Accordingly, we recommended[3] that federal agencies employ a balanced set of performance-based metrics that address (1) compliance with policies, standards, or legal and regulatory requirements; (2) effectiveness of information security controls; and (3) overall impact of an organization's information security program. When developing these measures, we also recommended that agencies (1) focus on their risks, (2) involve

[1] GAO, *Information Security: Federal Agency Efforts to Encrypt Sensitive Information Are Under Way, but Work Remains*, GAO-08-525 (Washington, D.C.: Jun. 27, 2008).

[2] GAO, *Information Security: Agencies Continue to Report Progress, but Need to Mitigate Persistent Weaknesses*, GAO-09-546 (Washington, D.C.: July 17, 2009).

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

key stakeholders, (3) assign accountability for the measures to individuals, and (4) link measures to security and business goals.

In order for OMB to effectively monitor whether agencies are making progress and securing their systems, we recommended[4] that it revise annual reporting guidance to agencies to require (1) reporting on a balanced set of measures, including measures that focus on the effectiveness of control activities and program impact, and (2) inclusion of key attributes in the development of measures. In addition, we recommended that OMB revise the annual report to Congress to provide better status information, including information on the effectiveness of agency information security programs, the extent to which major risks are being addressed, and progress that has been made in improving the security posture of the federal government.

While there are many possible metrics that can be used to measure security activities at federal agencies, three notable effectiveness metrics that we have identified that are used by leading organizations are the *percentage of system or network downtime due to security incidents over time*, the *mean time to incident discovery*, and the *percentage of security incidents caused or facilitated by improperly configured devices*. We identified the practices of leading organizations as part of our work on federal information security measures.[5]

3. I was in disbelief at a hearing I chaired last year on this issue to learn that many of the people that are responsible for securing our networks aren't allowed to know how the bad guys are getting into our systems because they don't have clearances. However, as you know, we can't spend unlimited resources on cyber security. So that means we need to be wise with our money and prioritize our risks so that our defenses are strongest where the attackers are nailing us. It struck me that all of the witnesses agree that penetration testing, essentially good guys breaking into our systems to see where our weaknesses are, is something that all agencies should be doing. Please explain to me how you think agencies currently prioritize their risks and whether the money we spend on our defenses is actually stopping the attackers. Further, provide me with some possible improvements to the current system so that if new sophisticated threats arise, the American people can have confidence that agencies will protect their systems in a timely manner.

Regarding the current prioritization of risks by federal agencies, we have identified multiple instances where agencies have failed to properly assess their information security risks.[6] In part, this was due to agencies not having timely or complete information on cyber threats, not appropriately considering the effect of known

---

[4] GAO-09-617.

[5] GAO-09-617.

[6] See, for example: GAO, *Information Security: NASA Needs to Remedy Vulnerabilities in Key* Networks, GAO-10-4 (Washington, D.C.: Oct. 15, 2009); *Information Security: Continued Efforts Needed to Address Significant Weaknesses at IRS*, GAO-09-136 (Washington, D.C.: Jan. 9, 2009); and *Information Security: TVA Needs to Address Weaknesses in Control Systems and Networks*, GAO-08-526 (Washington, D.C.: May 21, 2008).

vulnerabilities in their systems, and not fully understanding the potential impact on agency operations, assets, or individuals should there be a security breach. Agencies need to mitigate the current weaknesses in their risk assessment processes to improve their abilities to ensure that systems apply the appropriate level of controls to prevent the unauthorized access, use, disclosure, disruption, modification, or destruction of data. In addition, federal agencies can include additional information in their risk assessments, such as known security vulnerabilities reported by third parties and analysis of confirmed incidents on the agency's systems.

Federal agencies have been able to stop attackers using the defenses they currently have in place. For example, the chief information security officer of the Department of State testified that in a typical week, the department blocks 3.5 million spam e-mails, intercepts 4,500 viruses, and detects over a million external probes to its network.[7] Nevertheless, attacks continue to be successful. The number of security incidents reported by federal agencies to the United States Computer Emergency Readiness Team (US-CERT) has increased from 5,503 incidents reported in fiscal year 2006 to 16,843 incidents in fiscal year 2008 (slightly more than 200 percent).[8] This indicates that agencies need to better protect their networks and systems.

Several opportunities exist to improve federal defenses against cyber threats, about which we testified in November 2009.[9] First, federal agencies can implement the hundreds of recommendations made by GAO and the inspectors general for actions necessary to resolve previously identified significant control deficiencies and information security program shortfalls. For example, we recommended that agencies mitigate specific deficiencies in controls intended to (1) identify and authenticate users, (2) restrict user access to systems, (3) protect network boundaries, (4) encrypt network services and sensitive information, (5) audit and monitor security-related events, (6) physically protect system resources, (7) manage system configurations, and (8) plan for contingencies. 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.

Second, continued progress can be made on key initiatives being undertaken by the White House, OMB, and certain federal agencies that are intended to enhance information security at federal agencies. These initiatives include the Comprehensive National Cybersecurity Initiative, the Federal Desktop Core Configuration, the Einstein system, and the Trusted Internet Connections Initiative. We currently have

---

[7] United States Department of State Chief Information Security Officer, *Cybersecurity: Emerging Threats, Vulnerabilities and Challenges*, statement before the House Subcommittee on Government Management, Organization and Procurement, Committee on Oversight and Government Reform (May 5, 2009).

[8] GAO-09-546.

[9] GAO, *Cybersecurity: Continued Efforts Are Needed to Protect Information Systems from Evolving Threats*, GAO-10-230T (Washington, D.C.: Nov. 17, 2009).

ongoing work that addresses the status, planning, and implementation of these initiatives.

Third, the Department of Homeland Security (DHS) can continue to address recommendations to fully satisfy its key responsibilities for protecting critical infrastructures. For example, DHS can address recommendations in key areas, including bolstering cyber analysis and warning capabilities, improving cybersecurity of infrastructure control systems, and reducing organizational inefficiencies.

Finally, improvements can be made to the National Cybersecurity Strategy. For example, key improvements identified by cybersecurity experts include establishing White House responsibility and accountability for leading and overseeing national cybersecurity policy, focusing greater attention on addressing the global aspects of cyberspace, and increasing the cadre of cybersecurity professionals.[10]

4. Mr. Wilshusen, you have testified before this committee on several occasions, and I appreciate all of your work. In your travels exploring the issue of cyber security, are there any other methods or tools being utilized by other agencies or private sector folks that could be leveraged as a means to substitute or complement the current certification and accreditation process? The State Department seems to have found a good approach, and I hope we can build off that. But I am sure there are some other agencies or companies that are doing good work too that we should look at.

In a draft publication, the *Guide for Applying the Risk Management Framework to Federal Information Systems*,[11] the National Institute of Standards and Technology (NIST) proposes revising the certification and accreditation process into a six-step risk-management framework. This framework de-emphasizes the point-in-time evaluations that are central to the current certification and accreditation process; instead, the focus is expected to be placed on monitoring security controls while the system is in operation. If adopted and effectively implemented, this development is intended to provide more timely risk management information to senior leaders and lead to better risk-based decisions regarding the operation of systems and implementation of security controls.

In addition, an opportunity exists to complement the process of testing information systems for security. As we stated in our response to question 1, implementing a continuous monitoring capability that includes the use of automated tools for information security analysis can improve an agency's awareness of security problems and its ability to quickly mitigate weaknesses found.

5. The inspectors general have a special role ensuring that agencies are securing their systems to extent possible. If agencies move to a system like the State Department, it seems that an inspector general, or anyone for that matter,

---

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

[11] NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (Gaithersburg, Md.: Nov. 2009).

could come at anytime and see what the security posture of the agency is. If you believe that to be true, what should be the role of the inspector general and how often should the inspector general be required to test the effectiveness of an agency's security controls?

Because we have yet to examine the State Department's system, we cannot comment on whether the system provides sufficient information to reasonably determine the security posture of the agency. Regardless, agency inspectors general have an important role in that they can provide an independent and objective evaluation of the agency's information security policies, procedures, practices, and controls. FISMA requires agency inspectors general or an independent external auditor to conduct an evaluation of their agency's information security program and practices on an annual basis. Regardless of how an agency is testing and reporting the security of its systems, the important role of the inspector general in conducting these annual evaluations should remain.

We have previously discussed[12] the importance of annual independent evaluations of agency FISMA implementation as well as possible ways to improve these evaluations. According to our annual analysis of FISMA reports and our information security work, such independent evaluations lack a common approach, culminating in disparities in the type of work conducted, as well as its scope, methodology, and content. The use of generally accepted government auditing standards to perform the independent evaluations, already in use at 13 of 24 major departments and agencies, would provide a baseline for consistent evaluations and help ensure their quality.

6. I find that sometimes after a hearing, there are certain points that I wish had made or questions I wanted to explore further. That is the case with me and maybe with you too. If you have anything else on this topic that you would like to bring to my attention, please do so now and I look forward to working with you going forward.

A number of current issues related to federal information security merit attention. These issues include:

Security over contractor-operated systems. FISMA requires the head of each agency to assume responsibility for ensuring risk-based information security protections for information processed and systems operated on the agency's behalf by contractors and other third parties. According to the FISMA reports for 24 major agencies, which we reviewed as part of our prior work mandated by FISMA,[13] the number of contractor systems increased 40 percent during fiscal year 2008, while the number of agency inspectors general responding that the agency "almost always" ensured that contractors complied with FISMA, OMB, and NIST requirements declined from 14 to 8 between fiscal years 2006 and 2008. Several incidents reported in the press involving the unauthorized disclosure of sensitive federal information stored on contractor-operated systems highlight the vulnerability of such information and

---

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

[13] See, for example: GAO-09-546 and GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: Jul. 27, 2007).

indicate that improvements can be made to the oversight of contractor system security by federal agencies.

IT security human capital. We previously reported the views held by nationally recognized experts of critical aspects of the nation's cybersecurity strategy, including areas for improvement.[14] The experts highlighted key improvements that were, in their view, essential to improving the strategy and our national cybersecurity posture. One of the areas highlighted was the need to increase the cadre of cybersecurity professionals. According to these experts, prior efforts to address this need have not created sufficient numbers of professionals, including information security specialists and cybercrime investigators. Expert panel members stated that actions to increase the number of professionals with adequate cybersecurity skills should include (1) enhancing existing scholarship programs (e.g., Scholarship for Service) and (2) making the cybersecurity discipline a profession through testing and licensing.

Agency inspectors general also have a pressing need for cybersecurity professionals. Because each inspector general is required to conduct an annual evaluation of the information security program and practices of that agency and because the threats to systems are ever-increasing, they need skilled personnel to conduct highly technical in-depth security audits.

Security incident reporting. Although strong controls may not block all intrusions and misuse, agencies can reduce the risks associated with such events if they take steps to detect and respond to them before significant damage occurs. Accounting for and analyzing security problems and incidents are also effective ways for an agency to improve its understanding of threats and the potential costs of security incidents, and doing so can pinpoint vulnerabilities that need to be addressed so that they are not exploited again. As we have previously reported,[15] at least 12 inspectors general noted specific weaknesses in incident procedures at their agencies, such as a lack of fully documented policies and procedures for responding to security incidents, a lack of control procedures to ensure that audit trails were being maintained and reviewed, and instances where incidents were not always handled and reported in accordance with requirements. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. Without proper incident response and documentation, agencies risk losing valuable information needed to prevent future exploits and to understand the nature and cost of the threats directed at them.

Information security training and awareness. Federal agencies rely on their employees and contractors to protect the confidentiality, integrity, and availability of the information in their systems. It is critical for system users to understand their security roles and responsibilities and to be adequately trained to perform them. As we have previously reported,[16] federal agencies reported a smaller percentage of employees and contractors who received security awareness training in fiscal year

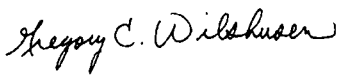
[14] GAO-09-432T.

[15] GAO-09-546.

[16] GAO-09-546.

2008 compared to the percentage in fiscal year 2006. In addition, agencies reported a lower percentage of employees with significant security responsibilities who had received specialized training. Due to the increasing number of attacks targeting end-user systems, sustained focus on providing high-quality information security training for federal employees and contractors remains crucial.

In responding to these questions, we relied on previous audit work we performed in developing prior reports and testimonies regarding federal information security practices. That prior work on which this letter is based was performed in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits 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. If you have any questions regarding this letter, please contact me at (202) 512-6244 or wilshuseng@gao.gov. GAO staff who made major contributions to this letter are Anjalique Lawrence (Assistant Director), Min Lee Hyun, Vernetta Marquis, Lee McCracken, and Jayne Wilson.



Gregory C. Wilshusen
Director, Information Security Issues

(311040)

Questions for the Record Submitted to
John Streufert by
Senator Tom Carper (#1)
Homeland Security Committee
October 29, 2009

Question:

I think everyone can agree that during a time when the federal government is racking up record-high deficits, we need cut out as much waste as possible. At the hearing, we discussed whether the current paper-work laden method of conducting certification and accreditation is a wise investment of our tax dollars. It doesn't make sense to me that agencies will spend $1.3 billion to produce paperwork that, in the end, is quickly out-dated and doesn't help secure our networks. But I doubt that this is the only area where the federal government may not be spending its money wisely defending the networks. What are one or two other opportunities that we didn't discuss at the hearing that we can pursue together and will lead to greater efficiencies?

Answer:

The State Department has employed a continuous monitoring and automated technique that conducts scanning every two weeks. The hope and intent is to provide for a more secure infrastructure and provide more frequent, complete, comprehensive and accurate summaries to OMB and other oversight entities of how technical control improvements are being made as compared to quarterly Plans of Action and Milestones and annual configuration management status reports required under the current implementation of FISMA and its related authorities. Other Department and agencies may wish to research and develop similar approaches.

Questions for the Record Submitted to
John Streufert by
Senator Tom Carper (#2a)
Homeland Security Committee
October 29, 2009

Question:

As the saying goes, "what gets measured gets done." It strikes me that for the past few years agencies have spent billions of dollars and seen little to no improvement in their security. For example, it seems every year OMB tells Congress in their annual FISMA report that agencies are making progress, yet we continue to hear of massive intrusions into our government networks. Fortunately, it seems that the State Department has developed a system that measures the right things, holds people accountable, and reduces the department's risks.
[2a.] What specific performance based measures and tools would you recommend agencies employ that are likely to make the government more secure?

Answer:

While the current iteration of the Department of State's continuous monitoring dashboard primarily measures the vulnerabilities facing information systems, future enhancements to the dashboard will measure the sensitivity of data, prioritization of vulnerabilities based upon the prevalence of the threat and factoring in compensating controls.

The Department of State's utilizes multiple scanners that provide valuable information on a continuous basis, thereby allowing timely identification of security problems and guidance on remediation. An additional opportunity that would benefit the federal agency community would be to establish of a government-wide process for specification, selection, and qualification of monitoring tools under the "Smart Buy"

program. This would provide the federal community with contracts offering a consolidated listing of available interoperable security software tools. These contracts would provide a vehicle under which the federal community may collectively use to purchase the necessary security software.

Questions for the Record Submitted to
John Streufert by
Senator Tom Carper (#2b)
Homeland Security Committee
October 29, 2009

Question:

Further, what do you recommend would be the appropriate way for OMB to effectively monitor whether agencies are making progress and securing their systems?

Answer:

An example of a program that is currently doing thismodel is the Department of State's program where it assigns point values to cyber security vulnerabilities according to the National Institute of Standards and Technology (NIST) guidelines.

More specifically, the Department of State's measures begin with using the NIST National Vulnerability Database (NVD), a database that assigns point values between .1 and 10 with 10 being the highest according to the Common Vulnerability Scoring System (CVSS) for known vulnerabilities. Then the Department of State electronically scans its roughly 70,000 computers and 6,000 servers assigning CVSS risk points to each organization. When security professionals in each Department of State organization successfully reduce known particular security risks, corresponding CVSS risk points are reduced. Progress is measured daily in multiple formats that is easily understandable and actionable from the technical subject matter experts to the senior decision makers.

Questions for the Record Submitted to
John Streufert by
Senator Tom Carper (#3)
Homeland Security Committee
October 29, 2009

Question:

I was in disbelief at a hearing I chaired last year on this issue to learn that many of the people that are responsible for securing our networks aren't allowed to know how the bad guys are getting into our systems because they don't have clearances. However as you know, we can't spend unlimited resources on cyber security. So that means we need to be wise with our money and prioritize our risks so that our defenses are strongest where the attackers are nailing us. It struck me that all of the witnesses agree that penetration testing, essentially good guys breaking into our systems to see where our weaknesses are, is something that all agencies should be doing. [3a.] Please explain to me how you think agencies currently prioritize their risks and [3b.] whether the money we spend on our defenses is actually stopping the attackers. [3c.] Further, provide me with some possible improvements to the current system so that if new sophisticated threats arise, the American people can have confidence that agencies will protect their systems in a timely manner.

Answer a:

One possible approach to prioritizing risk would be to develop a guidance document, updated on a frequent basis, instructing how agencies should prioritize risks based upon how the agency is being attacked.

Answer b:

Attacks are increasing and very likely will not be diminished, regardless of the amount of monies spent. Automated and continuous monitoring measures allow for more effective and efficient use of expenditures to address those vulnerabilities. The Department of State maintains a robust penetration testing program that mirrors our adversaries

attack methodologies and complements our continuous monitoring program. This program provides validation that our current defense in depth strategy matches the technology being used against our infrastructure, as best as can be reasonably ascertained.

Answer c:

The Department of State plans for expanding continuous monitoring with scanning for each of the 20 Most Critical Controls susceptible to automated verification as determined by the Consensus Audit Guidelines from computers and servers to all infrastructure and all applications. The Department of State's goal is to measure known security risks on all computers not less than every 72 hours by the end of FY2010. This measure is only one element of a balanced defense in depth cyber security program.

In addition to the Department of State specific improvements underway, improvements can be achieved through continued support of NIST's National Vulnerability Database and Security Content Automation Protocol given it provides the federal agency community with valuable tools needed to apply the risk management principles. Improvements can also be more readily achieved through greater incorporation of "white listing" concepts as compared to "black listing" for software given the inability of the later to address zero day threats and its unmanageable volume.

Questions for the Record Submitted to
John Streufert by
Senator Tom Carper (#4)
Homeland Security Committee
October 29, 2009

Question:

I find that sometimes after a hearing, there are certain points that I wish had made or questions I wanted to explore further. That is the case with me and maybe with you too. If you have anything else on this topic that you would like to bring to my attention, please do so now and I look forward to working with you going forward.

Answer:

The Department looks forward to working with the Chairman and the Subcommittee on these matters and will gladly share any other related topics with you in the future.