DHS'S EFFORT TO SECURE .GOV

HEARING

BEFORE THE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

JUNE 24, 2015

Serial No. 114–23

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

96–169 PDF WASHINGTON : 2015

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

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

JOHN RATCLIFFE, Texas, *Chairman*

PETER T. KING, New York
TOM MARINO, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
DANIEL M. DONOVAN, JR., New York
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(ex officio)*

BRETT DEWITT, *Subcommittee Staff Director*
DENNIS TERRY, *Subcommittee Clerk*
CHRISTOPHER SCHEPIS, *Minority Subcommittee Staff Director*

CONTENTS

DHS'S EFFORT TO SECURE .GOV

Wednesday, June 24, 2015

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES,
Washington, DC.

The subcommittee met, pursuant to call, at 2:42 p.m., in Room 311, Cannon House Office Building, Hon. John Ratcliffe [Chairman of the subcommittee] presiding.

Present: Representatives Ratcliffe, Perry, Clawson, Donovan, McCaul, Richmond, Jackson Lee, and Langevin.

Mr. RATCLIFFE. The Homeland Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies will come to order.

The subcommittee meets today to hear what the Department of Homeland Security is doing to secure U.S. Government networks from cyber hackers. The magnitude of the latest breach at the Office of Personnel Management, or OPM, and the impact that it will have on tens of millions of Americans and our National security for decades to come is simply unacceptable.

OPM was warned about its poor IT security. Yet, we still found them asleep at the switch. To put it in perspective, OPM was responsible for safeguarding extremely sensitive data, personnel files, and security clearance information for tens of millions of Federal employees. Yet, OPM's efforts to secure its networks were frankly laughable. The stakes were immense. Yet, the cybersecurity efforts were pathetic. In my opinion, this could be classified as cybersecurity malpractice.

The Federal agency guarding this sensitive information demonstrated gross negligence and willful disregard of earlier warnings. We need to know who in this administration is really in charge and who is truly responsible for securing our Federal Government's civilian information systems.

The nature of the compromised data is particularly concerning because it contained the personally identifiable information, or PII, of what is now known to be at least 14 million Federal and Congressional employees and military personnel. Not only did we fail to protect that PII, we failed to protect the security clearance background check information contained on the Questionnaire for National Security Position form, also known as the SF–86.

The individuals who serve our country, often risking their lives, disclose substantial personal information on these forms to get special clearances to handle our Government's secrets, and they have

every right to expect that their information will be safe. But, as we have learned, OPM struggled to implement even the most basic network security protocols.

This was spelled out in the November 2014 inspector general report 1 month before the breach occurred. The Government Accountability Office has drawn similar conclusions. Specifically, the inspector general found lackluster information security governance and even recommended that OPM shut down all of its information systems that lacked the valid authorization.

Additionally, in 2014, DHS presented to OPM a mitigation plan with recommendations for improving its information security. The question then is why the recommendations from DHS and others were not required and fully implemented by OPM.

Unfortunately, the White House response to the OPM breach has been incredibly disappointing. The Federal Government was attacked. Yet, there is no indication that there will be any consequences from these actions. In addition, the U.S. Chief Information Officer, Tony Scott, has called for a, "30-day cybersecurity sprint," for Federal agencies to secure their networks and data.

So the White House is essentially calling on Federal agencies to step up and do in the next 30 days what they were already required to do. Our country's cybersecurity shouldn't be a 30-day sprint exercise, but, rather, a dedicated marathon, a long, sustained, and comprehensive effort to protect our country from escalating and rapidly evolving cyber attacks. This administration's response is superficial. It is not serious, and it doesn't reflect the gravity of the threats facing our Nation right now in cyber space.

It is clear that the Nation is under attack, under siege, by state and non-state actors and our defenses at OPM and in the Federal Government are woefully inadequate. As such, in this hearing today, we will examine the cyber capabilities that DHS is providing to OPM and to other Federal civilian agencies, how quickly these tools are being deployed Government-wide, and, ultimately, what vulnerabilities and gaps remain in our cybersecurity posture.

Last December Congress passed the Federal Information Modernization Act, or FISMA, to give DHS the authority to carry out the operational activities to protect Federal civilian information systems from cyber intrusions. Now that DHS has these authorities, we want to hear how DHS plans to execute the new law and rapidly implement its binding directives and other Federal information security capabilities to more quickly secure the .gov domain.

Additionally, DHS' EINSTEIN and Continuous Diagnostics and Mitigation program, or CDM, were designed to protect Federal civilian agency systems. Yet, not every Federal agency has adopted them. Why is that the case?

Although these programs aren't a silver bullet to prevent further cyber attacks, both play a vital role in what should be a defense-in-depth cybersecurity strategy. Now more than ever DHS needs to rapidly deploy its cyber capabilities and show strong leadership to protect our Government's networks and most sensitive information from cyber hackers.

I also hope that, if nothing else, this latest attack on OPM servers will prove to be a catalyst to get the United States Senate to

act and pass the strong and bipartisan House-passed cybersecurity information-sharing legislation.

These bills would, in part, authorize DHS' EINSTEIN program and allow for greater sharing of cyber threat indicators so both the public and private sectors can more effectively block known and malicious cyber intrusions.

From my vantage point as Chairman of this subcommittee and as a former terrorism prosecutor, cybersecurity is National security. The United States Government is under cyber attack from nation-states and criminal groups, and I look forward to hearing from our witnesses today on what the Department of Homeland Security is doing about it.

[The statement of Chairman Ratcliffe follows:]

STATEMENT OF CHAIRMAN JOHN RATCLIFFE

JUNE 24, 2015

The subcommittee meets today to hear what the Department of Homeland Security is doing to secure the U.S. Government's networks from cyber hackers. The magnitude of the latest breach at the Office of Personnel Management (OPM), and the impact it will have on tens of millions of Americans and our National security for decades to come, is simply unacceptable. OPM was warned about its poor IT security; yet we still found them asleep at the switch. To put it into perspective, OPM was responsible for safeguarding extremely sensitive data-personnel files and security clearance information for tens of millions of Federal employees—yet OPM's efforts to secure its network were laughable. The stakes were immense, yet the cybersecurity efforts were pathetic. In my opinion, this could be classified as a "cybersecurity malpractice" of sorts. The Federal agency guarding this sensitive information demonstrated gross negligence and willful disregard of earlier warnings. We need to know who in this administration is in charge, and who is responsible for securing our Federal Government's civilian information systems.

The nature of the compromised data is particularly concerning because it contained the personally identifiable information (PII) of up to 14 million Federal and Congressional employees, and military personnel. Not only did we fail to protect PII, we failed to protect the security clearance background check information contained on the Questionnaire for National Security Positions form, called an SF–86. The individuals who serve our country, often risking their lives, disclose substantial personal information on these forms to get special clearances to handle our Government's secrets and expect their information will be safe.

As we've learned, OPM struggled to implement even the most basic network security protocols. This was spelled out in a November 2014 Inspector General report, 1 month before the breach occurred. The Government Accountability Office has drawn similar conclusions. Specifically, the IG found lackluster information security governance and even recommended that OPM shut down all its information systems that lacked a valid authorization. Additionally in 2014, DHS presented to OPM a mitigation plan with recommendations for improving its information security. The question, then, is why the recommendations from DHS and others were not required and fully implemented by OPM?

Unfortunately, the White House response to the OPM breach has been extremely disappointing. The Federal Government was attacked, yet there is no indication that there will be consequence for these actions. Additionally, the U.S Chief Information Officer Tony Scott has called for a "30-day cybersecurity sprint" for Federal agencies to secure their networks and data. The White House is essentially calling on Federal agencies to do in the next 30 days what they were already required to do. Our country's cybersecurity should not be a sprint exercise; but rather a marathon—a long, sustained, and comprehensive effort to protect our country from escalating and rapidly evolving cyber-attacks. This administration's response is not serious and does not reflect the gravity of the threats facing our Nation in cyberspace.

It is clear that the Nation is under siege by state and non-state actors, and our defenses at OPM and in the Federal Government are woefully inadequate. As such, today we will examine the cyber capabilities that DHS is providing to OPM and other Federal civilian agencies, how quickly these tools are being deployed Government-wide, and ultimately, what vulnerabilities and gaps remain in our cybersecurity posture.

Last December, Congress passed the Federal Information Modernization Act (FISMA) to give DHS the authority to carry out the operational activities to protect Federal civilian information systems from cyber intrusions. Now that DHS has these authorities, we want to hear how DHS plans to execute the new law and rapidly implement its binding directives and other Federal information security capabilities to more quickly secure the .gov domain. Additionally, DHS' Einstein and Continuous Diagnostics and Mitigation (CDM) programs were designed to protect Federal civilian agencies' systems, yet not every Federal agency has adopted them. Why is that the case? Although these programs are not a silver bullet to preventing further cyber attacks, both play a vital role in what should be a "defense-in-depth" cybersecurity strategy. Now more than ever, DHS needs to rapidly deploy its cyber capabilities, and show strong leadership to protect our Government's networks and most sensitive information from cyber hackers.

I also hope that if nothing else, this latest attack will prove to be a catalyst to get the Senate to act and pass the strong and bipartisan House-passed cybersecurity information sharing legislation. These bills would, in part, authorize DHS' Einstein program and allow for greater sharing of cyber threat indicators so both the public and private sectors can more effectively block known and malicious cyber intrusions.

From my vantage point as Chairman of this subcommittee and a former terrorism prosecutor, cybersecurity is National security. The U.S. Government is under cyber-attack from nation-states and criminal groups and I look forward to hearing from our witnesses today on what the Department of Homeland Security is doing about it.

Mr. RATCLIFFE. The Chairman now recognizes the Ranking Minority Member of the subcommittee, the gentleman from Louisiana, Mr. Richmond, for any statements that he may have.

Mr. RICHMOND. Thank you, Mr. Chairman. Thank you for convening this hearing on DHS' responsibilities in helping all of the Federal agencies secure their cyber networks and databases.

I want to welcome our witnesses, Dr. Ozment, Mr. Wilshusen, and Dr. Gerstein. Thank you for taking the time to appear before us today.

Securing the Federal Government's networks and databases is a monumental task. DHS has been charged with the primary task to coordinate and provide cybersecurity guidance for the many Federal agencies, critical infrastructure sectors, and Government programs, whether it be Government, personnel information, Classified background information, patents, taxpayer data, nuclear facilities, health records, port complexes, or any number of other vital Government services.

However, under the Federal Information Security Modernization Act of 2014, FISMA, the White House Office of Management and Budget is responsible for Federal information security, oversight, and policy issuance.

However, OMB executes its responsibilities in close coordination with its Federal cybersecurity partners, including the Department of Homeland Security and the Department of Commerce's National Institute of Standards and Technology.

Both state and non-state actors are attempting to breach our Government and commercial systems. As President Obama said a few days ago, this problem is not going to go away. It is going to accelerate.

I think we all recognize that certifying the security of information on the Federal Government's networks and systems should remain a core focus of the administration as we here in Congress should continue to be looking at innovative solutions that provide DHS with the authorities to respond quickly to the new challenges as they arise, and Congress must continue our search for legisla-

tive initiatives that will help further protect our Nation's critical networks and systems.

As a result of the latest Government network breaches, we have been told that OMB has launched a 30-day cybersecurity sprint, a review and recommendations effort. The review team is made up of OMB, the White House E-Gov Cyber National Security Unit, the National Security Council Cybersecurity Directorate, the Department of Homeland Security, and Department of Defense, among other agencies.

As part of the effort, OMB has instructed Federal agencies to immediately take a number of steps to protect Federal information and assets and improve the resilience of Federal networks.

Specifically, Federal agencies must immediately deploy indicators provided by DHS which can identify priority threat active techniques and tactics and procedures and tools to scan systems and check logs; No. 2, patch critical vulnerabilities without delay and report to OMB and DHS on the progress and challenges within 30 days; No. 3, tighten policies and practices for privileged users; and, No. 4, dramatically accelerate implementation of multi-factor identification, especially for privileged users.

While I am pleased to see the White House taking immediate action, all of the above efforts are generally recognized as security measures that should already be in place, especially in vital Government networks.

I hope to hear today from our witnesses a clear explanation why many of the standard recognized security practices were not in place in Federal agencies and clearly identify the plan that DHS has to make sure and certify that Federal agencies' cybersecurity standards are up to date.

Of particular interest to me in my district and I know to others on this subcommittee is the status of port cybersecurity. Overall maritime ports handle more than $1.3 trillion in cargo annually. The operations of these ports are supported by information and communications systems that, like all other network systems, are susceptible to cyber-related threats.

Failures in these systems could degrade or interrupt operations at ports, including the flow of commerce. Federal agencies—in particular, DHS—and industry stakeholders have specific roles in protecting maritime facilities and ports from physical and cyber threats.

GAO did an audit last year of maritime port cybersecurity efforts to assess actions taken by DHS and two of its front-line component agencies, the U.S. Coast Guard and FEMA, as well as other Federal agencies.

The GAO found that, while the Coast Guard initiated a number of activities and coordinating strategies to improve physical security in specific ports, it has not conducted a risk assessment that fully addresses cyber-related threats, vulnerabilities, and consequences.

The report also noted that FEMA identified enhancing cybersecurity capabilities as a funding priority for the first time in 2013.

I look forward to today's testimony on both of these issues. It will be crucial that stakeholders appropriately plan and allocate re-

sources to protect ports and other maritime facilities from increasingly persistent and pervasive cyber intrusions.

With that, Mr. Chairman, I yield back.

Mr. RATCLIFFE. The gentleman yields back.

The Chairman now welcomes and recognizes the Chairman of the full committee, the gentleman from Texas, Mr. McCaul, for his opening statement.

Mr. MCCAUL. I would like to thank Chairman Ratcliffe for his leadership in holding this hearing today.

Our Government, in my opinion, is still reeling from what appears to be the most significant breach of Federal networks in U.S. history. This insidious attack was aimed at Federal employees who handle our National security, many with security clearances working to defend our country. Yet, the administration failed to defend them.

Instead, it appears that Chinese hackers were able to cut through our defenses and extract information about millions of current and former U.S. Government employees with sensitive security clearances.

As one who has filled these out in the past—I know the Chairman has as well in our tenure at the Justice Department—it is astounding to me that these very sensitive documents went unprotected by the administration.

There can be no doubt that this attack will lead to more brazen attempts to steal America's secrets. Yet, there is no telling if we will be lucky enough to spot it the next time. Clearly the administration needs to take this more seriously.

What is equally appalling to me is the administration's response. No Government employee has been held accountable. No foreign adversary has been warned. No one can say with any degree of confidence whether we can stop this from happening again.

We talk often now about how we have entered a new age that requires new rules of the road. It is very true. I think this is a watershed moment. It appears now that a foreign country has invaded our networks and stolen sensitive data.

Yet, the administration's response is not to promise retaliation. Instead, it has promised to add the issue to the agenda of this week's strategic dialogue with China. I would submit that is not strong enough. There are no consequences to the actions.

What if this had been a foreign adversary invading our territory instead of our networks to steal secrets? How would the White House respond then? What if foreign espionage, we caught them physically stealing the paper files? What would be the response? This is the same action, just in the digital world.

The abilities of our cyber adversaries are no secret. The alarm bell has been going off for years. In 2012, Iran hackers hit Saudi Arabia's national oil company, Aramco, destroying 30,000 computers.

Iran has targeted major U.S. banks to shut down websites and restrict Americans' ability to access their accounts. We have seen intrusions into Target, Neiman Marcus, Home Depot, J.P. Morgan. All these were designed to steal the personal information of private citizens.

In December, North Korea used a digital bomb to destroy computer systems at Sony Pictures, an attack that was destructive, but also a cowardly attempt to stifle our freedom of expression.

In just this year we have seen the breaches of two major health care companies, Anthem and Premera, that together affected up to 90 million Americans.

I hope this latest breach will stir our Government to action and, quite frankly, the Congress in a frank acknowledgment that we have fallen behind.

Our Government is responsible for providing for the common defense under the Constitution, and that also means defending our cyber space.

During the last Congress, I led the efforts to strengthen our cybersecurity foundations, and we managed to get five key cybersecurity bills passed into law. We did this with the support of both industry and privacy advocates.

This year we passed legislation in the House to enhance cyber threat information sharing, which possibly could have prevented this attack from occurring if we had the signature threat information to block the breach from China.

In light of this attack—you know, we always say around here it is going to take a big event for Congress to act. I think the big event has happened and now it is time for Congress to act.

The House has acted. It is now time for the Senate to act and pass the bill that we passed out of the House with overwhelming bipartisan support, 355 votes, supported by both industry and privacy.

The Department of Homeland Security has several cyber tools to defend these networks, such as the EINSTEIN and the Continuous Diagnostics and Mitigation program that were authorized in our bill as well.

But these are only effective if they have been deployed to our sprawling and disparate Federal networks. As of now, only half of the Federal civilian agencies have deployed the latest version of EINSTEIN.

I know, Dr. Ozment, you and I have talked about this. I commend your efforts in expanding this now. Getting just to the 50 percent was quite an accomplishment. But I think we want to hear about the expansion all across the Federal Government, which I think would protect the networks better.

This digital frontier and safeguarding it is one of our leading National security challenges of our time, and we, as Americans, need to apply the same innovation, discipline, and creativity that produced the information age into protecting what we have created.

I want to thank the Chairman again for holding this hearing. With that, I yield back.

Mr. RATCLIFFE. I thank the Chairman.

Other Members of the committee are reminded that opening statements may be submitted for the record.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

JUNE 24, 2015

I thank the leadership of this subcommittee for continuing to focus on our Nation's most pressing cyber vulnerabilities—protecting our Nation's critical infrastructure systems, and protecting citizens and Federal workers and their personal information. Over the past few months, the committee has found the repeated news that some of our most valuable Government agencies have been infiltrated, and Government employees' detailed personal information have been exposed quite appalling.

We have seen the Internal Revenue Service breached. At the Defense Department, Secretary Carter has told us about the Russian's hacking from earlier this year, and now, we have a multi-layered exposure of Federal workers exposed in an Office of Personnel Management incident. Our networks and databases cannot be protected by one protocol, one sophisticated procedure, or one magic arrow. We have cybersecurity programs in place, but for them to take hold, either in the private sector or across Government agencies, it will require leadership, cooperation, and accountability. For example, the President's cybersecurity Executive Order 13636 has charged the Department of Homeland Security to be the motivator, teacher, and implementer of the art and science of network and database security, across the Federal Government.

However, for DHS to fulfill this mission, it has to engage with both the public and private sectors. I want to hear more from Dr. Ozment on how DHS is fulfilling this mission, and how it has responded to previous intrusions. It is important for all of us to remember that cybersecurity is a shared responsibility, and that no single approach can protect us completely. Cyber threat protection is a complex and incomplete process and it crosses several important intersections, especially regarding privacy and civil liberties.

As people and Government become more dependent on technology, technology-based opportunities for crime, espionage, and physical disruption will most certainly increase. Today, some contend that greater security means ceding some degree of personal privacy, or vice versa. But in my book, cybersecurity enables privacy—because it protects individuals, companies, and governments from malicious intrusions. Privacy and security are not competing interests; we can and must do both. The United States can set a positive example regarding the role that cybersecurity standards play globally, for both industry and Government. If we can develop effective, secure protocols and standards that are easily implemented, it will represent an important opportunity for U.S. products around the globe.

Finally, I would be remiss if I did not mention the cost of these programs discussed today. All of this cybersecurity effort does not come cheap. While the majority has seen fit to increase cybersecurity funding by large amounts in some cases, House and Senate Republicans have started to show how they plan to budget at discretionary levels for other programs.

Compared to the President's budget, their budget will force cuts in areas critical to the economy, as well as in National security priorities. Homeland security, peacekeeping efforts, defense, and foreign assistance will be impacted. These funding levels are the result of Congressional Republicans' decision to lock in the funding cuts imposed by sequestration. As we all know, sequestration was never intended to take effect: Rather, it was supposed to threaten such drastic cuts to both defense and non-defense funding that policymakers would be motivated to come to the table and reduce the deficit through smart, balanced reforms. Unfortunately, the bills and appropriations targets released to date double-down on a very different approach.

Mr. RATCLIFFE. We are pleased to have with us today a panel of distinguished witnesses on this important topic.

Dr. Andy Ozment is the assistant secretary for the Office of Cybersecurity and Communications within the National Protections and Programs Directorate at the United States Department of Homeland Security.

Welcome back, Dr. Ozment.

Mr. Greg Wilshusen is the director for information security issues at the Government Accountability Office.

We're glad to have you with us today, sir.

At this time I will ask both witnesses to stand and raise your right hand so that I may swear you in to provide testimony.

[Witnesses sworn.]

Mr. RATCLIFFE. You may be seated.

The witnesses' full written statements will appear in the record.

The Chairman now recognizes Dr. Ozment for 5 minutes for his opening statement.

STATEMENT OF ANDY OZMENT, ASSISTANT SECRETARY, OFFICE OF CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTIONS AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY

Mr. OZMENT. Thank you, Chairman Ratcliffe, Ranking Member Richmond, and Chairman McCaul, Members of the committee. I appreciate the opportunity to appear before you today.

Like you, my fellow panelists, and countless Americans, I am deeply concerned about the recent compromise at OPM, and I am dedicated to ensuring that we take all necessary steps to protect our Federal workforce and to drive forward the cybersecurity of the entire Federal Government.

As a result, I want to focus these remarks on how DHS is accelerating our efforts to protect Federal agencies and help Federal agencies better protect themselves.

To begin, it is important to note that we are now making up for 20 years of underinvestment in cybersecurity across both the public and the private sector. At the same time, we are facing a major challenge in protecting our most sensitive information against sophisticated, well-resourced, and persistent adversaries. This is a complex problem without a simple solution.

To effectively address this challenge, our Federal agencies need to deploy defense-in-depth. Consider protecting a Government facility. Adequate security is not only a fence or a camera or locking the doors of a building, but a combination of these measures and others that, in aggregate, make it difficult for an adversary to gain physical access. Cybersecurity also requires multiple layers of security measures. No one measure is sufficient.

Under legislation passed by this Congress last year, Federal agencies are responsible for their own cybersecurity. To assist them, DHS provides a common baseline of cybersecurity across the civilian government.

It helps agencies manage their cyber risk through four key lines of effort:

First, we protect agencies by providing a common set of capabilities through the EINSTEIN and Continuous Diagnostics and Mitigation, or CDM, programs.

Second, we measure and motivate agencies to implement best practices.

Third, we serve as a hub for information sharing.

Finally, we provided incident response assistance when agencies suffer a cyber intrusion.

In my statement this morning, I will focus on the first area, how DHS provides a baseline of security through EINSTEIN and CDM. I have described the other three areas in my written statement, and I am happy to take your questions on them. Our first line of defense against cyber threats is the EINSTEIN system, which protects agencies at their perimeters.

Returning to the analogy of a Government facility that I mentioned earlier, EINSTEIN 1 is similar to a camera at the road onto the facility that records all traffic and identifies anomalies in the numbers of cars. EINSTEIN 2 adds the ability to detect suspicious cars based upon a watch list. EINSTEIN 2 does not stop the cars, but sounds the alarm if a suspicious car enters the facility.

Agencies report that EINSTEIN 1 and 2 are screening over 90 percent of all Federal civilian traffic. EINSTEIN 1 and 2 played a key role in identifying the recent compromise at the Department of Interior.

The latest phase of the program, known as EINSTEIN 3A, is akin to a guard post at the highway that leads to multiple Government facilities. EINSTEIN 3A uses Classified information to look at the cars and compare them with a watch list. EINSTEIN 3A then actively blocks prohibited cars from entering the facility.

As the Chairman noted, we are accelerating our efforts to protect all civilian agencies with EINSTEIN 3A. The system currently protects 15 Federal civilian agencies with over 930,000 Federal personnel, or approximately 45 percent of the civilian government, with at least one security countermeasure.

We have added EINSTEIN 3A protections to over 20 percent of the Federal civilian government in the last 9 months alone. During this time, EINSTEIN 3A has blocked nearly 550,000 attempts to access potentially malicious websites.

EINSTEIN 3A is a signature-based system. It can only block attacks that it knows about. This is necessary, but not sufficient, for protecting the civilian government. We are also working on adding other technology to the EINSTEIN 3A platform that can block attacks that we have not previously seen.

As we accelerate EINSTEIN deployment, we also recognize that security cannot be achieved through only one type of tool. EINSTEIN is not a silver bullet, and it will never be able to block every threat. For example, it must be complemented with tools to monitor the inside of agency networks.

Our CDM, Continuous Diagnostics and Mitigation Program, helps address this challenge. We have purchased CDM Phase 1 capabilities for 8 agencies covering over 50 percent of the Federal civilian government, and we expect to purchase CDM for 97 percent of the Federal civilian government by the end of this fiscal year.

Now, there's a caveat. The deadlines that I've just given you are when DHS will provide a capability. It takes a few additional months for each agency to fully implement both EINSTEIN and CDM once the services are available. Of course, agencies must supplement EINSTEIN and CDM with additional tools appropriate to the needs of the agency.

I want to thank you again for the legislation Congress passed in December 2014. As you know, additional legislation is needed. This committee and the House have passed a bill authorizing EINSTEIN and establishing DHS as the portal for liability-protected information-sharing between the private sector and the Government. We need information sharing and EINSTEIN authorization legislation passed.

I'd like to conclude by noting that Federal agencies are a rich target and will continue to experience frequent attempted intru-

sions. As our detection methods improve, we will detect more incidents, incidents that are already occurring, we just didn't know it yet.

The recent breach at OPM is emblematic of this trend, as OPM was able to detect the intrusion by implementing best practices recommended by DHS. We are accelerating the deployment of the tools we have, and we are bringing cutting-edge capabilities online. We are asking our partner agencies and Congress to take action and work with us to strengthen the cybersecurity of our Federal agencies.

Thank you again for the opportunity to appear before you today. I look toward to any questions.

[The prepared statement of Mr. Ozment follows:]

PREPARED STATEMENT OF ANDY OZMENT

INTRODUCTION

Chairman Ratcliffe, Ranking Member Richmond, and Members of the committee, thank you for the opportunity to appear before you today. Recent compromises clearly demonstrate the challenge facing the Federal Government in protecting our citizens' and employees' personal information against sophisticated, agile, and persistent threats. Addressing these threats is a shared responsibility. I will discuss the roles of the Department of Homeland Security (DHS) in protecting civilian Federal departments and agencies and in helping agencies better protect themselves.

THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY IN FEDERAL CYBERSECURITY

The *Federal Information Security Modernization Act of 2014* specifies that Federal agencies are responsible for their own cybersecurity. In addition, DHS has the mission to provide a common baseline of security across the civilian government and help agencies manage their cyber risk. DHS, through its National Protection and Programs Directorate (NPPD), assists agencies by providing this baseline for the Federal Government through the EINSTEIN and Continuous Diagnostics and Mitigation (CDM) programs, by measuring and motivating agencies to implement best practices, by serving as a hub for information sharing, and by providing incident response assistance when agencies suffer a cyber intrusion. I will discuss each of these in turn. NPPD has two additional cybersecurity customers besides the Federal Government: Private-sector infrastructure owners and operators, and State, local, Tribal, and territorial governments. While several of the capabilities outlined below, such as information sharing and best practices, apply to all three customers, this statement focuses on NPPD's approach to Federal cybersecurity in the context of the recent compromise at OPM.

EINSTEIN

EINSTEIN protects agencies' unclassified networks at the perimeter of each agency. Furthermore, EINSTEIN provides situational awareness across the Government, as threats detected in one agency are shared with all others so they can take appropriate protective action. The U.S. Government could not achieve such situational awareness through individual agency efforts alone.

The first two versions of EINSTEIN—EINSTEIN 1 and 2—identify abnormal network traffic patterns and detect known malicious traffic. This capability is fully deployed and screening all Federal civilian traffic that is routed through a Trusted Internet Connection (a secure gateway between each agency's internal network and the internet). EINSTEIN 3 Accelerated (EINSTEIN 3A), which actively blocks known malicious traffic, is currently being deployed through the primary Internet Service Providers serving the Federal Government. EINSTEIN 1 and 2 use only Unclassified information, while EINSTEIN 3A uses Classified information. Using Classified indicators allows EINSTEIN 3A to detect and block many of the most significant cybersecurity threats. We are working aggressively to ensure that all agencies are protected by EINSTEIN 3A, including by implementing alternative deployment options that address the inability of some Internet Service Providers to implement EINSTEIN 3A in a sufficiently timely manner.

We are now accelerating our efforts and making significant progress in implementing EINSTEIN 3A across the Federal Government. The system now protects 15 Federal civilian departments and agencies and over 930,000 Federal personnel

with at least one of its two security "countermeasures." Thus, EINSTEIN 3A protects approximately 45% of the civilian government—a 20% increase over the past 9 months alone. During this time, EINSTEIN 3A has blocked nearly 550,000 attempts to access potentially malicious web sites via one of its countermeasures. Any one of these blocked attempts could have conceivably resulted in an incident of severe consequence.

As we fully deploy EINSTEIN 3A, we are also mindful that to stay ahead of the adversary, we must go beyond the current approach that uses indicators of known threats. To that end, we are developing advanced malware and behavioral analysis capabilities that will automatically identify and separate suspicious traffic for further inspection, even if the precise indicator has not been seen before. We are examining best-in-class technologies from the private sector to evolve to this next stage of network defense. As I will discuss later, EINSTEIN played a key role in understanding the recent compromise at OPM.

Continuous Diagnostics and Mitigation (CDM)

Security cannot be achieved through only one type of tool. That is why security professionals believe in defense-in-depth: Employing multiple tools to, in combination, manage the risks of cyber attacks. EINSTEIN is a perimeter system, but it will never be able to block every threat. For example, it must be complemented with systems and tools inside agency networks. Through the CDM program, DHS provides Federal civilian agencies with tools to monitor agencies' internal networks. CDM is divided into three phases:

- CDM Phase 1 identifies vulnerabilities on computers and software on agency networks.
- CDM Phase 2 will monitor users on agencies' networks and detect if they are engaging in unauthorized activity.
- CDM Phase 3 will assess activity happening inside of agencies' networks to identify anomalies and alert security personnel.

We have provided CDM Phase 1 capabilities to 8 agencies, covering over 50% of the Federal civilian government. We expect to purchase CDM for 97% of the Federal civilian government by the end of this fiscal year. CDM will provide an invaluable tool in helping agencies protect against cybersecurity compromises. Although NPPD provides both EINSTEIN 3A and CDM capabilities to Federal civilian agencies, each agency must still take action to implement these systems. In some cases, it may take agencies some months to fully implement a given capability once it is made available by DHS.

For example, a vignette from the current incident may be useful to illustrate how EINSTEIN and CDM jointly help protect Federal agencies:

- As soon as OPM identified malicious activity on their network, they shared this information with DHS. NPPD then developed a signature for the particular threat, and used EINSTEIN 2 to look back in time for other compromises across the Federal civilian government. Through this process, we identified a potential compromise at another location with OPM data that would not have been identified and mitigated as quickly without the EINSTEIN system. We then used the EINSTEIN 1 system to determine whether data exfiltration had occurred.
- This same threat information is used by EINSTEIN 3A to block potential threats from impacting Federal networks. Thus, DHS used EINSTEIN 3A to ensure that this cyber threat could not exploit other agencies protected by the system. As noted, DHS is accelerating EINSTEIN 3A deployment across the Federal Government. While it is challenging to estimate the potential impact of a prevented event, each of these malicious DNS requests or emails that were blocked by EINSTEIN 3A may conceivably have led to a cybersecurity compromise of severe consequence.
- When implemented across the Federal Government, CDM will help agencies identify and prioritize vulnerabilities within their network. For example, CDM would have helped OPM identify any vulnerabilities within its database of Federal personnel information and mitigate those vulnerabilities before they could be exploited by an adversary.

Measuring and Motivating Agencies to Adopt Best Practices

Many cybersecurity incidents can be avoided by simple measures. Implementing best practices is the foundation of cybersecurity. DHS works closely with individual agencies and governance bodies such as the Federal Chief Information Officer (CIO) Council to motivate agencies to implement best practices and to measure their progress in reaching particular goals and outcomes. Examples of best practices include patching critical vulnerabilities, implementing workforce training and awareness programs, and using multi-factor authentication. Secretary Johnson recently

issued a Binding Operational Directive, based upon authority provided by Congress in the *Federal Information Security Modernization Act of 2014,* which directed civilian agencies to promptly patch vulnerabilities on their internet-facing devices. These vulnerabilities are identified by recurring scans conducted by the DHS National Cybersecurity and Communications Integration Center (NCCIC). These vulnerabilities are accessible from the internet, and thus present a significant risk if not quickly addressed. Agencies have responded quickly in implementing Secretary Johnson's directive, as over half of the stale critical vulnerabilities that existed when the Directive was issued have been mitigated within the 20 days since its issuance.

Under the authority provided by Congress in last year's FISMA legislation, DHS has a statutory role in developing, implementing, and evaluating operational cybersecurity guidance, in conjunction with the Office of Management and Budget. In this role, DHS leverages metrics, consultation, and strategic engagements with agency CIOs and Chief Information Security Officers (CISOs) to motivate agencies toward better cybersecurity. In fact, OPM was able to first identify the recent compromise of its network based upon technical recommendations provided by NPPD.

Information Sharing

Information sharing is an essential aspect of NPPD's cybersecurity role. By sharing information quickly and widely, we help other agencies block cyber threats before damaging incidents occur. Equally importantly, the information we receive from other agencies and the private sector help us understand emerging risks and develop effective protective measures. Our NCCIC is the civilian government's hub for cybersecurity information sharing, incident response, and coordination. In fiscal year 2015, the NCCIC has disseminated over 6,000 alerts, warnings, and bulletins.

To effectively combat sophisticated and agile adversaries, we must share information quickly enough to block threats before they can penetrate Federal networks. We now have a system to automate our sharing of cyber threat indicators, and we are working aggressively to build this capability across Government and to the private sector so we can share this information in near-real-time. One agency is already receiving cyber threat information via this automated system. We expect that multiple agencies and private-sector partners will begin sharing and receiving information through this system by the end of October, 2015. As more agencies join us in automated information sharing, we will increase our adversaries' cost and reduce the prevalence of damaging incidents across the Federal Government and the private sector.

Incident Response

Cybersecurity is about risk management, and we cannot eliminate all risk. Agencies that implement best practices and share information will increase the cost for adversaries and stop many threats. But ultimately, there exists no perfect cyber defense, and persistent adversaries will find ways to infiltrate networks in both Government and the private sector. When an incident does occur, the NCCIC offers on-site assistance to find the adversary, drive them out, and restore service. In fiscal year 2015, the NCCIC has already provided on-site incident response to 32 incidents—nearly double the total in all of fiscal year 2014. The NCCIC also coordinate responses to significant incidents to give senior leaders a clear understanding of the situation and give operators the information they need to respond effectively. Similar to the recent incident at OPM, providing on-site incident response assistance also allows the NCCIC to identify indicators of compromise that can then be shared with other agencies and applied to EINSTEIN for broad protection across the Federal Government.

CYBERSECURITY LEGISLATION

Last year, Congress acted in a bipartisan manner to pass critical cybersecurity legislation that enhanced the ability of the Department of Homeland Security to work with the private sector and other Federal civilian departments in each of their own cybersecurity activities, and enhanced the Department's cyber workforce authorities. As I noted, DHS is using the authority granted in one of those bills—the Federal Information Security Modernization Act of 2014—to direct Federal civilian Executive branch agencies to fix critical vulnerabilities on their Internet-facing devices.

Additional legislation is needed. I previously highlighted EINSTEN's key role in identifying and mitigating an additional potential compromise during the OPM activity. The Department and administration have a long-standing request of Congress to remove obstacles to the EINSTEIN program's deployment across Federal civilian agency information systems by codifying the program's authorities and resolving lingering concerns among certain agencies. Some agencies have questioned

how deployment of EINSTEIN under DHS authority relates to their existing statutory restrictions on the use and disclosure of agency data. DHS and the administration are seeking statutory changes to clarify this uncertainty and to ensure agencies understand that they can disclose their network traffic to DHS for narrowly-tailored purposes to protect agency networks, while making clear that privacy protections for the data will remain in place. I look forward to working with Congress to further clarify DHS's authority to rapidly and efficiently deploy this protective technology.

In addition, carefully updating laws to facilitate cybersecurity information sharing within the private sector and between the private and Government sectors is also essential to improving the Nation's cybersecurity. While many companies currently share cybersecurity threat information under existing laws, there is a heightening need to increase the volume and speed of information shared without sacrificing the trust of the American people or the protection of privacy, confidentiality, civil rights, or civil liberties. It is essential to ensure that cyber threat information can be collated quickly in the NCCIC, analyzed, and shared quickly among trusted partners, including with law enforcement, so that network owners and operators can take necessary steps to block threats and avoid damage.

CONCLUSION

Federal agencies are a rich target and will continue to experience frequent attempted intrusions. This problem is not unique to the Government—it is shared across a global cybersecurity community. The key to good cybersecurity is awareness and constant vigilance at machine speed. As our detection methods continue to improve, more events will come to light. The recent breach at OPM is emblematic of this trend, as OPM was able to detect the intrusion by implementing cybersecurity best practices recommended by DHS. As network defenders are able to see and thwart more events, we will inevitably identify more malicious activity and thwart the adversary's attempts to access sensitive information and systems. We are facing a major challenge in protecting our most sensitive information against sophisticated, well-resourced, and persistent adversaries. In response, we are accelerating deployment of the tools we have and are working to bring cutting-edge capabilities on-line. We are asking our partner agencies and Congress to take action and work with us to strengthen the cybersecurity of our Federal agencies.

Mr. RATCLIFFE. Thank you, Dr. Ozment.

The Chair now recognizes Mr. Wilshusen for 5 minutes for his opening statement.

STATEMENT OF GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

Mr. WILSHUSEN. Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, thank you for the opportunity to testify at today's hearing on DHS's efforts to secure the .gov domain.

As you know, the Federal Government faces an array of cyber-based threats to its computer networks and systems, as illustrated by the recent OPM data breaches which affected millions of Federal employees. Such incidents underscore the urgent need for effective implementation of information security programs at Federal agencies.

Since 1997, we have designated Federal information security as a Government-wide high-risk area and, in 2003, expanded the area to include computerized systems supporting the Nation's critical infrastructure. We further expanded this area in 2015 to include protecting the privacy of personally identifiable information.

Today I will discuss several cybersecurity challenges facing Federal agencies and Government-wide initiatives, including those led by DHS aimed at improving agency cybersecurity.

Before I begin, Mr. Chairman, if I may, I'd like to recognize several members of my team who were instrumental in developing my statement and some of the work underpinning it.

With me today is Larry Crosland, who is an assistant director who led this work. Also, Brad Becker, Rosanna Guerrero, Lee McCracken, Kush Malhotra, Chris Businsky, and Scott Pettis also made significant contributions.

Mr. Chairman, most Federal agencies face challenges securing their computer networks and systems. One such challenge is designing and implementing risk-based cybersecurity programs.

Agencies continue to have shortcomings in assessing risks, developing and implementing security controls, and monitoring results. Nineteen of 24 agencies covered by the CFO Act reported that information security weaknesses were either a significant deficiency or material weakness for financial reporting purposes. In addition, IGs at 23 of these agencies cited information security as a major management challenge for their agency.

Overseeing security of contractor-operated systems is another challenge. Agencies rely on contractors to perform a wide variety of IT services. However, five of six agencies we reviewed did not consistently assess or review assessments of their contractors' information security practices and controls, resulting in security lapses.

Even with effective control, security incidents and data breaches can still occur. Agencies need to react swiftly and appropriately when they do. However, seven agencies we reviewed had not consistently implemented key operational practices for responding to data breaches involving personally identifiable information.

GAO and agency IGs have made hundreds of recommendations to assist agencies in addressing these and other challenges. Implementing these recommendations will strengthen agencies' ability to protect their systems and information.

DHS and OMB have also launched several Government-wide initiatives to enhance cybersecurity. One such initiative is requiring strong authentication of users through the use of personal identity verification, or PIV, cards.

These cards provide a more secure method of verifying a user's identity than do passwords. However, OMB recently reported that only 41 percent of agency user accounts at 23 civilian agencies required PIV cards for accessing agency systems.

DHS' Continuous Diagnostics and Mitigation Initiative is intended to provide agencies with tools that identify and prioritize cyber risk on an on-going basis and enable cybersecurity personnel to mitigate the most significant programs or problems first. If effectively implemented, the initiative may assist agencies in resolving long-standing security weaknesses.

The National Cybersecurity Protection System is intended to detect and prevent malicious network traffic from entering Federal civilian networks, among other things. GAO is presently reviewing the implementation of this system. Our preliminary observations indicate that the system's intrusion detection and prevention capabilities may be useful, but are also limited.

While Government-wide initiatives hold promise for bolstering the Federal cybersecurity posture, no single technology or set of

practices is sufficient to protect against all cyber threats. A multi-layered defense-in-depth strategy that includes well-trained personnel, effective and consistently applied processes, and appropriate technologies is needed to better manage these risks.

This concludes my statement. I'd be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

PREPARED STATEMENT OF GREGORY C. WILSHUSEN

JUNE 24, 2015

CYBERSECURITY.—RECENT DATA BREACHES ILLUSTRATE NEED FOR STRONG CONTROLS ACROSS FEDERAL AGENCIES

GAO–15–725T

Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee: Thank you for inviting me to testify at today's hearing on the Department of Homeland Security's (DHS) efforts to secure Federal information systems. As you know, the Federal Government faces an array of cyber-based threats to its systems and data, as illustrated by the recently-reported data breaches at the Office of Personnel Management (OPM), which affected millions of current and former Federal employees. Such incidents underscore the urgent need for effective implementation of information security controls at Federal agencies.

Since 1997, we have designated Federal information security as a Government-wide high-risk area, and in 2003 expanded this area to include computerized systems supporting the Nation's critical infrastructure. Most recently, in the 2015 update to our high-risk list, we further expanded this area to include protecting the privacy of personally identifiable information (PII)[1]—that is, personal information that is collected, maintained, and shared by both Federal and non-Federal entities.[2]

My statement today will discuss: (1) Cybersecurity challenges that Federal agencies face in securing their systems and information and (2) Government-wide initiatives, including those led by DHS, aimed at improving agencies' cybersecurity. In preparing this statement, we relied on our previous work in these areas, as well as the preliminary observations from our on-going review of DHS's EINSTEIN initiative. We discussed these observations with DHS officials. The prior reports cited throughout this statement contain detailed discussions of the scope of the work and the methodology used to carry it out. All the work on which this statement is based was conducted or is being conducted 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.

BACKGROUND

As computer technology has advanced, both Government and private entities have become increasingly dependent on computerized information systems to carry out operations and to process, maintain, and report essential information. Public and private organizations rely on computer systems to transmit proprietary and other sensitive information, develop and maintain intellectual capital, conduct operations, process business transactions, transfer funds, and deliver services. In addition, the internet has grown increasingly important to American business and consumers, serving as a medium for hundreds of billions of dollars of commerce each year, and has developed into an extended information and communications infrastructure that supports vital services such as power distribution, health care, law enforcement, and National defense.

Ineffective protection of these information systems and networks can result in a failure to deliver these vital services, and result in:

- loss or theft of computer resources, assets, and funds;

[1] Personally identifiable information is information about an individual, including information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, mother's maiden name, or biometric records, and any other personal information that is linked or linkable to an individual.

[2] See GAO, *High-Risk Series: An Update,* GAO–15–290 (Washington, DC: Feb. 11, 2015).

- inappropriate access to and disclosure, modification, or destruction of sensitive information, such as National security information, PII, and proprietary business information;
- disruption of essential operations supporting critical infrastructure, National defense, or emergency services;
- undermining of agency missions due to embarrassing incidents that erode the public's confidence in Government;
- use of computer resources for unauthorized purposes or to launch attacks on other systems;
- damage to networks and equipment; and
- high costs for remediation.

Recognizing the importance of these issues, Congress enacted laws intended to improve the protection of Federal information and systems. These laws include the Federal Information Security Modernization Act of 2014 (FISMA),[3] which, among other things, authorizes DHS to: (1) Assist the Office of Management and Budget (OMB) with overseeing and monitoring agencies' implementation of security requirements; (2) operate the Federal information security incident center; and (3) provide agencies with operational and technical assistance, such as that for continuously diagnosing and mitigating cyber threats and vulnerabilities. The act also reiterated the 2002 FISMA requirement for the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the agency's information or information systems. In addition, the act requires Federal agencies to develop, document, and implement an agency-wide information security program. The program is to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Cyber Threats to Federal Systems

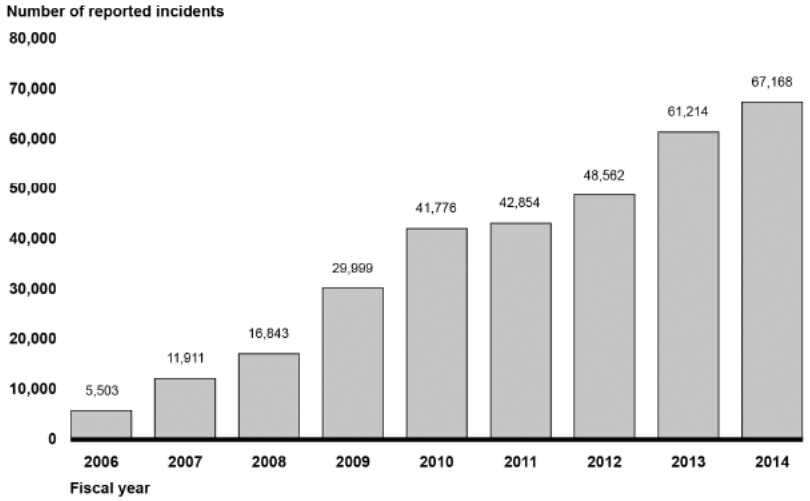
Risks to cyber-based assets can originate from unintentional or intentional threats. Unintentional threats can be caused by, among other things, natural disasters, defective computer or network equipment, and careless or poorly-trained employees. Intentional threats include both targeted and untargeted attacks from a variety of sources, including criminal groups, hackers, disgruntled employees, foreign nations engaged in espionage and information warfare, and terrorists.

These adversaries vary in terms of their capabilities, willingness to act, and motives, which can include seeking monetary gain or a political, economic, or military advantage. For example, adversaries possessing sophisticated levels of expertise and significant resources to pursue their objectives—sometimes referred to as "advanced persistent threats"—pose increasing risks. They make use of various techniques—or exploits—that may adversely affect Federal information, computers, software, networks, and operations.

Since fiscal year 2006, the number of information security incidents affecting systems supporting the Federal Government has steadily increased each year: Rising from 5,503 in fiscal year 2006 to 67,168 in fiscal year 2014, an increase of 1,121 percent (see fig. 1).

[3] The Federal Information Security Modernization Act of 2014 (Pub. L. No. 113–283, Dec. 18, 2014) largely superseded the very similar Federal Information Security Management Act of 2002 (Title III, Pub. L. No. 107–347, Dec. 17, 2002).

Figure 1: Incidents Reported to the U.S. Computer Emergency Readiness Team by Federal Agencies, Fiscal Years 2006 through 2014



Source: GAO analysis of United States Computer Emergency Readiness Team data for fiscal years 2006-2014. | GAO-15-725T

Furthermore, the number of reported security incidents involving PII at Federal agencies has more than doubled in recent years—from 10,481 incidents in fiscal year 2009 to 27,624 incidents in fiscal year 2014. These incidents and others like them can adversely affect National security; damage public health and safety; and lead to inappropriate access to and disclosure, modification, or destruction of sensitive information. Recent examples highlight the impact of such incidents:

- In June 2015, OPM reported that an intrusion into its systems affected personnel records of about 4 million current and former Federal employees. The director of OPM also stated that a separate incident may have compromised OPM systems related to background investigations, but its scope and impact have not yet been determined.
- In June 2015, the commissioner of the Internal Revenue Service (IRS) testified that unauthorized third parties had gained access to taxpayer information from its "Get Transcript" application. According to IRS, criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts. These data included Social Security information, dates of birth, and street addresses.
- In April 2015, the Department of Veterans Affairs (VA) Office of Inspector General reported that two VA contractors had improperly accessed the VA network from foreign countries using personally-owned equipment.
- In February 2015, the Director of National Intelligence stated that unauthorized computer intrusions were detected in 2014 on OPM's networks and those of two of its contractors. The two contractors were involved in processing sensitive PII related to National security clearances for Federal employees.
- In September 2014, a cyber-intrusion into the United States Postal Service's information systems may have compromised PII for more than 800,000 of its employees.

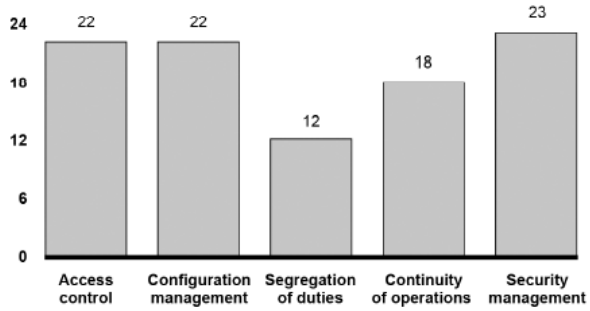
FEDERAL AGENCIES FACE ON-GOING CYBERSECURITY CHALLENGES

Given the risks posed by cyber threats and the increasing number of incidents, it is crucial that Federal agencies take appropriate steps to secure their systems and information. We and agency inspectors general have identified challenges in protecting Federal information and systems, including those in the following key areas:

- *Designing and implementing risk-based cybersecurity programs at Federal agencies.*.—Agencies continue to have shortcomings in assessing risks, developing and implementing security controls, and monitoring results. Specifically, for fiscal year 2014, 19 of the 24 Federal agencies covered by the Chief Financial Offi-

cers (CFO) Act[4] reported that information security control deficiencies were either a material weakness or a significant deficiency in internal controls over their financial reporting.[5] Moreover, inspectors general at 23 of the 24 agencies cited information security as a major management challenge for their agency. As we testified in April 2015, for fiscal year 2014, most of the agencies had weaknesses in the five key security control categories.[6] These control categories are: (1) Limiting, preventing, and detecting inappropriate access to computer resources; (2) managing the configuration of software and hardware; (3) segregating duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an on-going basis. (See fig. 2.)

Figure 2: Information Security Weaknesses at 24 Federal Agencies for Fiscal Year 2014



Source: GAO analysis of agencies, Inspector General and GAO reports as of April 17, 2015. | GAO-15-725T

Examples of these weaknesses include: (1) Granting users access permissions that exceed the level required to perform their legitimate job-related functions; (2) not ensuring that only authorized users can access an agency's systems; (3) not using encryption to protect sensitive data from being intercepted and compromised; (4) not updating software with the current versions and latest security patches to protect against known vulnerabilities; and (5) not ensuring employees were trained commensurate with their responsibilities. GAO and agency inspectors general have made hundreds of recommendations to agencies aimed at improving their implementation of these information security controls.

- *Enhancing oversight of contractors providing IT services*.—In August 2014, we reported that five of six agencies we reviewed were inconsistent in overseeing

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

[5] A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or combination of control deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[6] GAO, *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems,* GAO–15–573T (Washington, DC: Apr. 22, 2015).

assessments of contractors' implementation of security controls.[7] This was partly because agencies had not documented IT security procedures for effectively overseeing contractor performance. In addition, according to OMB, 16 of 24 agency inspectors general determined that their agency's program for managing contractor systems lacked at least one required element. We recommended that OMB, in conjunction with DHS, develop and clarify guidance to agencies for annually reporting the number of contractor-operated systems and that the reviewed agencies establish and implement IT security oversight procedures for such systems. OMB did not comment on our report, but the agencies generally concurred with our recommendations.

- *Improving security incident response activities*.—In April 2014, we reported that the 24 agencies did not consistently demonstrate that they had effectively responded to cyber incidents.[8] Specifically, we estimated that agencies had not completely documented actions taken in response to detected incidents reported in fiscal year 2012 in about 65 percent of cases.[9] In addition, the 6 agencies we reviewed had not fully developed comprehensive policies, plans, and procedures to guide their incident response activities. We recommended that OMB address agency incident response practices Government-wide and that the 6 agencies improve the effectiveness of their cyber incident response programs. The agencies generally agreed with these recommendations. We also made two recommendations to DHS concerning Government-wide incident response practices. DHS concurred with the recommendations and, to date, has implemented one of them.
- *Responding to breaches of PII*.—In December 2013, we reported that 8 Federal agencies had inconsistently implemented policies and procedures for responding to data breaches involving PII.[10] In addition, OMB requirements for reporting PII-related data breaches were not always feasible or necessary. Thus, we concluded that agencies may not be consistently taking actions to limit the risk to individuals from PII-related data breaches and may be expending resources to meet OMB reporting requirements that provide little value. We recommended that OMB revise its guidance to agencies on responding to a PII-related data breach and that the reviewed agencies take specific actions to improve their response to PII-related data breaches. OMB neither agreed nor disagreed with our recommendation; four of the reviewed agencies agreed, two partially agreed, and two neither agreed nor disagreed.
- *Implementing security programs at small agencies*.—In June 2014, we reported that six small agencies (i.e., agencies with 6,000 or fewer employees) had not implemented or not fully implemented their information security programs.[11] For example, key elements of their plans, policies, and procedures were outdated, incomplete, or did not exist, and two of the agencies had not developed an information security program with the required elements. We recommended that OMB include a list of agencies that did not report on the implementation of their information security programs in its annual report to Congress on compliance with the requirements of FISMA, and include information on small agencies' programs. OMB generally concurred with our recommendations. We also recommended that DHS develop guidance and services targeted at small agencies. DHS has implemented this recommendation.

Until Federal agencies take actions to address these challenges— including implementing the hundreds of recommendations we and inspectors general have made— Federal systems and information will be at an increased risk of compromise from cyber-based attacks and other threats.

GOVERNMENT-WIDE CYBERSECURITY INITIATIVES PRESENT POTENTIAL BENEFITS AND CHALLENGES

In addition to the efforts of individual agencies, DHS and OMB have several initiatives under way to enhance cybersecurity across the Federal Government. While these initiatives all have potential benefits, they also have limitations.

---

[7] GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls,* GAO–14–612 (Washington, DC: Aug. 8, 2014).

[8] GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices,* GAO–14–354 (Washington, DC: Apr. 30, 2014).

[9] This estimate was based on a statistical sample of cyber incidents reported in fiscal year 2012, with 95 percent confidence that the estimate falls between 58 and 72 percent.

[10] GAO, *Information Security: Agency Responses to Breaches of Personally Identifiable Information Need to Be More Consistent,* GAO–14–34 (Washington, DC: Dec. 9, 2013).

[11] GAO, *Information Security: Additional Oversight Needed to Improve Programs at Small Agencies,* GAO–14–344 (Washington, DC: June 25, 2014).

Personal Identity Verification.—In August 2004, Homeland Security Presidential Directive 12 ordered the establishment of a mandatory, Government-wide standard for secure and reliable forms of identification for Federal Government employees and contractor personnel who access Government-controlled facilities and information systems. Subsequently, the National Institute of Standards and Technology (NIST) defined requirements for such personal identity verification (PIV) credentials based on "smart cards"—plastic cards with integrated circuit chips to store and process data—and OMB directed Federal agencies to issue and use PIV credentials to control access to Federal facilities and systems.

In September 2011, we reported that OMB and the 8 agencies in our review had made mixed progress for using PIV credentials for controlling access to Federal facilities and information systems.[12] We attributed this mixed progress to a number of obstacles, including logistical problems in issuing PIV credentials to all agency personnel and agencies not making this effort a priority. We made several recommendations to the 8 agencies and to OMB to more fully implement PIV card capabilities. Although 2 agencies did not comment, 7 agencies agreed with our recommendations or discussed actions they were taking to address them. For example, we made 4 recommendations to DHS, who concurred and has taken action to implement them. In February 2015, OMB reported that, as of the end of fiscal year 2014, only 41 percent of agency user accounts at the 23 civilian CFO Act agencies required PIV cards for accessing agency systems.[13]

Continuous Diagnostics and Mitigation (CDM).—According to DHS, this program is intended to provide Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an on-going basis, prioritize these risks based on potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. These tools include sensors that perform automated searches for known cyber vulnerabilities, the results of which feed into a dashboard that alerts network managers. These alerts can be prioritized, enabling agencies to allocate resources based on risk. DHS, in partnership with the General Services Administration, has established a Government-wide contract that is intended to allow Federal agencies (as well as State, local, and Tribal governmental agencies) to acquire CDM tools at discounted rates.

In July 2011, we reported on the Department of State's (State) implementation of its continuous monitoring program, referred to as iPost.[14] We determined that State's implementation of iPost had improved visibility over information security at the Department and helped IT administrators identify, monitor, and mitigate information security weaknesses. However, we also noted limitations and challenges with State's approach, including ensuring that its risk-scoring program identified relevant risks and that iPost data were timely, complete, and accurate. We made several recommendations to improve the implementation of the iPost program, and State partially agreed.

National Cybersecurity Protection System (NCPS).—The National Cybersecurity Protection System, operationally known as "EINSTEIN," is a suite of capabilities intended to detect and prevent malicious network traffic from entering and exiting Federal civilian Government networks. The EINSTEIN capabilities of NCPS are described in table 1.[15]

TABLE 1.—NATIONAL CYBERSECURITY PROTECTION SYSTEM EINSTEIN CAPABILITIES

Operational Name	Capability Intended	Description
EINSTEIN 1	Network Flow	Provides an automated process for collecting, correlating, and analyzing agencies' computer network traffic information from sensors installed at their internet connections.*

[12] GAO, *Personal ID Verification: Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards,* GAO–11–751 (Washington, DC: Sept. 20, 2011).

[13] OMB, *Annual Report to Congress: Federal Information Security Management Act* (Washington, DC: Feb. 27, 2015).

[14] GAO, *Information Security: State Has Taken Steps to Implement a Continuous Monitoring Application, but Key Challenges Remain,* GAO–11–149 (Washington, DC: July 8, 2011).

[15] In addition to the EINSTEIN capabilities listed in table 1, NCPS also includes a set of capabilities related to analytics and information sharing.

TABLE 1.—NATIONAL CYBERSECURITY PROTECTION SYSTEM EINSTEIN CAPABILITIES—Continued

Operational Name	Capability Intended	Description
EINSTEIN 2	Intrusion Detection	Monitors Federal agency internet connections for specific predefined signatures of known malicious activity and alerts US–CERT when specific network activity matching the predetermined signatures is detected.**
EINSTEIN 3 Accelerated.	Intrusion Prevention	Automatically blocks malicious traffic from entering or leaving Federal civilian Executive branch agency networks. This capability is managed by internet service providers, who administer intrusion prevention and threat-based decision-making using DHS-developed indicators of malicious cyber activity to develop signatures.***

Source.—GAO analysis of DHS documentation and prior GAO reports. GAO–15–725T

* The network traffic information includes source and destination Internet Protocol addresses used in the communication, source and destination ports, the time the communication occurred, and the protocol used to communicate.

** Signatures are recognizable, distinguishing patterns associated with cyber attacks such as a binary string associated with a computer virus or a particular set of keystrokes used to gain unauthorized access to a system.

*** An indicator is defined by DHS as human-readable cyber data used to identify some form of malicious cyber activity. These data may be related to Internet Protocol addresses, domains, e-mail headers, files, and character strings. Indicators can be either Classified or Unclassified.

In March 2010, we reported that while agencies that participated in EINSTEIN 1 improved their identification of incidents and mitigation of attacks, DHS lacked performance measures to understand if the initiative was meeting its objectives.[16] We made four recommendations regarding the management of the EINSTEIN program, and DHS has since taken action to address them.

Currently, we are reviewing NCPS, as mandated by Congress. The objectives of our review are to determine the extent to which: (1) NCPS meets stated objectives, (2) DHS has designed requirements for future stages of the system, and (3) Federal agencies have adopted the system. Our final report is expected to be released later this year, and our preliminary observations include the following:

- DHS appears to have developed and deployed aspects of the intrusion detection and intrusion prevention capabilities, but potential weaknesses may limit their ability to detect and prevent computer intrusions. For example, NCPS detects signature anomalies using only one of three detection methodologies identified by NIST (signature-based, anomaly-based, and stateful protocol analysis). Further, the system has the ability to prevent intrusions, but is currently only able to proactively mitigate threats across a limited subset of network traffic (i.e., Domain Name System traffic and e-mail).
- DHS has identified a set of NCPS capabilities that are planned to be implemented in fiscal year 2016, but it does not appear to have developed formalized requirements for capabilities planned through fiscal year 2018.
- The NCPS intrusion detection capability appears to have been implemented at 23 CFO Act agencies.[17] The intrusion prevention capability appears to have limited deployment, at portions of only 5 of these agencies. Deployment may have been hampered by various implementation and policy challenges.

In conclusion, the danger posed by the wide array of cyber threats facing the Nation is heightened by weaknesses in the Federal Government's approach to pro-

[16] GAO, *Information Security: Concerted Effort Needed to Consolidate and Secure Internet Connections at Federal Agencies,* GAO–10–237 (Washington, DC: Mar. 12, 2010).

[17] The Department of Defense is not required to implement EINSTEIN.

tecting its systems and information. While recent Government-wide initiatives hold promise for bolstering the Federal cybersecurity posture, it is important to note that no single technology or set of practices is sufficient to protect against all these threats. A "defense-in-depth" strategy is required that includes well-trained personnel, effective and consistently-applied processes, and appropriately implemented technologies. While agencies have elements of such a strategy in place, more needs to be done to fully implement it and to address existing weaknesses. In particular, implementing GAO and inspector general recommendations will strengthen agencies' ability to protect their systems and information, reducing the risk of a potentially devastating cyber attack.

Chairman Ratcliffe, Ranking Member Richmond, and Members of the subcommittee, this concludes my statement. I would be happy to answer any questions you may have.

Mr. RATCLIFFE. Thank you, Mr. Wilshusen.

I now recognize myself for 5 minutes for questions. As I mentioned in my opening statement, the OPM servers that were breached contained National security clearance information and other highly sensitive personal information.

When asked why that information was not encrypted, OPM administrators have testified that the servers in question were obsolete and would have crashed had that been attempted.

Dr. Ozment, if that is the case, it begs the question: Why on earth would OPM be storing such sensitive information on obsolete systems that cannot be encrypted?

Mr. OZMENT. Mr. Chairman, I will defer to OPM to speak to the specifics of their decision making, but I can talk to you about some of the tradeoffs that CIOs, in general, face with legacy systems.

As I mentioned in my opening remarks, looking across the public and private sector, broadly I would say that, for the last 20 years, both Government and industry have underinvested in cybersecurity. So, frankly, there is a backlog of cybersecurity work that needs to be done. That requires significant investment.

If an organization also has legacy systems that require investment to upgrade to more modern systems, the bill and resources required to do that can be extraordinary.

So all CIOs are faced with extreme demands for a capability that they have to balance with the need to manage risks appropriately and, of course, in a world of limited resources.

Speaking specifically to encryption, I would note that, in the case of this particular intrusion at OPM, the adversary compromised what is known as an administrative credential.

Think about this as a computer network being an apartment building where each user has a key to their own apartment, but there's a superintendent who has keys to all the apartments in the building. The adversary compromised, essentially copied, the superintendent's key ring and, therefore, had legitimate access to the information on the network.

Mr. RATCLIFFE. Let me ask you about that, Dr. Ozment, because I have two questions that relate to that.

I read a summary of your testimony last week, and it appeared that it was your opinion that, even had this sensitive information been encrypted, it wouldn't have made a difference in the breach for that reason that you just mentioned.

But isn't it true that, had there been multi-factor authentication in addition to encryption, that this breach could have been prevented?

Mr. OZMENT. As both Mr. Wilshusen and I mentioned in our opening remarks, you need defense-in-depth. You need multiple layers of security. Both encryption and multi-factor authentication are important layers of security.

You cannot confidently say that you can prevent any given intrusion, but the more layers of security you have, the more difficult you make it for an adversary.

I do believe that multi-factor authentication is an important security technique, and that is one reason why OMB, for example, is highlighting that in their 30-day sprint.

Mr. RATCLIFFE. Right. But I am asking for your opinion.

Do you think, had there been multi-factor authentication at OPM, that this particular breach could have been prevented?

Mr. OZMENT. I don't know that I can say the breach could have been prevented. I think some of the damage could have been mitigated. In fact, some of the damage was mitigated when OPM rolled out multi-factor authentication in January 2015.

Mr. RATCLIFFE. Okay. So let me ask you about this authorized credentials that you just mentioned.

So, as I understand that, the user, if you will, on its face was authorized to be there. That being the case, what cybersecurity measures or best practices are intended to specifically identify anomalies in the behavior of purported authorized users?

In other words, some authorized users might be in places or using devices that they typically wouldn't be using. Isn't that right?

Mr. OZMENT. That's right. So you can employ what is generally known as insider threat detection technology.

Mr. RATCLIFFE. Were those employed at OPM?

Mr. OZMENT. I do not know for sure whether those were employed at OPM or not.

Mr. RATCLIFFE. Okay.

Mr. OZMENT. But insider threat technology will stop either a legitimate user who is behaving illegitimately or a legitimate user whose accounts have been compromised. It is not perfect, and you often have false positives that you have to investigate. But, again, it is a useful layer of security to add.

Mr. RATCLIFFE. All right. Very quickly, Mr. Wilshusen, the Chairman referenced the enactment of FISMA back in December 2014.

Do you think that the Department of Homeland Security has the necessary authorities right now to be successful in carrying out its mission of protecting Government networks?

Mr. WILSHUSEN. I think the provisions provided in the modernized FISMA of 2014 greatly strengthened DHS' authorities to perform those functions, which previously they had certain responsibilities under a memorandum delegated to it by the Office of Management and Budget. But given the statutory authorities to DHS, certainly strengthens its hand in performing those functions.

Mr. RATCLIFFE. Terrific. I think Dr. Ozment commented on the information-sharing bill that passed the House that the Chairman referenced earlier. I would like your opinion.

Do you agree with Dr. Ozment that that bill could help block future threats?

Mr. WILSHUSEN. I would say that sharing of cyber threat and incident information is a critical element to assuring that agencies in the Department have appropriate threat intelligence to help protect against those threats.

Mr. RATCLIFFE. Thank you. My time is expired for this round at least.

I would like to recognize the Ranking Member for 5 minutes for his questions.

Mr. RICHMOND. Thank you, Mr. Chairman.

Dr. Ozment, Mr. Wilshusen, let me just ask a question. It is something I have always toyed with.

I will start with Dr. Ozment. How much do you all spend yearly on cybersecurity? Do you have an idea?

Mr. OZMENT. My organization within the Department of Homeland Security has an annual budget for fiscal year 2016 of approximately $900 million. Some of that budget goes to emergency communications, essentially ensuring that the phone lines work in the case of a crisis, which, depending on your definition of cybersecurity, could be included or not included.

Mr. WILSHUSEN. Government-wide OPM has reported that, for fiscal year 2014, 24 agencies covered by the Chief Financial Officers Act spent about $13 billion on cybersecurity activities out of an IT budget of around $80 billion.

So the vast majority of that, though, relates to the Department of Defense. Pulling that information—their budgets out, the numbers are significantly less.

Mr. RICHMOND. I guess I was asking those questions because, as we continuously focus on Government spending and spending alone without looking at return on investment, without looking at threats, and we continue to hear the mantra of "We are going to do less with more"—I guess my general question becomes—and I think of it in terms of defending President Bush and the fact that colleagues on my side of the aisle like to say he squandered a surplus and, also, defending President Obama in terms of looking at the National debt.

We have expenses we didn't have before. Before 9/11, you didn't have TSA. Now, with the proliferation of the internet and, as the Chairman just mentioned, the criminals and the nation-states that are attempting to do bad things on the internet, we didn't have those costs before.

So I am just trying to get a sense of—do you think that this is an area where we can do less with more or do you think this is an area where you think we are going to have to continue to invest funds and resources to keep the .gov, .com, .org, all of those domains, safe?

Mr. OZMENT. From my perspective, sir, I think we are going to have to continue to invest for two reasons. One is that we are catching up on many years of underinvestment. The second one is this is risk management. It is not risk elimination.

So the adversaries are not going to go away in cyber space. As we improve our defenses, they will improve their offense. So we will have to continue to invest to maintain pace with an adversary who is also investing.

Mr. WILSHUSEN. I would agree that it will require effective management in addition to resources to accomplish this.

One of the areas that we typically find on our audits of agencies' systems is that many of the vulnerabilities and defects in their security controls can be implemented without necessarily the use or expenditure of additional resources.

It's basically applying patches in a timely manner, assuring that agencies limit the privileges that they grant to their users to the least privilege that's necessary for them to perform their duties, as well as continually testing and evaluating their systems and then taking corrective actions to mitigate known vulnerabilities.

In certain instances, particularly now, agencies will likely need to invest in improving their intrusion detection capabilities to identify and mitigate and reduce the intrusions and impact of intrusions that are likely to occur.

Mr. RICHMOND. My final question would be back to Dr. Ozment. That is: How can your office accelerate the Department's cyber strategy that confronts Federal targets, but still maintain its focus on National critical infrastructure needs against aggressive, persistent, malicious actors that continue to target our Nation's critical infrastructure, for example, for me, our ports? Do you need additional resources to do that? If so, what do you think the ticket price is?

Mr. OZMENT. Thank you.

You will find that our budget requests for cybersecurity in the Department have been growing steadily over the years, and I would not be surprised for them to continue to grow.

You put your finger on an important challenge, which is that we have a responsibility both to the private sector, to the Federal civilian government, and, also, to our State, local, Tribal, and territorial government colleagues.

The good news is, as we improve our Federal cybersecurity, we learn things that will also help us support our private sector and State, local, Tribal, and territorial colleagues. This is where cyber information sharing becomes so important.

When we use the EINSTEIN or CDM programs and detect a threat and learn about a new threat, with the information-sharing legislation, we'll be able to share that information outward.

At the same time, when an adversary attacks a private-sector network and they share that information with the Government, if we're able to receive it, we can then use that information to protect Government networks.

So there's absolutely a synergy between our work in the private sector and our work in the Government. The crux of that synergy is taking information that one entity learns and sharing it with the Government or vice versa.

Mr. RICHMOND. With that, Mr. Chairman, I yield back.

Mr. RATCLIFFE. The gentleman yields back.

The Chairman now recognizes and welcomes to the subcommittee the former district attorney from New York and gentleman from New York, Mr. Donovan, for 5 minutes for his questions.

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

Doctor, I was just wondering if you could help me understand this a little bit. There has been a lot of criticism in the reportings about the breach that EINSTEIN didn't work.

My understanding is that it did what it was built to do and it was part of a multi-layered approach to securing the data and part of this defense-in-depth theory.

Did EINSTEIN actually do what it was created to do?

Mr. OZMENT. Yes, sir, it did. I can go into more detail if you'd like.

Mr. DONOVAN. Please.

Mr. OZMENT. So, in this instance, first, OPM and the Department of Interior are not covered by EINSTEIN 3 yet, which is the system that blocks intrusions. We are working with the Department of Interior to roll that out aggressively. It just became available to them this winter.

It is not yet available to the OPM because we have not yet completed the work with that internet service provider who services OPM.

Now, what happened in this incident is OPM rolled out security capabilities in accordance with a mitigation plan we provided them in May 2014. As they rolled out those capabilities, they caught an intruder on their networks and they shared the cyber threat indicators with us.

We took those cyber threat indicators and put them into the EINSTEIN system. With EINSTEIN 2, we looked back in time and saw that the Department of Interior had also suffered an intrusion, as evidenced by these threat indicators.

We then used EINSTEIN 1 to help us pinpoint what was exfiltrated and from which computers at the Department of Interior. In this case, it turned out to be OPM data that was being stored at a data center at the Department of Interior. That is the 4.2 million personnel records that you read about in the media.

So the trick with EINSTEIN is, as it currently is built, it has to know about a threat before it can detect or block it. This is what it was designed to do. It is a necessary tool. It is not a sufficient tool.

So even as we finish rolling out EINSTEIN across the breadth of the Government, we are also focused on the depth of capability that it offers. One layer of depth that we need to provide is a layer that will help us detect and block intrusions that we have not previously seen.

That gets riskier because you have false positives when you are doing that. That means that we will block legitimate traffic. That could be a problem, but that is a risk we will have to take.

Mr. DONOVAN. Doctor, I am not well-versed in computers. In fact, I still have a VCR that blinks 12.

Just so you could clarify for me, it seems that EINSTEIN was created to block known intruders rather than allowing friendly traffic to come through and block everyone else who is not identified as friendly.

I understand from your analogy about the superintendent that even that wouldn't have worked in this case because the intruder was looked upon as a friendly user.

But is it a better system to just allow friendly users instead of just blocking people who we know because we don't know who all the intruders are?

Mr. OZMENT. Representative, that is an accurate assessment of the situation.

EINSTEIN goes around the entire Federal civilian government. At that distance from an individual agency, it's not possible to identify "This is good traffic only, and we'll only let in the known good traffic."

Because departments and agencies conduct such wildly different business, it's not possible to identify "This is what is appropriate and acceptable and only let this happen." Even within a single department in an agency that is probably not possible.

There may be parts within the department or agency, smaller systems or organizations, that have a limited remit that would be able to say "This is all that we do. And, therefore, we only accept this type of traffic or communications from these computers" or something of that nature.

Mr. DONOVAN. Thank you, Doctor.

Chairman, I yield back my time.

Mr. RATCLIFFE. The gentleman yields back.

The Chair now recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank our witnesses here today.

I want to point out one thing before I go into my questions. We talk about the rollout of EINSTEIN 3 and where we are today. It is unacceptable that we are at this for the better part of a decade now and still such a small percentage of the .gov network has even basic levels of EINSTEIN 3 on it yet.

We have a long way to go. I understand that we are making progress and rolling out EINSTEIN 3 to protect the .gov network, but it is laughable that it has taken this long to get to this point.

Part of the reason, Mr. Chairman, is the fact that no one is in charge despite the fact that we have a cyber coordinator—and I applaud the work that Michael Daniel does with limited tools, really, at his disposal because he lacks policy and budgetary authority to compel compliance of departments and agencies to do more in cyber. Neither does the Secretary of Homeland Security.

I know that in the last Congress we gave additional authorities through FISMA reform, but still even the Secretary of Homeland Security does not have the ability to reach across Government and tell an agency like OPM they are not doing enough on cyber, which is why we are here today and is why the OPM breach happened, because OPM did not take cybersecurity seriously enough.

It wasn't even like they were coming to Congress and asking for more resources. It was only until fiscal year 2016 that they asked for more money for cyber. It wasn't like they were coming here asking for money and they were told no. They didn't even ask. They weren't taking cyber seriously.

So I hope that, at some point, we will get somebody in charge that does have both policy and budgetary authority who can compel compliance of departments and agencies.

But, with that, Dr. Ozment, I noticed that you were at the OGR hearing earlier this morning, and I have a number of questions about the OPM breach.

So, to begin with—and I know the Chairman touched on this briefly on the encryption side—you said that encrypting data stolen may not have helped in this case. Now, you are not suggesting that we shouldn't encrypt, I take it. I want to make sure that you have the opportunity to be clear.

What is your view on encryption? Because I hope you would still agree that encrypting PII is still a best practice that agencies should be following. Is that correct?

Mr. OZMENT. Encryption is absolutely a best practice that agencies should follow, although I would highlight that you always have a limited cybersecurity budget. Let's say its $100. There's always $200 of layers of security you could buy.

So you look at a particular system and look at what's the best value. You select the layers that provide the best value based on the needs of that system.

Mr. LANGEVIN. I would make the point that I think encrypting is vitally important and, if someone were to think that we shouldn't encrypt, it would be like saying, "Well, they came in through the window. So we shouldn't lock the front door and the back door of the house just because they came through the window." We want to make sure that we follow the industry's best practices on the encryption.

Dr. Ozment, did the Federal Network Resilience division work with OPM prior to the discovery of the March 2014 breach?

Mr. OZMENT. So Federal Network Resilience is part of my organization that manages, in part, the annual FISMA reporting.

So prior to the March 2014 breach, we collect data that agencies report on their cybersecurity, and we use that data with OMB to construct the annual FISMA report and, also, to hold cyber stat sessions, sessions where we bring agencies to the White House and essentially go through their cybersecurity posture and work with them to address any challenges.

Mr. LANGEVIN. Did you bring in OPM?

Mr. OZMENT. I will have to come back to you on the date of our last cyber stat with OPM. We have had one, but I don't recall the date of the cyber stat surrounding the March 2014.

Mr. LANGEVIN. I would appreciate it if you would get that to the committee for the record.

It is my understanding that the Federal Network Resilience division did not work with OPM and that OPM never made the request.

The Federal Network Resilience division is precisely the kind of entity that a department or agency whose private mission isn't necessarily going to be cybersecurity could go to the Federal Network Resilience division and ask for the expertise and do a vulnerability assessment and say, "How can we get better?" It is my understanding that OPM never did that.

Dr. Ozment, just to clarify for my sake, does DHS view the OPM breach of personnel data as part of the same incident as the breach of security clearance information? The same threat acted in both

cases? Correct? The same threat acted in both cases. Is that correct?

Mr. OZMENT. I'm going to have to defer to the intelligence community any questions about which actor in specific and even, to a degree, the specifics about the relationships between incidents.

What I will absolutely say is there are clearly relationships between the Government incidents, including the two that we are talking about today, and other recent incidents targeting the PII, the personally identifiable information, of Government employees.

Mr. LANGEVIN. Thank you, Mr. Chair. I know my time is expired. I hope we are going to do a second round. I have a bunch of other questions. I yield back.

Mr. RATCLIFFE. The gentleman yields back.

The Chair now recognizes my colleague from the great State of Texas, Ms. Jackson Lee.

Mr. JACKSON LEE. Mr. Chairman, thank you for your kindness and that of the Ranking Member, first of all, for this very important hearing, and my dear colleague, Mr. Clawson, for yielding not his time, but his place in order, to allow me just a moment.

I have a meeting with the Secretary—and it is starting as we speak—on some matters. But this committee I have always said has been the front-line committee.

Mr. Langevin is correct that we have been talking about the issues of cybersecurity and protecting data and documents for a very long time. You know, I know there is a myriad of issues that we are discussing, but it disturbs me that, in fact—and we heard this generally—OPM used old software that could not be encrypted. We face this enormous debacle that has many fingerprints. We know that there are many elements to it.

I know that I served as the Chairwoman of the Transportation Security and Infrastructure Protection Committee before the Cybersecurity Committee was created, and we talked about the percentage of infrastructure in the cyber world in the private sector—85 percent—and that we had a small percentage thereof.

So I guess for the record I want to express the recognition of our public servants who work very hard, but my absolute consternation and frustration that we are where we are today, task forces that are being discerned and established not necessarily under this administration.

Because, if it was 2015 under another administration—unfortunately, hard heads made a very difficult spot to sit down on. I am baffled why the Government finds itself in this place.

My colleague indicated resources, that that was one of the issues, but focusing one's mind—we talked about getting the brightest and the best to be able to address this question. We predicted it was coming. Not that we were geniuses, but the writing was on the wall. Everyone was turning to technology. Everyone was using technology.

I am enormously saddened for the millions of Federal workers in this recent incident that are now subjected to personal violations. But from the White House to the vast array of Federal departments, agencies, we are not the standard-bearer for the tightest cybersecurity that we can have, having at hand, I think, a bipartisan

commitment that this is a serious issue. Many legislative initiatives have been introduced.

So let me just ask. I indicated to Mr. Clawson I would not be long. I have a number of questions. My staff, Mr. Chairman, is going to frame them in a letter.

Let me indicate that some very thoughtful questions have been put forward, but I do want to heighten this level of frustration. I could listen to the Government Accountability, but let me just ask the two witnesses, being mindful of the time.

You have heard my level of frustration. We are here today. Will we be here next week? Will we be here next month? Will we be here next year? This hacking, breaching, is not going to stop.

So I just want to ask this question: Why is the Government at this place at this time? Why are we here?

Mr. WILSHUSEN. I think there are probably several reasons, one of which is the fact that many of the computer systems that Federal agencies use—and it's not dissimilar to what's happening out in the private sector—is based on defective software.

Much of the software that agencies use have a number of vulnerabilities in it that aren't fixed before they're bought, sold, purchased, and deployed. So, over time, as these vulnerabilities come to light, agencies as well as any users of that software need to take steps to mitigate and correct those vulnerabilities.

Mr. JACKSON LEE. I am not going to cut you off. You gave me a powerful answer. As I said, I am going to follow up with questions coming to you because I want to get to Mr. Wilshusen for that very same question.

So is the answer now "stop, move out all your software, and begin again"? Yes or no.

Mr. WILSHUSEN. No. The answer is no. You can't stop and move out all your software.

Mr. JACKSON LEE. All right. I wanted to hear that.

So it is piecemeal.

Mr. WILSHUSEN. I think what one has to do is, as corrections and patches are identified to correct vulnerabilities in software, that they be applied promptly to the——

Mr. JACKSON LEE. Which we have had some problems with doing that. Thank you, sir.

Mr. JACKSON LEE. Mr. Wilshusen, why are we here where we are today?

Mr. OZMENT. So I would actually echo the points that Mr. Wilshusen made. I would flag that it's, in part, the complexity of software——

Mr. JACKSON LEE. Sorry. Mr. Wilshusen was over here, and you are over here. Sorry.

Mr. OZMENT. No problem.

I would flag that it's the complexity of software, which means that, even as we build it, it's insecure. Even if we could build individual pieces of software securely, we, as a Nation, don't know how to compose those into larger systems that are themselves secure. This is a place where both the Government and the private sector are.

We're in a world right now where we rely upon information technology. We're not able to manage securely the complexity of that

technology, but neither can we back away from that technology. So we are in a world where we will have to manage the risks, but we will not be able to prevent intrusions.

Mr. JACKSON LEE. Well, the first thing is to know that we need to manage the risks in the Federal Government, even though you have the larger—I think you are in the private sector—the larger component.

You are in Homeland Security, but you do realize the private sector has the largest amount. So we need to manage it. That is what you are suggesting that we need to do.

We need to engage with the private sector, and we need to confront the horror that it is and be diligent constantly on our managing, on trying to get our hands around the issue.

With that, Mr. Chairman, I am going to yield back. Forgive me for putting Government people in private hats. But I know that they have probably weaved in and out of the private sector at some point.

But I see that this is going to be a looming issue, and I think this committee is right and the full committee is right for us to be enormously penetrating on solutions of getting the Government where it needs to be and getting the private sector in its cooperative mode to help the Nation be where it needs to be on this issue of cybersecurity.

With that, Mr. Chairman, thank you.

Mr. Clawson, thank you.

I yield back.

Mr. RATCLIFFE. I thank the gentlelady. The gentlelady yields back.

I now would like to recognize my friend and colleague from Florida, Mr. Clawson, for his questions.

Mr. CLAWSON. Thank you for coming today.

I am going to lay out a couple of observations, two or three maybe, and then you all can respond and tell me if you agree with me or where you think I am wrong.

My first observation is, if one of my nieces and nephews came to me and said they were going to take a job at the Federal Government, I would say, "Don't do it. Your information is not secure. It is probably a lot less secure than most places you could go to work."

Therefore, I am not sure how we attract great talent to do the things that we talk about doing in this committee not just for the security, but just to run the Government.

I am not sure that putting employees at this kind of risk will attract "A" players to work in the Government. Just all of my instincts tell me there is going to be residual impact from these kind of breaches that impact how well the Government does across the board. That is my first observation.

My second observation is, if I was sitting there running that enterprise, I would say to myself, "Delete, delete, and more delete." My guess is that there is a lot of legacy data that aren't mission-critical right now, right now, particularly employees that have come and gone, records that are years old.

I know you are going to tell me you can't. But all of my own managerial experience would say to delete the hell out of this so

that, even though that might make our job more difficult in the future, it will make the hacker's job impossible. He can't hack what doesn't exist.

My third observation would be, from a managerial perspective, to decentralize. Even if you roll it up on the internet in summary format later, decentralize. Decentralize everywhere you can.

I understand that everybody wants an ERP on a centralized basis, but do that at a summary level and keep the data decentralized so that the hacker's job is much more complicated and you don't have a mother lode of data that he can get into.

Now, I know you are going to take issue with those things. But if this was my board of directors and you all came in with this problem to me, those would be my first three reactions. If we ignore those outcomes and those possible solutions, it seems to me that we are living in yesterday's world.

Now, I know you are going to tell me why what I say is impracticable, but I still want to hear from you.

Mr. WILSHUSEN. I guess I'll take first crack versus your first observation on whether or not an individual should be hired or try to seek work with the Federal Government versus private sector.

First, I would just say that the scourge of cyber malfeasance is not unique to the Federal Government. The same security vulnerabilities, the same types of attacks, the same types of data leakage and theft, occurs in private sector as well as the Federal Government. I think many Federal employees look beyond just that element to work for the Federal Government. It's more, perhaps, out of a civic duty and responsibility.

Mr. CLAWSON. But you would agree—excuse me for interrupting to reclaim my time—you would agree that a Chinese hacker would probably rather get into the central government than a shock absorber maker or a wheel maker or a basic industry parts maker.

Mr. WILSHUSEN. It depends on their motives.

Mr. CLAWSON. When you make that equivalency, I am just having a hard time with that. You know, having protected my own network, I kind of have to call you on that. That doesn't feel like the same level of being a target.

Mr. WILSHUSEN. It depends on what the motives of the hacker are, whether it's economic, monetary gain, or seeking a political or military advantage.

If I'm a competitor and I'm seeking to gain information about a private company and what their products might be, I might be interested in hacking a private company's system. I might very well be in tune to trying to hack into Federal Government because——

Mr. CLAWSON. Right. I have never had a personnel system hacked. I have had my product designs hacked. I have had my process technology hacked. I never had my personnel records hacked. It doesn't help my competitor.

Mr. WILSHUSEN. As you mention, it's not just personnel records. It's other proprietary information, intellectual property, that might be the target of a hacker.

Regarding the deleting data, of course, in the Federal Government, we do have records management requirements where we have to retain and archive certain data for a period of time.

But I agree. After those time limits have expired, sure, get rid of it. To the extent we're able to, deleting information that's no longer necessary in accordance with Federal requirements should be done on a regular basis.

Mr. CLAWSON. Well, if Congress can help with that at all, I would really like to be involved. In our company, we kept things a year unless we absolutely—you can't hack what was there 3 years ago because it is gone. That would eliminate a lot of risk, I think.

I am sorry I am going on here, Doctor. You can also take issue with me.

Mr. OZMENT. I agree with Mr. Wilshusen. So I won't belabor the first two points.

I'll add to the final point that there is a constant tension between centralization and decentralization in IT and, also, between homogeneity and heterogeneity in the sense of do you have a few systems of the same type or systems of very different types.

It really depends on what you're trying to accomplish in the broader environment. So I don't think there's a right answer there. I think we should absolutely, however, consider that question when we design our networks.

Mr. CLAWSON. My final follow-up. I spent a lot of years trying to centralize, as you say, to get the same kind of data all across the world.

I found out just by rolling it up on the internet and leaving it decentralized it was just a lot cheaper. I didn't have all this management problem. It ended up being safer because I didn't have a lot of hackers in the Czech Republic.

I yield back. Thank you.

Mr. RATCLIFFE. The gentleman yields back.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Perry, for his questions.

Mr. PERRY. Thank you, Mr. Chairman.

I know it is a little unexpected. Sorry to be late to the game here.

I am thinking about like the data services hub and the law that we have in place now in particular where you are required by law to be involved in the Government and then, by transposition, your data is then within the Government purview and then we don't necessarily have the best systems, maybe, that we could or should and how we also, as a Government, treat private entities that have been hacked and we penalize them for having not done enough soon enough or notified appropriately or what have you.

I don't know how we have the moral high ground, as the Federal Government in this, you know, and we are not necessarily talking about the particular OPM breach, but because these things happen on a—at least the hacks happen on a regular basis. Right? We know that there are those who have been hacked and those who don't know it yet. Right? That is kind of how things go.

So DHS, I think, has done everything within their current power. Right? They have advised. They have urged other agencies, "This is the gold standard. This is where you need to be." But they still have no authority to force the agencies, like OPM or anybody else.

They can tell them where they think they should be based on what DHS knows. "This is why we have the Department of Home-

land Security, among other reasons, is to determine threats that we have and solutions sets" and so on and so forth. So they can advise, but they have no authority.

So, in a broad sense, my question to you would be: Should DHS have the authority regarding other agencies to impose—we are talking about individual citizen's data which, in this particular instance, not necessarily OPM, but the data services hub associated with the ACA.

You are mandated by Federal law to have your data, everything about you, be in that repository. If that is the case, should it be DHS? Should they have the authority? If not, who? If not anybody, then what is the solution set to make sure that agencies are on the cutting edge of safeguarding America's data?

Mr. WILSHUSEN. Well, with regard to the first question, in terms of does DHS have the authority to compel agencies to take certain actions, the Federal Information Security Modernization Act of 2014 gave DHS statutory authorities to perform additional activities to help assist Federal agencies in improving their information security.

One of those tools that's available to the Department is what is known as a binding operational directive. This is guidance and actually direction to the agency that the agency is required to implement. These directives are, I believe, prepared and developed in collaboration with OMB and others. But they do have a tool at least in their tool kit to help direct agencies to take corrective actions.

Mr. PERRY. They can help, they can assist, but they can't compel, or they can compel?

Mr. WILSHUSEN. I believe those directives may be compulsory. But I will defer to Dr. Ozment.

Mr. LANGEVIN. Will the gentleman yield?

So what is the consequence if they fail to comply?

Mr. OZMENT. I think, Mr. Langevin, Mr. Perry represents—you get to the crux of the matter, which is we have the formal authority to compel. We do not have a stick to enforce that compulsory order.

That being said, I don't know that it's possible for one department to be given that sort of compulsory ability with some sort of budgetary authority over another department, the way our overarching system is structured. So in the sense of our ability to issue compulsory orders, I think we do have that existing authority.

I would highlight the two areas where we absolutely are lacking in necessary authorities right now are authorizing legislation for the EINSTEIN program, which this committee sponsored and passed and the House has passed, and, also, the information-sharing legislation, again, which this committee sponsored and the House has passed.

Mr. PERRY. So you think that we have at least some form, in the remaining time, of oversight to where we can urge and maybe even compel, but there is no—you can compel all you want, but if there is no consequence to inaction, there is nothing to compel you.

Your assertion would be, as usual, not that—this isn't meant to be personal. How can the Government penalize itself? Because you

are taking from one pocket—out of one pocket and putting it another pocket, if it is financial or what have you.

But I think that smart folks like you and people on this committee need to find a way to compel, if that is the right solution set—you know, our individual citizen's data is at risk here and, if we have that authority, we have a responsibility to safeguard it. They are mandated to provide that information, mandated to, and then it is at risk. That is unacceptable, and I am sure you know it.

Thank you, Mr. Chairman. I yield back.

Mr. RATCLIFFE. The gentleman yields back.

Like Congressman Langevin, I was hoping that we might get to a second round of questions. But based on the updated vote schedule and out of respect to our witness on the second panel, we will move now to that second panel.

So I thank the witnesses for their testimony and the Members for their questions at this first part of our hearing today.

As was indicated, some of the Members have additional questions for the witnesses. We will ask you to respond to those in writing. The committee will now take a very short break so that the clerks can prepare the second panel.

[Recess.]

Mr. RATCLIFFE. I would like to welcome our second distinguished panel today, Dr. Daniel Gerstein, with The RAND Corporation and former acting under secretary for the Science and Technology Directorate at the Department of Homeland Security.

Welcome, Dr. Gerstein. At this time I will ask you to stand and raise your right hand so that I can swear you in to testify.

[Witness sworn.]

Mr. RATCLIFFE. You may be seated.

Dr. Gerstein's full statement will appear in the record.

The Chair recognizes you now for 5 minutes for an opening statement.

STATEMENT OF DANIEL M. GERSTEIN, THE RAND CORPORATION

Mr. GERSTEIN. Well, thank you. Good afternoon.

Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee, I thank you for the opportunity to testify today on the strategies for defending U.S. Government networks in cyberspace.

Recent events occurring on U.S. Government networks over the past several years, punctuated most recently by the OPM breach, demonstrate clearly the need for developing and maintaining capabilities to assess the status of the Government's internal networks and protect them from intrusion.

These events have also underscored concerns about the growing sophistication of the threat and the risk posed to personal data, Government networks, and even mission assurance.

Two foundational elements of the Department of Homeland Security's cybersecurity program are EINSTEIN, also called EINSTEIN 3A, and Continuous Diagnostics and Mitigation, or CDM. The two systems are designed to work in tandem, with EINSTEIN focusing on keeping threats out of Federal networks and CDM identifying

them when the threats are inside the Government networks. The phased rollouts of both CDM and EINSTEIN are expected to continue over the next several years.

Now, despite recent progress, critics have argued that both programs have taken too long to implement, and I have to say there is some validity to these concerns. However, CDM is now at a point in development and deployment where additional resources could accelerate the program. EINSTEIN, on the other hand, still requires additional development and coordination with internet service providers, which will be contracted to implement the program.

In my judgment, both programs are necessary, but not sufficient for ensuring the security of Government networks. Therefore, even with EINSTEIN and CDM, more will be needed to defend Government networks in cyber space.

For the remainder of my remarks, I would like to provide a more strategic look at this issue. Now, the internet is a complex system of systems, requiring a comprehensive approach to ensuring security across the vast Government network. Any single approach or program will be insufficient to ensure security in cyber space. As such, defense-in-depth strategies will be essential for securing Government networks.

Now, when considering the development of a comprehensive cybersecurity approach, one must examine how new policies and processes, improvements to the internet architecture, hardware and software hardening, and personnel training and education must be combined into a system that will provide security, privacy, and resiliency.

Inherent in efforts to secure the Federal cyberspace is the critical need for a National cybersecurity strategy. Such a document would include articulation of concepts for governance of the .gov domain in addition to cyber doctrine for deterrence, denial, attribution, response, and resilience. Today no such doctrine exists.

It is my belief that the U.S. Government is at a crossroads concerning cybersecurity. The goal to date has been to balance two competing demands: Availability of data and security of the enterprise.

As recent breaches have demonstrated over the past several years and with the OPM breach as an exclamation point, it is time to consider developing secure enclaves to protect key Government information, data, and networks.

The technology exists today to re-architect the Government internet systems, and several agencies within the National security community have implemented such re-engineering with good results.

Implementing these approaches to modernize and improve the security architectures will require resources and focused attention, both of which Congress and the Executive branch can provide.

Appropriate funding for research, development, and acquisition programs remains another foundational element in the critical race to secure Federal Government networks. Government must partner with the cyber industries to ensure the pipeline of critical solutions continues to be developed.

Finally, workforce issues both for cyber professionals that manage the Government networks and for the broader Government

workforce that utilizes the network must be considered as a top priority.

In the Government's cyber space, the security of the overall network is directly linked to the security of each of the nodes, to include the individuals operating each terminal device.

I appreciate the opportunity to discuss recommendations to improve cybersecurity in our Government networks and, thereby, the homeland security of our Nation, and I look forward to your questions. Thank you.

[The prepared statement of Mr. Gerstein follows:]

PREPARED STATEMENT OF DANIEL M. GERSTEIN [1]

STRATEGIES FOR DEFENDING U.S. GOVERNMENT NETWORKS IN CYBERSPACE [2]

JUNE 24, 2015

INTRODUCTION

Good morning Chairman Ratcliffe, Ranking Member Richmond, and distinguished Members of the subcommittee. I thank you for the opportunity to testify today on the Department of Homeland Security's (DHS's) Federal cybersecurity efforts. Specifically, I will discuss overarching cyber concerns, the Continuous Diagnostics and Mitigation (CDM) program, and other strategies for defending networks in cyber space.

The CDM program is an important foundation for the security of Government networks. The concept was designed to provide a set of tools for enabling network administrators to know the state of their respective networks, inform on current threats, and allow system personnel to identify and mitigate issues at network speed. However, it is worth noting that CDM is not intended to be a stand-alone system, but rather one part of an overarching system-of-systems approach.

EINSTEIN, which provides perimeter security for U.S. Government networks, is a complementary system to CDM. EINSTEIN functions by installing sensors at web access points and employs signatures to identify cyber attacks. Of note, both CDM and EINSTEIN are in early stages of deployment.

Recent breaches occurring on U.S. Government networks over the past several years demonstrate clearly the need for developing and maintaining capabilities to assess the status of the Government's internal networks and protect them from intrusion. These events have also underscored concerns about the growing sophistication of the threat and the risk to personal data, Government networks, and even mission assurance.

OVERARCHING CYBER ISSUES AND THE CONTINUOUS DIAGNOSTICS AND MITIGATION (CDM) AND EINSTEIN PROGRAMS

Several key points undergird my comments about the CDM and EINSTEIN programs. These points concern the nature of the cyber threat, the demonstrated ability to sense and respond to threats, the importance of the programs, and, finally, the need to employ CDM in concert with others' cybersecurity strategies.

The cyber threat continues to grow and evolve

The range, pace, persistence, and intensity of cyber threats to U.S. Government networks continues to grow. Even before this most recent breach of Government data from the Office of Personnel Management (OPM), ample evidence was available to indicate that our networks have been and likely continue to be penetrated. The goals of these attacks vary and include mapping Government networks, build-

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to Federal, State, or local legislative committees; Government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a non-profit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] This testimony is available for free download at *http://www.rand.org/pubs/testimonies/CT436.html.*

ing databases on personnel, and intellectual property theft. The perpetrators include both state actors—in particular, China and Russia—and non-state actors.

The cyber adversary is determined and technically competent and has demonstrated significant agility in attacking Government networks. Additionally, the cyber adversary has a low cost of entry, allowing for large numbers of potential threat actors. Coupling the growing number of hackers with the potential for high payoffs for successful attacks provides indications that the current pace of attacks is unlikely to change unless the perceived cost-benefit dynamics are also changed.

Concerning the recent OPM database hack, the private data of over 4 million people were compromised, with up to 18 million personnel whose records were exposed to the hackers. Speculation is that the goal behind the attack is to build a database of Federal employees, perhaps even to use the stolen personal information to impersonate Government workers or for future "insider" attacks. Experts speculate that the goal behind the attack could be to reveal who has security clearances and at what level, so that the Chinese may be able to identify, expose, and even blackmail U.S. Government officials around the world.[3]

Several years ago, U.S. Cyber Command (CYBERCOM) estimated that there were 250,000 probes or attacks every hour, or over 6 million per day, against U.S. Government networks.[4] Today, an estimated 3 billion people use the internet, and another 4.9 billion devices are connected—a phenomenon known as the Internet of Things (IoT). Estimates are that by 2020, the number of IoT connections will be in excess of 25 billion devices.[5] This expansion implies that more Government internet users, data, and systems will be placed at risk from a rapidly expanding internet footprint.

The loss of Government intellectual property (IP) is another significant cause for concern. Russia and China have active programs to penetrate U.S. Government networks for the purpose of gaining IP. China uses these intrusions to fill gaps in its own research programs, map future targets, gather intelligence on U.S. strategies and plans, enable future military operations, shorten research and development (R&D) time lines for military technologies, and identify vulnerabilities in U.S. systems and develop countermeasures.[6] Estimates are that the loss of IP has exceeded well over $1 trillion including the loss of plans and technical details for the F–22 and F–35 aircraft.[7]

Major concerns about our ability to sense threats in real time and respond rapidly

The OPM data breach provides ample evidence that the Government's ability to sense threats in real time has not been adequate. Reports indicate that the OPM breach first occurred in December 2014, but was not discovered until April 2015 or publically acknowledged until June 4, 2015.

Also noteworthy when considering the OPM breach is that the intrusion was detected in April only after OPM's cybersecurity detection and monitoring tools had been upgraded. Therefore, any Government organization that has not already upgraded its detection and monitoring tools is likely to be unaware of any similar intrusions that are on-going or that previously occurred.

Given the large number of attacks on Government networks that CYBERCOM estimates occur on a daily basis, one can conclude that there is a high likelihood of additional successful malicious attacks that have been conducted or are on-going and that have not been detected.

Continuous Diagnostic Monitoring (CDM) and EINSTEIN as key components of our defensive cyber capacity for .gov users

The two foundational programs of DHS's cybersecurity program are EINSTEIN (also called EINSTEIN 3A) and CDM. These two systems are designed to work in tandem, with EINSTEIN focusing on keeping threats out of Federal networks and CDM identifying them when they are inside Government networks.

---

[3] See Andy Medici, "Massive OPM Data Breach Went Undetected for Months," *Federal Times,* June 5, 2015, and OPM, "Information About Recent Cybersecurity Incidents," web page, updated June 18, 2015 (*http://www.opm.gov/news/latest-news/announcements/*).

[4] Jim Garamone, "Cybercom Chief Details Cyberspace Defense," *DoD News,* September 23, 2010.

[5] Gartner, "Gartner Says 4.9 Billion Connected 'Things' Will Be in Use in 2015," press release, Barcelona, Spain, November 11, 2014 *(http://www.gartner.com/newsroom/id/2905717).*

[6] Larry M. Wortzel, *Cyber Espionage and the Theft of U.S. Intellectual Property and Technology, Testimony Before the House of Representatives Committee on Energy and Commerce, Subcommittee on Oversight and Investigations,* Washington, DC, July 9, 2013.

[7] Ellen Nakashima and Andrea Peterson, "Report: Cybercrime and Espionage Costs $445 Billion Annually," *Washington Post,* June 9, 2014.

EINSTEIN provides a perimeter around Federal (or .gov) users, as well as select users in the .com space that have responsibility for critical infrastructure. EINSTEIN functions by installing sensors at web access points and employs signatures to identify cyber attacks.

CDM, on the other hand, is designed to provide an embedded system of sensors on internal Government networks. These sensors provide real-time capacity to sense anomalous behavior and provide reports to administrators through a scalable dashboard. It is composed of commercial-off-the-shelf equipment coupled with a customized dashboard that can be scaled for administrators at each level.

CDM operates by providing:

"Federal departments and agencies with capabilities and tools that identify cybersecurity risks on an on-going basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources."[8]

CDM will be fully implemented in three phases, allowing for 15 diagnostic capabilities. The first phase focuses on endpoint integrity, which is the functionality that examines all endpoints attempting to attach to the network and prohibits unsafe or noncompliant endpoints from gaining access. Specifically, endpoint integrity includes management of hardware and software assets, configuration management, and vulnerability management, which are foundational capabilities to protect systems and data. Phases 2 and 3 are continuing to be further defined to include Least Privilege and Infrastructure Integrity, and Boundary Protection and Event Management, respectively.[9] In the end-state, CDM is expected to cover over 60 Federal agencies.

DHS, partnering with the General Services Administration (GSA), established a Blanket Purchase Agreement (BPA) for CDM that allows Government departments and agencies at the Federal, State, local, Tribal, and territorial levels to contract for continuous diagnostic monitoring. The BPA has a total ceiling of $6 billion.

The phased roll-outs of both CDM and EINSTEIN are expected to continue over the next several years. Despite recent progress, critics have argued that both programs have taken too long to implement, and there is some validity to the concerns. However, CDM is now at a point in development and deployment where additional resources could accelerate the program. EINSTEIN, on the other hand, still requires additional early-stage development and coordination with the internet service providers that would be contracted to support the program.

Lack of defensive capacity is placing the Nation at risk and we should expect additional intrusions and hacking to occur

The skill of the adversaries, low cost of entry, relative ease of conducting attacks and the potential for high payoffs suggests that cyber attacks against Government networks are likely to remain a significant threat.

Programs such as EINSTEIN and CDM are necessary but not sufficient to change the cost-benefit calculus or provide sufficient defensive capacity to keep cyber attacks from penetrating U.S. Government networks.

Recent legislative actions are also necessary but not sufficient to ensure protection of Government networks. These include: (1) The National Cybersecurity Protection Act of 2014, which provides explicit authority for DHS to provide assistance to the private sector in identifying vulnerabilities and restoring their networks following an attack, and establishes in law the National Cybersecurity and Communications Integration Center (NCCIC) as a Federal civilian interface with the private sector; and (2) the Federal Information Security Modernization Act of 2014, which provides DHS authority to administer the implementation of Federal information security policies, develop and oversee implementation of binding cybersecurity directives, provide technical assistance to other agencies through the U.S. Computer Emergency Response Team (US–CERT), and deploy cybersecurity technology to other agencies upon their request.

A third piece of legislation that is still being debated is the Cybersecurity Information Sharing Act of 2015. This legislation would require the sharing of information between the Government and industry concerning threats and other cyber information. While the specifics are still being developed, the general concept of great-

---

[8] U.S. Department of Homeland Security, "Continuous Diagnostics and Mitigation (CDM)," web page, updated June 16, 2015 *(http://www.dhs.gov/cdm).*

[9] U.S. Department of Homeland Security, "Implementation of Continuous Diagnostics and Mitigation (CDM)," web page, updated June 16, 2015 *(http://www.dhs.gov/cdm-implementation).*

er sharing of information on cyber incidents between industry and the Government would be welcomed. However, even with such new legislation, recent cybersecurity trends are unlikely to be reversed without a more comprehensive program.

Even with EINSTEIN and CDM, more will be needed to defend Government networks in cyber space—developing doctrine for deterrence, denial, attribution, and response will be imperative. It may also be time to reevaluate the U.S. Government information architecture.

The internet is a complex system-of-systems requiring a comprehensive approach to ensuring security across the vast Government network. Any single approach or program will be insufficient to ensure security in cyber space. As such, a defense-in-depth strategy will be essential for securing Government networks.

In considering the development of a comprehensive cybersecurity approach, one must examine how new policies and processes, improvements to the internet architecture, hardware and software hardening, and personnel training and education must be combined into a system that will provide security, privacy, and resiliency.

Inherent in efforts to secure the Federal cyber space is the development of a National Cybersecurity Strategy. Such a document would include articulation of concepts for governance of the .gov domain, in addition to cyber doctrine for deterrence, denial, attribution, response, and resilience.

In my judgment, the U.S. Government is at a crossroads concerning cybersecurity. The goal to date has been to balance two competing demands: Availability of data and security of the enterprise. As recent breaches have demonstrated over the past several years—with the OPM breach as an exclamation point—it is time to develop secure enclaves to protect key Government information, data, and networks.

The technology exists today to re-architect Government internet systems, and several agencies within the National security community have implemented such a re-engineering with good results.

Implementing these existing approaches to modernize and improve security architectures will take resources and focused attention—both of which Congress and the Executive branch can provide. We must start thinking of security as one of the top imperatives and systematically evaluate and change the U.S. Government's information architectures, along with applying programs such as CDM and EINSTEIN, if we are going to be better able to prevent, detect, and respond to these sorts of attacks.

Appropriate funding for research, development, and acquisition programs remains another foundational element in this critical race to secure Federal Government networks. Government must partner with the cyber industries to ensure that the pipeline of critical solutions continues to be developed. At the same time, critical infrastructure industries such as transportation and energy must be beneficiaries of this cyber research, development, and acquisition.

Workforce issues, both for the cyber professionals that manage the Government networks and for the broader Government workforce that utilizes the network, must be considered as a top priority.

In the Government cyber space, the security of the overall network is directly linked to the security of each node, including the individuals operating the terminal devices. Training and education must be fully embedded throughout the workforce.

CONCLUSIONS

Recent cyber attacks demonstrate a disconcerting trajectory. Attackers are evolving their strategies and are becoming more emboldened. With little by way of deterrence, hackers—including state and non-state actors—are continuing to find opportunities to penetrate U.S. Government networks.

These networks have demonstrated significant weaknesses that have been exploited resulting in loss of a large amount personal identifiable information, intellectual property, acquisition information, and sensitive security information.

CDM and Einstein must be considered as one part of a layered defense strategy, but they cannot be the only tools employed. No one technology or solution can be utilized in isolation. Employing a systems approach to cybersecurity will be essential.

Thank you, and I look forward to your questions.

Mr. RATCLIFFE. Thank you, Dr. Gerstein.

I now recognize myself for 5 minutes for questions.

So, Dr. Gerstein, you were in the room today and had a chance to listen to the testimony of our first panel. So I want to start there.

Obviously, we spent some time in this hearing and much of last week talking about the OPM breach. As a former DHS officer now on the outside looking in, I would like to get your perspective on that and specifically whether or not you have an opinion to the question that I was asking earlier about whether or not there is any legitimate excuse for why encryption and multi-factor identification shouldn't have been deployed at OPM.

Mr. GERSTEIN. Thank you, Mr. Chairman.

I absolutely believe that, in fact, OPM had been slow to make necessary enhancements to its cyber network. The list of deficiencies that they are trying remediate and have been trying to remediate over the past, say, 9 months or so has been quite long.

It begins with not even having a common understanding of what systems were part of their network. So they had not had a mapped network to be able to understand what was on their entire OPM network. So that is problematic.

The multi-factor authentication is absolutely key. They were not in charge of their configuration because they had not had necessarily a professional IT force until 2013, when they actually did get an IT staff. So you have those sorts of systemic problems that are now being addressed.

I clearly think that Dr. Ozment's comment about we are fighting a catch-up battle is right to the point, that we have underinvested in cybersecurity strategies.

At the same time, interestingly, we have, in a sense, overinvested in information-sharing strategies. That is, we have put a premium on how to share information, but not necessarily how to secure the information.

Mr. RATCLIFFE. Well, you mentioned underinvesting. But Federal agencies face similar problems with budgets and resources all the time.

I guess I would like to know if you have any recommendations for Federal CISOs with respect to devoting those resources to combat this particular threat.

Mr. GERSTEIN. Well, Mr. Chairman, it's really above the CISO. It's about strategic decisions to protect the network. What we lack in this entire architecture is a governance structure and a National cybersecurity strategy.

I go back to several months ago now. The Department of Defense put out its own defense cybersecurity strategy. Normally, when there is such a strategy, you would expect that there would have been a National strategy that would have helped to inform.

Such is always the case, for example, with the National security strategy of the United States coming out, and then the National military strategy falls shortly thereafter. One would expect and one would hope there would be such a thing as a National cybersecurity strategy.

This strategy, as I mentioned in my opening remarks, should really think about, what is the doctrine for deterrence, how do we tell potential adversaries what the consequences are for actions in cyber space, how do we find the proper balance between the security of the network and the privacy of individuals? These are tradeoff questions that have to be addressed in such a strategy.

Mr. RATCLIFFE. So, Dr. Gerstein, you heard Dr. Ozment's testimony. I asked him specifically about—and he was able to confirm—the published reports out there that this breach was accomplished by using authorized credentials.

So, in effect, the user here with respect to the network appeared to be an authorized user. We seem to be increasingly seeing that as a cyber intrusion method in other places besides the OPM attack.

So I guess I would like to hear your perspective on what cybersecurity measures and best practices can be employed to identify those anomalies where you have authorized users in places where they shouldn't be.

Mr. GERSTEIN. So there are a number of different strategies that one can consider. Certainly you brought out multi-factor authentication. That is key. PIV cards. Incorporating those into your architecture is also key. I think we need to look hard now at, do we develop enclaves? Let me just talk for a moment about that.

Today we have a system, an internet, which has evolved over the past 40 years in which you have normal information sharing. I use the tongue-in-cheek grandma's recipes residing on the same system that you have industrial control systems for hydroelectric plants and even nuclear facilities.

The question has to be: Is it now time to segment the internet such that you do develop secure enclaves that have a greater degree of security? This is something that should be considered as part of this National cyber strategy that I've alluded to.

Mr. RATCLIFFE. Thank you, Dr. Gerstein. My time has expired.

The Chair now recognizes the Ranking Member, Mr. Richmond. The gentlemen yields.

The Chair recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman.

I want to thank the Ranking Member for yielding.

Dr. Gerstein, thank you for your testimony. It has been very insightful.

I want to begin by saying I completely agree with you on the National cyber strategy. In fact, the legislation that I have introduced in now a few Congresses, including this one, the Executive Cyberspace Coordination Act, would basically put somebody in charge, giving them both policy and budgetary authority. That act would also require a National strategy to be completed within 1 year. So you and I are of like mind on that subject.

So, Dr. Gerstein, in your written testimony, you say that balancing data access and security has been a driving factor in cybersecurity strategies. I understand that this is often a fundamental trade-off and that we must support research and development to allow us to better achieve both goals.

But I wonder if a bigger problem in many agencies like, say, OPM is that the security risk assessments are not even being conducted adequately. In other words, there is not so much a conscious decision to prize usability at the expense of security, but a lack of understanding that security is being comprised. Is that a fair analysis?

Mr. GERSTEIN. Yes, sir. I think there is some of that. But I do believe that some of the recent legislation—I think the implementation of EINSTEIN and CDM across the .gov space will be important.

We have to continue, though, to stress to all elements of the network, which includes the personnel and their terminal devices, how important they are as a first line of defense.

Many of the intrusions that occur are due to people not understanding issues such as phishing attacks, spear-phishing attacks, and, therefore, opening up their networks through inadvertently opening up a piece of software that contains, say, malware.

Mr. LANGEVIN. Thank you.

So, Dr. Gerstein, I sincerely believe that we are going to keep seeing breaches of sensitive Government networks, unfortunately, until we start holding attackers accountable.

This is not to absolve OPM for the weak cybersecurity posture. Far from it. But I do believe that the administration and Congress have to take stronger actions in response to cyber attacks.

Do you believe that we have sufficiently explored options for deterrence? What avenues would we be exploring?

Mr. GERSTEIN. Absolutely not, sir. I think we have much more to do in cyber deterrence. Today we're having discussions about what constitutes an attack and what level of intrusion is going to be acceptable on networks. I take you back to the Cold War when there was spying going on between adversaries within the Warsaw Pact and NATO.

So we have not yet said what is going to be our response to such intrusions. Are we going to just consider them to be the course of doing business or are we going to react?

I would presume that, if we did talk about deterrence in a realistic and measured way, that we would come up with limits on what we are prepared to accept before taking actions. These actions need to be thought of across the full range, from economic- and political-type activities and, if necessary, even considering use-of-force activities. But we have not had those discussions across the U.S. Government.

Mr. LANGEVIN. Could you speculate on some of what those actions would be beyond the broad categories that you talked about?

Mr. GERSTEIN. Well, of course, there are a number of opportunities to use organizations such as United Nations and things at the lower end, such as démarche. You can have economic sanctions. You can do something that is very asymmetric. So you could have a blockade, for example.

But I'm not suggesting any one set of actions, rather, that we need to, as a Government, consider what actions would be reasonable, given the activities that are on-going.

Mr. LANGEVIN. Well, I clearly agree that we should have some more international rules of the road. This isn't just a U.S. problem, but an international one. Right now it is kind of the Wild West out there.

On the experience of the cyber attacks that we have experienced here in the United States—and OPM is a perfect example—our adversaries or these hackers are eating our lunch, and we are not seeming to be able to stop it and not doing much about it.

That should change. We have to change the calculus so that our enemies or adversaries know that there is a cost to hacking our systems and stealing our data.

So, with that, Mr. Chairman, I will yield back.

I thank Dr. Gerstein for his testimony.

Mr. RATCLIFFE. The gentleman yields back.

The Chair now recognizes the gentleman from Pennsylvania, Mr. Perry.

Mr. PERRY. Thank you, Mr. Chairman.

Hey, Dr. Gerstein. Good to see you again.

So you were sitting here during the last panel and the questioning that I had. I just would like to get your perception, if you recall.

Is DHS the correct place? Do they have the authority? What are the consequences? Your perception there. Also, just thinking through some of your comments, National security strategy, National military strategy, National cybersecurity strategy, your thoughts on where—where would be the repository of that strategy? Who would develop it? Maybe some tenets of the strategy.

Also, what is topical today just came to me while we are having this discussion. So maybe it has already been brought up. But the naming convention, circumstances that we find ourselves in now, is that something that should be included in this strategy? Should the United States allow that to leave the purview of our country and be more international with some other international body? How does that tie in? Then we can probably just have an on-going discussion based on your answers.

Mr. GERSTEIN. So I was jotting down some. That was quite a long list. But let me start at the top with the National cybersecurity strategy.

What I would say there is that I think the precedent exists. The National security strategy of the United States comes from the White House, and it's an interagency product. The interagency gets a chance to comment and to provide input.

I would see a National cybersecurity strategy similarly that would have the responsibility to be developed by the White House and coordinated and discussed within the interagency. So I think that's key.

On the question of authorities, I believe that the legislation concerning information sharing is critical. That's, of course, the work that this body has done. I think that's critical. Hopefully, in some form—I don't take a position on whether each word is correct. But, rather, the general concept of information sharing between the Government and industry in this space is absolutely imperative.

When you look at capabilities such as CDM and EINSTEIN, certainly EINSTEIN relies on signatures. The only way to get signatures is if there is information sharing. So it's absolutely essential.

On the broader question of authorities, I think for right now the biggest issue that remains is this idea of governance. Several years ago there were discussions on-going between three Cabinet departments about who would have authorities in cyber space, Department of Justice, FBI, and Department of Defense, and Department of Homeland Security.

I still believe that there are likely some seams that need to be considered, and I would think those should be considered as part of the National cybersecurity strategy. That would give an opportunity for the complete discussion to ensure that the authorities are appropriate.

Mr. PERRY. So two other questions in the time I have left.

The naming convention, just your thoughts on that. Just as, you know, it is not appropriate or proper to set up a shotgun in your cabin while you are away in case somebody shows up and they open the door, it is locked, and so it is set with a trigger with a string or something to shoot the intruder, that is not appropriate.

But would it be appropriate in cyber space to set up—and is it possible to set up a system where you are hacked by XYZ country or company, the Federal Government or what have you, that there is a response that is elicited by that attack that does something similar to what happened to Aramco's computer which rendered them useless? I mean, is that a possibility? Would that be something that would be appropriate or is contemplated?

Mr. GERSTEIN. So on the question first on the naming convention, I guess what I would say on this, which I think is pretty important to consider, is the naming convention is, with respect to the internet, a fairly low-level discussion. It's a technical discussion about how things are named. The sharing of that throughout the globe, I think that would be fine.

But I think the more important discussion is at a higher level: What is acceptable internet behavior for a State to allow within its borders? Those sorts of discussions have been had really more on an informal basis and not so much directly with all States like we do with sort of a typical arms control agreement.

This one has been—there have been some discussions with particular States, and they've been on a bilateral basis where they've talked about behaviors. But these continue to evolve.

So on your question about having some sort of shotgun shell, here's what I would be concerned about. This goes back to the question of attribution. So imagine if you think you understand who the perpetrator of the act is, but you have no way to definitively attribute a particular act. If you were to take a catastrophic attack against who you think is the perpetrator and you get it wrong, you would be doing a lot of damage.

So this goes back to this question of you can't just depend on attribution, retribution, proportionality, laws of war-type activities, but you also have to go to the front end and say, "How do I deter? How do I change the calculus of a potential adversary who is thinking about intruding on my networks? Also, how do I deny? So I won't be able to stop everything. But can I set up enclaves so that I'm not exposing my entire network, so I'm not exposing 4 million personnel records or perhaps 18–30 million"—as was reported today—"How do we do a better job in parsing that off so that we're not exposing our entirety of PII information?"

Mr. RATCLIFFE. The gentleman yields back.

The Chair now recognizes the Ranking Member, the gentleman from Louisiana, Mr. Richmond.

Mr. RICHMOND. Thank you, Mr. Chairman. I will try not to take up all of my time.

I will start where my colleague Mr. Perry left off. You know, as I think of sports and other things, even war, I mean, the best defense is a good offense.

So the question for me becomes maybe not the shotgun approach. But what about the Trojan horse approach, that we embed in all of our information something that, if you ever take all of our information, we just activate it, which wipes your computer out?

Look, I am not a programmer. I don't know code. I don't know any of that. But there are people that do. I would just think that we should be able to be in a position that we can put land mines in all of our data that we can activate whenever we need to activate it. If you just happen to have it by accident, so be it, because you shouldn't have it.

Because I think that, you know, for folks back home, the major concern is about our ability to sense these threats, our ability to stop them. I guess the pervasive question is just, where does it end? I don't think anybody fears us enough to not do this.

So the question becomes: Is there anything we can do besides defense to make hackers think twice about messing with us or our information?

Mr. GERSTEIN. So there are people who are thinking about offensive actions and how to use offensive capabilities. Obviously, that discussion needs to be had in a closed session, a Classified session.

But I think, from a general standpoint, again, I go back to establishing attribution is really key to being able to take any action, whether that action is legal action, for example, in the case of the Chinese hackers, where we indicted them in U.S. courts. So there are opportunities to do those kind of things if one can establish attribution.

You know, one topic that we haven't talked as much about today that concerns me greatly is the sensing capacity from the standpoint of our networks today are likely penetrated with either zero day attacks which have not been executed and are awaiting a point in time at which they would be executed or there's an on-going attack. I mean, the likelihood of such a case is very high.

So I worry about being able to establish security on our networks today with the capabilities that we have. As has been pointed out both by the Members of this subcommittee as well as by the other two witnesses, EINSTEIN and CDM have been slow to roll out, and we're still in the process of rolling them out.

Even once that occurs, there will be developmental periods and the departments and agencies will have to ensure that they have the proper procedures in place. So it's not just the DHS availability of the different programs, but it's the implementation within the departments and agencies that's key.

To the point that you asked about, you know, can we do some sort of Trojan horse, this is where research and development and follow-on, hopefully, with acquisition is key. You have to have robust research and development programs that are designed to make headway in this very competitive environment called cyber space. Right now we are largely in a defensive posture where an attack is discovered and then we take some sort of action to respond, mitigate, recover, resiliency, those sorts of action.

Mr. RICHMOND. I will yield the remainder of my time to my colleague, Mr. Perry.

Mr. PERRY. Thank you, Mr. Richmond.

So when you talk about attribution, much like what Mr. Richmond was thinking, I was thinking of, you know, if your computer, if your network, has our data—and I like the land mine concept, but, essentially, it is self-actuating or maybe it can be actuated by somebody on our side of the fence, so to speak, that there are consequences.

I am trying to think about how and maybe why I care whether somebody that didn't necessarily do the hack, so to speak, has the latest plans or the plans to our latest fighter or our personnel data. Do I care how they got them or why they got them? They are not supposed to have them. They are critical to us.

What does it hurt to just obliterate their system and make it nonfunctional as a consequence and maybe even everybody down the line, if that becomes an issue? Do hackers steal information and then store it on somebody else's computer?

Mr. GERSTEIN. They do, indeed. In fact, they even use other people's computers in what we call botnets. So a botnet is the use of another computer. You load the software on and you have attacks that emanate from, if you will, a computer that has nothing to do with the attack other than it is used as a platform.

In fact, if you look at the attacks against the financial sector that were occurring with great regularity 3, 4 years ago, those attacks were botnet attacks. They were denial, distributed——

Mr. PERRY. So is there no way—I mean, I think over time, with your indulgence, Mr. Chairman, the investigators follow the thread back through the botnet computer—right?—to find the original source. I mean, if that capability exists now, why can't the capability go along with it that follows the thread back to the origination and then takes care of business where it occurred?

Mr. GERSTEIN. Well, Congressman, I'm not saying that it couldn't. I guess what I'm saying is I would go back to we need a robust research and development program that looks at all alternatives.

Look at iPhones or cellular telephones today. They now come equipped with a kill switch so that, if your phone has been stolen, you have the ability to turn off that phone and make it so it is no longer anything viable for someone to use. It erases all the data.

So there could be some sort of capability. I would prefer not to speculate on the specifics, but rather say that a robust research and development program should be looking at how do we secure hardware, software, enclaves, networks, in a more cohesive fashion than perhaps we have thought about heretofore.

Mr. PERRY. Thank you, Mr. Chair. I yield.

Mr. RATCLIFFE. The gentleman yields back.

I thank Dr. Gerstein for his valuable testimony. I thank the Members for their questions today.

The Members of the committee may have some additional questions for you, Dr. Gerstein. If that is the case, we will ask you to respond to those in writing.

Pursuant to committee rule 7(e), the hearing record will be held open for a period of 10 days.

Without objection, the subcommittee stands adjourned.
[Whereupon, at 4:28 p.m., the subcommittee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR ANDY OZMENT

Question 1. Today's agency networks are not compartmentalized and as we've seen with several of the recent hacks, once the exterior perimeter is breached, the hacker remains undetected for months and is able to exploit vulnerabilities within the network(s) without passing through additional inspection or security measures. There has been a shift in the private sector towards a Zero Trust model of information security where the networks are segmented and additional security is brought within the network between compartments, thus limiting the ability for the hacker to move internally.

This is becoming an important part of the so-called "defense-in-depth" approach that agencies use today. Is DHS promoting this practice across agencies?

Answer. Response was not received at the time of publication.

Question 2. In April 2014, Deputy Under Secretary for Cybersecurity Phyllis Schneck testified before the Senate Appropriations Committee, "the lack of clear and updated laws reflecting the roles and responsibilities of civilian network security caused unnecessary delays in the incident response . . . In many cases 5 to 6 days were lost in responding to the Heartbleed incident as a result."

As of December 2014, FISMA was updated to give DHS the authorities needed to carry out the operational mission to protect the .Gov domain. Now that DHS has the needed authorities, what is in the way of fully implementing the needed capabilities to protect our Government networks? How does DHS plan to implement FISMA's new authorities?

Answer. Response was not received at the time of publication.

QUESTIONS FROM HONORABLE JAMES R. LANGEVIN FOR ANDY OZMENT

Question 1a. Dr. Ozment, is DHS treating the breach of personnel records and the breach of the SF–86 forms as a single incident or separate incidents?

What criteria does DHS use in making such a determination?

Answer. Response was not received at the time of publication.

Question 1b. What specific criteria did DHS use in making the determination regarding the OPM breach?

Answer. Response was not received at the time of publication.

Question 1c. What was the time line for said determination?

Answer. Response was not received at the time of publication.

Question 2a. Dr. Ozment, I understand that OPM discovered the most recent breach after upgrading their security based on recommendations from US–CERT following the 2014 breach.

Was DHS aware of the indicator of compromise—not its existence on the network but just the indicator itself—OPM used in making that discovery prior to OPM's alerting DHS?

Answer. Response was not received at the time of publication.

Question 2b. How did OPM acquire that indicator of compromise?

Answer. Response was not received at the time of publication.

Question 3a. Dr. Ozment, in your testimony, you reference a binding operational directive issued recently by DHS. The directive instructs agencies to close known vulnerabilities on their internet-facing systems.

Why weren't agencies already closing these known vulnerabilities?

Question 3b. Given that the statutory authority has been in place since December, why did DHS wait until May to issue the directive?

Answer. Response was not received at the time of publication.

Question 3c. Was the issuance of the directive in any way influenced by the OPM breach?

Answer. Response was not received at the time of publication.

Question 4. Dr. Ozment, it is clear that OPM's security posture was poor prior to the breach discovered in March 2014—US–CERT confirmed this, and OPM's Inspector General has been saying so since at least 2007. Do you believe DHS could have done more to help prevent either this most recent breach or the one earlier in 2014? If not, why not?

Answer. Response was not received at the time of publication.

Question 5. Dr. Ozment, in your opinion based on your experience with DHS, is it reasonable to expect agencies to be primarily responsible for defense of their own networks?

Answer. Response was not received at the time of publication.

Question 6. Do agencies have the management capabilities to understand the risks they face and make informed decisions about the resources they need—relative to other demands—to protect their systems and respond and recover from breaches?

Answer. Response was not received at the time of publication.

Question 7. Do agencies have the acquisition capabilities to appropriately contract for cybersecurity services?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR GREGORY C. WILSHUSEN

Question 1. How would you characterize the current state of cybersecurity for Federal civilian information systems?

Answer. The current state of cybersecurity for Federal civilian information systems is that these systems are at high-risk of unauthorized access, use, disclosure, modification, and disruption. In fiscal year 2014, Federal agencies reported 50,289 cyber-related information security incidents to the U.S. Computer Emergency Readiness Team (US–CERT).[1] These incidents included unauthorized access, improper usage, suspicious network activity, social engineering, malicious code, lost or stolen equipment, policy violations, phishing, and denial of service.

Cybersecurity for Federal civilian information systems needs significant improvement. Agencies continue to have shortcomings in assessing risks, developing and implementing security controls, and monitoring results. As I have previously testified,[2] for fiscal year 2014, 19 of the 24 Federal agencies covered by the Chief Financial Officers (CFO) Act reported that information security control deficiencies were either a material weakness or significant deficiency in internal control for financial reporting purposes.[3] In addition, most agencies have weaknesses in five key control categories.[4] For example, 22 of the 24 CFO Act agencies had weaknesses with limiting, preventing, and detecting inappropriate access to computer resources, and managing the configuration of software and hardware. Moreover, the Inspectors General at 23 of the 24 agencies cited information security as a major management challenge for their agency.

Question 2. In your view, who in the Federal Government is responsible for protecting Federal civilian information systems? What is DHS's role, and what is each Federal agency's role? Do you think their respective roles are clearly defined? Who is responsible for enforcing the standards and processes?

Answer. Every single user of Federal civilian information systems is responsible for protecting the systems. In addition, the Secretary of DHS, heads of Federal

---

[1] The number of cyber-related information security incidents (50,289) reported by Federal agencies was determined by subtracting the number of reported non-cyber-related information security incidents (16,879) from the total number of information security incidents (67,168) reported by Federal agencies in fiscal year 2014.

[2] GAO, *Cybersecurity: Actions Needed to Address Challenges Facing Federal Systems,* GAO–15–573T (Washington, DC, Apr. 22, 2015).

[3] A material weakness is a deficiency, or combination of deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected. A significant deficiency is a control deficiency, or a combination of control deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect and correct misstatements on a timely basis.

[4] These categories include controls that are intended to: (1) Limit, detect, and prevent unauthorized access to computer resources; (2) manage the configuration of software and hardware; (3) segregate incompatible duties to ensure that a single individual does not have control over all key aspects of a computer-related operation; (4) planning for continuity of operations in the event of a disaster or disruption; and (5) implementing agency-wide security management programs that are critical to identifying control deficiencies, resolving problems, and managing risks on an on-going basis.

agencies, and the Director of the Office of Management and Budget (OMB) have key responsibilities for protecting these systems, as discussed below.

The Federal Information Security Modernization Act of 2014 (FISMA 2014) assigns DHS a key role in protecting Federal civilian information systems.[5] With an exception for National security systems, the Secretary of DHS is to administer the implementation of agency information security policies and practices for information systems. In this regard, the Secretary of DHS is responsible for:

- assisting the director of OMB in carrying out his or her authorities and functions overseeing agency information security policies and practices;
- developing and overseeing the implementation of binding operational directives to agencies to implement the policies, principles, standards, and guidelines developed by the director of OMB and the requirements of the Act;
- monitoring agency implementation of information security policies and practices;
- convening meetings with senior agency officials to help ensure effective implementation of information security policies and practices;
- coordinating Government-wide efforts on information security policies and practices; and
- providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security.

The head of each Federal agency is to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information systems used or operated by an agency or by a contractor of an agency or other organization on the agency's behalf. To this end, each agency is to develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets ofthe agency, including those provided or managed by another agency, contractor, or other source.

FISMA 2014 helped to clarify the roles of OMB, DHS, and Federal agencies in protecting Federal civilian information systems and bestowed additional esponsibilities upon DHS for "administering the implementation of agency information security policies and practices for information systems." However, testimony by a DHS official at recent Congressional hearings suggests that agencies have questioned how sharing network data with DHS for security monitoring purposes relates to their existing statutory restrictions on the use and disclosure of agency data. Thus, the extent to which DHS can compel an agency to take a specific action in the name of information security may be unclear.

The director of OMB is responsible for enforcing information security standards and processes. FISMA 2014 states that the director shall oversee agency information security policies and practices including overseeing agency compliance with the requirements of the act. FISMA 2014 also states that the director can use any authorized action under section 11303 of title 40 to enforce accountability for compliance with such requirements. The authorized actions include recommending a reduction or an increase in the amount of information resources that the heard of the executive agency proposes for its budget, reducing or otherwise adjusting apportionments and reapportionments of appropriations for information resources, and using other administrative controls over appropriations. The secretary of DHS is responsible for assisting the director in carrying out this authority and function.

Question 3. GAO reported in 2014 that agencies' information security was a major struggle for 23 of 24 agencies. One major weakness identified was agencies' lack of oversight of contractor standards, which resulted in an inconsistent implementation of security standards.

What should Federal agencies be doing to address this problem? What is the role for DHS?

Answer. In August 2014, we recommended that agencies establish and implement IT security oversight procedures for contractor-operated systems.[6] Key procedures for effective oversight that agencies should implement include:

- communicating security and privacy requirements to contractors;
- selecting and documenting controls securing Federal information;
- selecting an independent assessor to evaluate contractor security;
- developing and executing a test plan for assessing security controls;

---

[5] The Federal Information Security Modernization Act of 2014 (Pub. L. 113–283, Dec. 18, 2014) largely superseded the very similar Federal Information Security Management Act of 2002 (Title III, Pub. L. No. 107–347, Dec. 17, 2002).

[6] GAO, *Information Security: Agencies Need to Improve Oversight of Contractor Controls,* GAO–14–612 (Washington, DC: August 8, 2014).

- recommending remedial actions to mitigate identified vulnerabilities;
- developing and implementing plans of actions and milestones for remediation efforts; and
- monitoring implementation and effectiveness of remedial actions.

DHS has a role in monitoring agency implementation of information security policies and practices and in providing operational and technical assistance to agencies in implementing policies and guidelines on information security. In this role, DHS can monitor and assist agencies with effectively overseeing their contractors' implementation of appropriate security controls over Federal information and systems.

Question 4. The Binding Operational Directive issued by Secretary Johnson directs agencies to fix the most critical vulnerabilities on their systems within 30 days. This seems like going after the lowest-hanging fruit. Why not direct agencies to address all their vulnerabilities not just the most critical ones?

Answer. Directing agencies to fix the most critical vulnerabilities helps to prioritize agency efforts by focusing remediation efforts on the vulnerabilities that are more likely to be exploited and cause most harm to the agency. In an environment of constrained resources, this is prudent. Once the most critical vulnerabilities have been mitigated, agencies should then proceed to resolve lower-priority vulnerabilities.

QUESTIONS FROM CHAIRMAN JOHN RATCLIFFE FOR DANIEL M. GERSTEIN [1]

STRATEGIES FOR DEFENDING U.S. GOVERNMENT NETWORKS IN CYBER SPACE ADDENDUM [2]

Question 1a. From your time at the U.S. Department of Homeland Security Science and Technology Directorate what do you see as improvements that can be made to improve DHS' ability to assist Federal agencies secure Government networks?

Answer. Cybersecurity must be looked at through the lens of a campaign plan. In such a plan, numerous initiatives must be implemented to ensure a layered defense, thereby increasing the difficulty of penetrating Government networks.

EINSTEIN 3A and the Continuous Diagnostics and Mitigation (CDM) program are part of such a layered defense. These two systems are designed to work in tandem, with EINSTEIN 3A focusing on keeping threats out of Federal networks and CDM identifying risks inside Government networks. These programs are necessary, but they are not sufficient to ensure cybersecurity across Government networks. Other measures must be developed that compliment these programs.

For example, hardware and software must be hardened. Enclaves can be developed and deployed using a combination of hardened hardware configurations in devices and operating software (such as network, data, access, and security management systems). In addition, newer concepts such as clouds and virtual machines are being used with some success to build enclaves to protect valuable data and sensitive computation. Emerging concepts under development—such as software-defined networking, trusted protection modules, and secure-by-design software systems—may improve our ability to create secure enclaves in the future.

Software assurance must continue to be a point of emphasis. New software must be developed that assures that products are free from vulnerabilities and perform as intended. Legacy systems must be evaluated to ensure that they have necessary security. In addition, information architectures—particularly software and database architectures—for our legacy systems should be rethought and perhaps overhauled for systems containing or dealing with personally identifiable information (PII). And consideration should be given to any future placement of especially sensitive information (such as PII) on secure sites. The Office of Personnel Management data breach should be a serious wake-up call to apply resources and common sense against these sensitive data.

Personnel who operate the networks and users of the systems must be appropriately trained to understand and prevent the various types of cyber attacks they

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research. This product is part of the RAND Corporation testimony series. RAND testimonies record testimony presented by RAND associates to Federal, State, or local legislative committees; Government-appointed commissions and panels; and private review and oversight bodies. The RAND Corporation is a nonprofit research organization providing objective analysis and effective solutions that address the challenges facing the public and private sectors around the world. RAND's publications do not necessarily reflect the opinions of its research clients and sponsors.

[2] This testimony is available for free download at *http://www.rand.org/pubs/testimonies/CT436z1.html.*

are likely to face. Examining previous attacks highlights the degree to which vulnerabilities result from insecurities caused by individuals' actions (for example, during phishing attacks).

Information sharing is a critical component of cybersecurity. The current system of securing software vulnerabilities largely relies on discovering a network intrusion, identifying the attack signature, and developing and deploying patches to address the vulnerabilities. Therefore, information sharing is essential both to gain knowledge that an attack has occurred and to share mitigation procedures.

Finally, inherent in efforts to secure the Federal cyber space is the critical need for a National Cybersecurity Strategy. Such a document would articulate concepts for governance of the .gov domain, as well as cyber doctrine for deterrence, denial, attribution, response, and resilience. Today, no such comprehensive document exists.

Question 1b. What should S&T's role be in helping further develop these programs and future technologies?

Answer. Research and development will be critical to identifying and deploying solutions to secure Federal networks. S&T must take the longer view of the security requirements for the Federal space. Additionally, the focus for DHS S&T should be to systematically examine the cybersecurity landscape and develop solutions that contribute directly to the future layered security architecture supporting Government networks.

This examination also involves looking comprehensively at EINSTEIN 3A and the CDM program to assess their effectiveness and to think more broadly about what the follow-on systems must look like to assure a more forward-looking posture.

Given the importance of cybersecurity to the Department and its components for both securing their networks and supporting their missions, S&T must also assure a keen understanding of their operational and security requirements and look to align its research and development to address identified shortfalls and gaps.

S&T can also serve an important function in assisting non-Governmental entities, such as the critical infrastructure sectors, in coordinating research and development activities for security solutions. One such S&T program exists in the oil and gas sector, and expanding this program into other sectors could provide significant benefit.

Question 2. In your short time at the RAND Corporation you have done extensive research in the cybersecurity field.

Based on your research what more can be done to encourage Federal agencies to adopt the most basic network security standards such as proper cyber hygiene?

Answer. Cybersecurity is not a one-time issue. That is, the Government cannot recruit a competent cyber workforce and train users to operate their information technology systems and expect that this will be sufficient. Rather, cybersecurity must receive constant attention, by all employees and at all levels.

The cyber workforce must be trained and educated to have the latest knowledge and capabilities. They must be continuously challenged through exercises—including simulated and Red Team intrusions—to keep their skills honed. The Federal cyber workforce must also be continuously refreshed to attract the best and brightest to serve. Limited-term appointments (including the highly-qualified experts program) that allow industry experts to serve in Government for periods of 2 or 3 years can provide a necessary infusion of talent.

Awareness campaigns serve to educate the workforce. The DHS "Stop, Think, Connect" campaign is an example of a program designed to increase personal awareness. In addition to awareness, training can be helpful as well. Individuals must be trained to recognize malicious cyber activity that could potentially surface during their interactions on Government information technology systems.

CDM remains a critical component for supporting cyber hygiene on Government networks. When fully deployed, CDM will allow for understanding the network architecture and identifying in near real-time the risks that are in the network by sensing vulnerabilities and anomalous behaviors that could that signal an attack is under way.

Question 3. Federal agencies face similar problems with budgets and resources when trying to address cybersecurity.

What recommendations do you have for DHS and Federal CISOs in devoting resources to combating this threat?

Answer. DHS and Federal chief information security officers must receive necessary funding that allows for up-to-date information technology and security systems for their networks and the users that reside on those networks. In some regards, this requires a culture change. Typically, budgets have been allocated for "mission" activities first and have funded the security of internal networks at minimum levels. This means that fielding advanced cybersecurity systems and even up-

to-date hardware and software does not receive the necessary funding to defeat the determined threats that are targeting Federal networks.

○