HOW SECURE IS VETERANS' PRIVACY INFORMATION?

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED THIRTEENTH CONGRESS

FIRST SESSION

TUESDAY, JUNE 4, 2013

Serial No. 113–21

Printed for the use of the Committee on Veterans' Affairs

U.S. GOVERNMENT PRINTING OFFICE
82–237 WASHINGTON : 2014

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

COMMITTEE ON VETERANS' AFFAIRS

JEFF MILLER, Florida, *Chairman*

DOUG LAMBORN, Colorado
GUS M. BILIRAKIS, Florida
DAVID P. ROE, Tennessee
BILL FLORES, Texas
JEFF DENHAM, California
JON RUNYAN, New Jersey
DAN BENISHEK, Michigan
TIM HUELSKAMP, Kansas
MARK E. AMODEI, Nevada
MIKE COFFMAN, Colorado
BRAD R. WENSTRUP, Ohio
PAUL COOK, California
JACKIE WALORSKI, Indiana

MICHAEL H. MICHAUD, Maine, *Ranking Minority Member*
CORRINE BROWN, Florida
MARK TAKANO, California
JULIA BROWNLEY, California
DINA TITUS, Nevada
ANN KIRKPATRICK, Arizona
RAUL RUIZ, California
GLORIA NEGRETE MCLEOD, California
ANN M. KUSTER, New Hampshire
BETO O'ROURKE, Texas
TIMOTHY J. WALZ, Minnesota

HELEN W. TOLAR, *Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

MIKE COFFMAN, Colorado, *Chairman*

DOUG LAMBORN, Colorado
DAVID P. ROE, Tennessee
TIM HUELSKAMP, Kansas
DAN BENISHEK, Michigan
JACKIE WALORSKI, Indiana

ANN KIRKPATRICK, Arizona, *Ranking Minority Member*
MARK TAKANO, California
ANN M. KUSTER, New Hampshire
BETO O'ROURKE, Texas
TIMOTHY J. WALZ, Minnesota

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Veterans' Affairs are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

June 4, 2013

HOW SECURE IS VETERANS' PRIVACY INFORMATION?

Tuesday, June 4, 2013

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS' AFFAIRS,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Washington, D.C.

The Subcommittee met, pursuant to notice, at 2:50 p.m., in Room 334, Cannon House Office Building, Hon. Mike Coffman [Chairman of the Subcommittee] presiding.

Present: Representatives Coffman, Lamborn, Roe, Huelskamp, Walorski, Kirkpatrick, O'Rourke, and Walz.

OPENING STATEMENT OF CHAIRMAN COFFMAN

Mr. COFFMAN. Good afternoon. I would like to welcome everyone to today's hearing titled "How Secure is Veterans' Private Information?" Reports from VA's Office of Inspector General, private inspector consultants brought on by VA, and this Subcommittee's own investigation have revealed tremendous problems within VA's Office of Information and Technology. Some of these issues have been made public in the Inspector General reports which outline mismanagement of human measures and the lack of much-needed technical expertise.

Other issues have been less publicized, such as those captured in the Deloitte, quote/unquote, "DeepDive" that identified gaps in OI&T's organizational structure and a poorly executed business model. The latter report recognized the growth of VA by 33 percent since 2006, growth that is mirrored by the expansion of VA's computer network. Unfortunately, there has not been a comparable growth in the technical personnel needed to manage security of VA's sprawling network.

These failures have created problems for both the Department and for veterans. The Inspector General substantiated that VA was transmitting sensitive data, including personally identifiable information and internal network routing information, over an unencrypted telecommunications carrier network, both violations of Federal regulation and basic IT security. The IG also noted that VA has not implemented technical configuration controls to ensure encryption of sensitive data, despite VA and Federal information security requirements.

Similarly, it is evident that software patches are not up-to-date across the network, too many users have administrative access, security software is not up-to-date on older computers, and computer ports are not properly secured. There is little to no security of file transfer protocol and Web pages are vulnerable, allowing unauthor-

ized access to veterans' unprotected personal information within the system.

While these issues alone give cause for grave concern, this Subcommittee's investigation has identified even greater problems. The entire veteran database in VA, containing personally identifiable information on roughly 20 million veterans, is not encrypted, and evidence suggests that it has repeatedly been compromised since 2010 by foreign actors, including China and possibly by Russia.

Recently, the Subcommittee discussed VA's authorization to operate, a formal declaration that authorizes operation of a product on VA's network which explicitly accepts the risk to agency operators and was told that, quote, "VA's secrecy posture was never at risk," unquote. In fact, VA's security posture has been an unacceptable risk for at least 3 years as sophisticated actors use weaknesses in VA's security posture to exploit the system and remove veterans' information and system passwords. While VA knew foreign intruders had been in the network, the Department was never sure what exactly these foreign actors took because the outgoing data was encrypted by the trespassers.

These actors have had constant access to VA systems and data, information which included unencrypted databases containing hundreds of thousands to millions of instances of veterans' information, such as veterans' and dependents' names, Social Security numbers, dates of birth, and protected health information. Notwithstanding these problems, VA has waived or arbitrarily extended accreditation of its security system on its network. It is evident that VA's waivers or extensions of accreditation only appear to resolve material weaknesses without actually resolving those weaknesses.

VA's IT management knowingly accepted the security risk by waiving the security requirements even though such waivers are not appropriate. This lapse in computer security and the subsequent attempts by VA officials to conceal this problem are intolerable, and I look forward to a candid discussion about these issues.

I now yield to Ranking Member Kirkpatrick for her opening statement.

[THE PREPARED STATEMENT OF CHAIRMAN COFFMAN APPEARS IN THE APPENDIX]

OPENING STATEMENT OF HON. ANN KIRKPATRICK

Mrs. KIRKPATRICK. Thank you, Mr. Chairman.

As the Department of Veterans Affairs works hard to serve the needs of today's veterans, they must work equally hard to protect their personal information. Today's hearing is an attempt to determine whether a veteran's private information is secure.

Mr. Chairman, veterans need to know that when they ask the VA for services and benefits that they have earned, the information they submit in order to get those benefits will not be compromised under any circumstances. I hope that the VA came prepared today to provide assurances to Congress and veterans that their information technology systems are secure. We expect VA to also answer our questions directly and honestly. As we get questions from veterans in our district, we want to provide complete and honest answers to them.

Congress received a letter from Mr. Jerry L. Davis, now a former employee at the VA, who states that, quote, "There is a clear and present danger and risk of exposure and compromise of sensitive data," end quote.

Mrs. KIRKPATRICK. I share the Chairman's concern on whether VA is following the required government practices and policies regarding the monitoring and remediation of system risk.

Two OIG reports, from 2012 and 2013, raised additional concerns. The 2012 report questions whether the agency has the proper strategic human capital management program to meet mission-critical system capabilities as the VA moves into the 21st century. The second, 2013, OIG report faults VA for failing to secure private information by not encrypting health data transmitted to outpatient clinics and external business partners. The VA must address the concerns raised and assure veterans who come to the VA for assistance that their personal information is secure.

I want to thank everyone for being here today. I would also like to thank the witnesses for their testimony and for answering questions about the security of veterans' private information at the Department of Veterans Affairs.

Thank you, Mr. Chairman. I yield back.

[THE PREPARED STATEMENT OF HON. KIRKPATRICK APPEARS IN THE APPENDIX]

Mr. COFFMAN. Thank you, Ranking Member Kirkpatrick.

I would now like to welcome our first panel to the witness table. On this panel we will hear from Ms. Linda Halliday, Assistant Inspector General for Audits and Evaluations from the VA's Office of Inspector General. Accompanying Ms. Halliday is Ms. Sondra McCauley, Deputy Assistant Inspector General for Audits and Evaluations, and Mr. Michael Bowman, Director of the Information Technology and Security Audits Division.

Before I recognize the panel, I ask that you please rise and raise your right hand.

[Witnesses sworn.]

Mr. COFFMAN. Ms. Halliday, you are now recognized for 5 minutes.

TESTIMONY OF LINDA A. HALLIDAY, ASSISTANT INSPECTOR GENERAL FOR AUDITS AND EVALUATIONS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY SONDRA MCCAULEY, DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDITS AND EVALUATIONS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS, AND MICHAEL BOWMAN, DIRECTOR, INFORMATION TECHNOLOGY AND SECURITY AUDITS DIVISION, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS

Ms. HALLIDAY. Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to testify on VA's security of veterans private information. With me today are Ms. Sondra McCauley, my deputy, and Mr. Michael Bowman, the Director of the OIG's Information Technology Security Division.

Secure systems and networks are essential to VA's programs and operations for delivering benefits and services to our Nation's veterans, yet OIG reports continue to disclose a pattern of ineffective information security which places VA at unnecessary risk. For more than 10 consecutive years, our consolidated financial statement audit reports have identified IT security as a material weakness.

We also perform annual reviews of VA's compliance with the requirements of the Federal Information Security Management Act, known as FISMA. This act serves as a catalyst for developing the framework to protect agency IT systems and sensitive information.

As last year's FISMA audit progressed, we did note VA focused more efforts to standardize information security controls. Mid-year in 2012, VA initiated CRISP, the Continuous Readiness and Information Security Program, to ensure year-round monitoring and to establish a team responsible for resolving the IT material weakness. However, CRISP was not in place long enough to adequately improve the material weakness for last year's FISMA report. The report will be issued this month and will include 32 recommendations for improving VA's information security program.

We found repeat weaknesses and vulnerabilities in four key areas. In the area of system access, we found password standards that were not consistently implemented and user accounts that were not enforcing minimal access privileges.

In the area of configuration management, we found critical systems lacked appropriate baseline controls and up-to-date vulnerability patches. Also, the policies and procedures for authorizing, testing, and approval of system changes were not consistently implemented.

In the area of security management, VA still had to address about 4,000 outstanding security vulnerabilities. We found its risk assessments and security plans were outdated and in some instances were not consistently put in place to reflect VA's current IT environment or Federal standards.

In the fourth area, contingency planning, we found some plans were not fully tested or updated, and in addition, backup tapes were not always encrypted prior to being sent to offsite storage. More importantly, we continue to identify significant technical weaknesses in databases, servers, network devices supporting sensitive data exchanges among VA facilities. Many of these weaknesses are due to inconsistent program enforcement and ineffective communication between VA management and field offices.

In addition to FISMA, OIG projects over the past 2 years have identified information security deficiencies, placing sensitive veterans data at risk of unauthorized access, loss, or disclosure. Specifically, we reported on a broad range of security concerns, including VA's transmission of sensitive data and internal network routing information over an unencrypted carrier network, and VA's external data-sharing agreements and system interconnections which resulted in unsecured electronic and hard copy data at VA medical centers and co-located research facilities. We reported that 48 percent of VA's 400,000 encryption software licenses, valued at about $5.1 million, remained unused, leaving VA computers vulnerable. And we reported on a backlog of personnel background checks

which were inappropriately prohibiting some 3,000 contractors from working on awarded contracts.

In summary, our audit reports and findings and recommendations provide a roadmap for VA to improve its information security program, and VA needs to focus on addressing previously reported security issues related to the IT material weakness, they need to remediate high-risk system issues in their Plans of Actions and Milestones, and they need to establish effective processes for continuous monitoring and to perform vulnerability assessments.

Mr. Chairman, this concludes my statement, and we would be happy to answer any questions you or the Subcommittee may have.

[THE PREPARED STATEMENT OF LINDA A. HALLIDAY APPEARS IN THE APPENDIX]

Mr. COFFMAN. Thank, Ms. Halliday.

How effective are VA facilities with protecting sensitive veteran data?

Ms. HALLIDAY. Well, based on our oversight, we're continuing to find information security vulnerabilities at almost every VA medical center we visit. We visit 20 to 30 VAMCs a year as part of our FISMA work and we consistently find problems. The types of vulnerabilities include weak passwords, missing software patches, lack of software updates, excessive permissions, and unnecessary user accounts left on the system.

Mr. COFFMAN. What are the foremost reasons why, after all this time, information security is still a major concern at the VA?

Ms. HALLIDAY. I would say that ineffective access controls, ineffective configuration management controls, I think ineffective management of systems interconnection and inadequate contractor oversight would be a fourth major reason.

Mr. COFFMAN. Ms. Halliday, based on your ongoing oversight work, is VA likely to get rid of its IT security material weaknesses this year?

Ms. HALLIDAY. At this point it is too early to conclude. We do expect that the CRISP initiative, which is starting to provide continuous monitoring, will be in place for the entire 12 months of this fiscal year 2013 FISMA review. Our concern, while we're seeing weaknesses occur with less frequency, they are still occurring and they are repeat occurrences and vulnerabilities that we have reported on in fiscal year 2012 and earlier years.

Mr. COFFMAN. What are VA's most significant risks related to adequately protecting its systems and sensitive data?

Ms. HALLIDAY. The first would probably be ineffective access controls. That's where critical systems had accounts with default passwords that were considered weak passwords, i.e. easy to guess. User accounts with access rights that were not appropriate. In other words, you want to make sure that all users have a need for that information and that they have a security level appropriate to that need. We also identify unsecured electronic and hard copy research data at VA medical centers and co-located research facilities.

So that covers access controls. Then we have inconsistent configuration management controls. Systems include key databases supporting critical applications, but they are not patched timely or secured and configured to mitigate previously known information

vulnerabilities. We have ineffective management of system interconnections. That's VA sensitive data such as health records and internal Internet protocol, addresses. They are transmitted between VA medical centers and the community-based outpatient clinics using unencrypted protocols. And then access control and configuration management. These are all very significant risks that VA faces.

As far as inadequate contractor oversight, contractors without the appropriate security clearances are gaining access to some VA mission critical systems, and we did a report on not having security clearances in place before gaining access to the systems with contractors.

Mr. COFFMAN. Moving forward, what steps can VA take to prevent the loss of sensitive data?

Ms. HALLIDAY. I think VA really needs to improve its continuous monitoring process to ensure all the controls are operating as intended, and it needs to address the external organizations that it works with to make sure that they are adequately protecting sensitive veteran data in accordance with the VA policy and FISMA requirements. VA needs to ensure all service provider contracts include provisions to implement information security protections in accordance with their policies and procedures.

Mr. COFFMAN. Thank you.

Ranking Member Kirkpatrick.

Mrs. KIRKPATRICK. You testified that there's a 10-year period of weakness and vulnerability. So there was a report given to the VA year after year after year. In that 10-year span, did you see an increase in vulnerability and weakness? A decrease? Can you quantify that for me over that 10-year period?

Ms. HALLIDAY. We do an audit of VA's consolidated financial statements annually and our contractors look at all of the controls associated with information security. They have felt that it has been a material weakness in VA for 10 full years.

Mrs. KIRKPATRICK. Has it been the same level of weakness and vulnerability? What I mean is, has it been getting worse for a while or has it gotten better?

Ms. HALLIDAY. I don't think you ever get the exact same level of vulnerability. I think our concern, we report out on these various problems based on the testing. A couple years ago, VA's Plan of Actions and Milestones addressing security vulnerabilities was almost at 15,000 items that were outstanding and unaddressed. This past year VA has gotten it down to about 4,000, but that's still 4,000 security weaknesses and vulnerabilities that haven't been addressed. It is too many.

Mrs. KIRKPATRICK. Do you think that the CRISP program is helping them address those vulnerabilities more quickly?

Ms. HALLIDAY. Based on the preliminary and early testing, yes. We are still seeing and identifying security weaknesses and vulnerabilities, but to a lesser extent that we've seen that in the past. I would also have to say that VA is actively working with us to try and make sure that they understand what we are finding as part of our FISMA testing, understand the full scope so that they can put the right fixes in place.

Mrs. KIRKPATRICK. That was going to be one of my questions. When you issue a report, do you actually have a conversation with leadership at the VA about what needs to be implemented?

Ms. HALLIDAY. Absolutely.

Mrs. KIRKPATRICK. And is that on an ongoing basis?

Ms. HALLIDAY. Yes, it is. With this information security material weakness rising to the last material weakness in the Department's financial statements, the Secretary on down through his chain of command has had it on their radar. They are working very hard. And we have made sure that we have been communicating with the Department. For example, that if we employ certain tools in our oversight to scan their systems, they are also acquiring those same state-of-the-art tools. So I think that there is an effort there, and at least this year and part of last year the communications have been better between what OIG is doing in the field, finding, and getting it remediated.

Mrs. KIRKPATRICK. I have one last question. I have a concern in your audit report. You say that you are concerned with a lack of human resources, and your statement says OIT experienced vacancies and excessive turnover in key leadership positions responsible for OIT's strategic human capital management program. Could you tell the Committee a little bit more about that? What do you mean by excessive turnover?

Ms. HALLIDAY. I'm going to ask Sondra McCauley to take that.

Mrs. KIRKPATRICK. If you could just quantify that and give some reasons why you think that's happening.

Ms. MCCAULEY. Excessive turnover in terms of the leadership within OIT in terms of managing the program. Turnover in terms of the program managers and project managers needed to manage each specific project, if you will, as well as a reliance on contractors to do a lot of the jobs that we really need government personnel to do.

Mrs. KIRKPATRICK. And why do you think that there is that excessive turnover?

Ms. MCCAULEY. Some of it was attributed to a lack of planning, that is the need for a human capital plan to really focus in on the succession planning at the leadership level. But also to better identify the skills that were needed to help manage these IT programs, and what would be a better contractor-to-FTE ratio to manage the programs.

Mrs. KIRKPATRICK. Okay. Thank you. I yield back, Mr. Chairman.

Mr. COFFMAN. Thank you, Ranking Member Kirkpatrick.

Mr. Lamborn, you are recognized for 5 minutes.

Mr. LAMBORN. Thank you, Mr. Chairman. And before I ask my questions, I want to thank you, Mr. Chairman, for having this hearing. This is such an important topic. And there is so much going on here that I was frankly not really aware of and should have been, and we need to be aware what's going on. So thank you for your leadership. This is so critical.

Ms. Halliday, I am stunned about what's going on here. And you said in your written testimony, "Lacking proper safeguards, IT systems are vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch at-

tacks against other systems. VA has at times been the victim of such malicious intent.''

Can you tell us what you know about these malicious attacks on the VA's sensitive information? Who committed these?

Ms. HALLIDAY. I will let Mr. Bowman speak to this one. It is in his area.

Mr. BOWMAN. Thank you.

We were informed of an intrusion by foreign countries through the Network Security Operations Center. The specifics of that, the foreign countries have actually compromised the domain controller and gained access to email accounts and were taking email information of the senior leadership at VA. The difficult part was, is VA was unsure how the foreign countries gained access to the networks and what was actually being transmitted out of the VA networks back to the original source. That's the one that's most current that I'm aware of. We also reference 2006 with the stolen laptop and the loss of the 26 million records. But those are the two main things that come to mind.

As far as our ongoing FISMA work, we do continue to identify weaknesses with the critical databases that does host sensitive data, and the Web applications that are facing the Internet do have well-known vulnerabilities that could be exploited from the Internet. And these are ongoing from year-to-year. So there are significant risks out there that are related to this.

Mr. LAMBORN. And why don't we know how much was taken?

Mr. BOWMAN. A lot of it is having the right tools in place, such as intrusion-detection systems, and audit logs turned on. In some cases, VA doesn't have audit logs enabled, so it is unaware of how these systems have been infiltrated and what data has been captured and what has been transmitted. Good Intrusion Detection Systems on all the network segments are important to identify the attack signatures.

Mr. LAMBORN. Okay. What is the kind of sensitive information concerning a veteran like in my district back in Colorado Springs that could have been compromised?

Mr. BOWMAN. It is more personal identifiable information that could be used to commit fraud. Let's say a malicious intruder gains access to a database and has the Social Security number, name, and the date of birth, they could use that to commit credit card fraud. And that's the main risk to veterans.

Mr. LAMBORN. And with the 20 or so million veterans who are on the system, the VA doesn't know how few or how many of their sensitive information like Social Security numbers have been compromised?

Mr. BOWMAN. That's a potential risk.

Mr. LAMBORN. It could be all of them?

Mr. BOWMAN. Yes, without having audit logging enabled, you don't know what has been compromised or how often those systems have been accessed in an unauthorized manner.

Mr. LAMBORN. Would either of you ladies like to add to what I've been asking?

Ms. HALLIDAY. No, I think Mike answered it perfectly.

Mr. LAMBORN. I'm just amazed at this. I mean, this is serious. And the VA has known about this for up to 10 years now?

Mr. BOWMAN. We've reported significant vulnerabilities for well over 10 years, as indicated by the IT material weakness. In the last 5 years, we have increased our assessment of the security controls through our user vulnerability assessment tools, database tools, Web app tools, so we think our evaluation is more comprehensive. In the last 5 years, we've shown consistent vulnerabilities from year to year that put the VA systems at risk.

Mr. LAMBORN. And you mentioned potential state actors with malicious intent. Was that fairly recent that those attempts or those actions were detected?

Mr. BOWMAN. I heard about that within the last year and a half.

Mr. LAMBORN. So there's a pattern of knowing about this for 10 years leading up to a malicious capture of who knows how many Social Security numbers or other sensitive pieces of information of up to 20 million veterans within the last year and a half. Is that a proper understanding?

Mr. BOWMAN. It is possible. We don't know.

Mr. LAMBORN. Thank you, Mr. Chairman. I yield back.

Mr. COFFMAN. Thank you, Mr. Lamborn.

Mr. O'Rourke for 5 minutes.

Mr. O'ROURKE. Thank you, Mr. Chair.

For Ms. Halliday, I actually wanted to follow up on some questions Mr. Lamborn was asking. For a veteran back home in the districts we represent, specifically, have we seen any consequences that we've been able to document in terms of their information being stolen and used by someone who has broken into this system? And not necessarily in my district, but can you point to some examples of how this has affected people that we represent?

Ms. HALLIDAY. VA has an NSOC program where you report security incidents to them. They will prioritize it and start to work on the severity of those incidents. There is normally a good record then given of the facts of what happened and they will look at the controls and try to put the remediation in place. There are hundreds of incidents reported on an annual basis.

Mr. O'ROURKE. And can you take us through one to illustrate the consequences? For example, Social Security information was taken. They used that to impersonate that veteran to try to take benefits or to obtain credit cards or—

Ms. HALLIDAY. I do not have an example.

Mr. O'ROURKE. Okay. Let me just ask you or Mr. Bowman, do you know of examples that have been documented, specific consequences? I mean, I agree with what everyone has said so far, the overall problem and the threat represented by these security vulnerabilities is unacceptable and needs to be addressed and needs to be fixed, but I also want to understand the human dimension of this, what problems it has already caused for veterans, if any, if you've been able to document them. I am assuming there have been. So anyhow, that's something we would like to follow up on.

Then I guess for Mr. Bowman, what's the expectation in terms of being able to address these? When should this Committee expect to hear back from Ms. Halliday at a future hearing that these findings and problems that have been uncovered have been addressed to our satisfaction and that we feel that we have a reasonable level

of security, these threats have been closed, and we are now happy with that system? What's a date that you could point us towards?

Mr. BOWMAN. VA plans to implement a fully developed continuous monitoring program within the next 6 to 8 months. Using that, they should have a better visibility of the security posture of their IT systems. We have 32 outstanding recommendations from our FISMA work that need to be addressed to improve the security posture. It will probably take VA well over a year, year and a half to get a good handle on that and address those issues.

So if we could possibly convene maybe a year from now, VA may be able to communicate some significant progress in their IT security program; we will be able to communicate that as well.

Mr. O'ROURKE. And just to make sure that I understand what you just said, within 12 to 18 months those 32 recommendations would be implemented?

Mr. BOWMAN. I don't know for sure, but I think that's a reasonable timeline if VA takes an aggressive approach for improving its security program.

Mr. O'ROURKE. Okay.

Ms. HALLIDAY. Sir, we just received the official comments from Mr. Warren on the 32 recommendations and the implementation plans that they will deploy regarding those 32 recommendations. There are various timeframes associated with that. But our first conclusion will come at the end of this year's audit of the consolidated financial statements as to whether they would drop that material weakness or not, and all of the testing will be happening over the summer. So that report is issued on November 15th, and it will assess whether the material weakness remains or it drops to a significant deficiency. At this point, since VA has not fully implemented its continuous monitoring, Mike is exactly correct that it is probably going to take longer than a few months to take care of this.

Mr. O'ROURKE. Okay. Thank you.

Mr. Chairman, I yield back.

Mr. COFFMAN. Thank you, Mr. O'Rourke.

Dr. Roe for 5 minutes.

Mr. ROE. I thank the Chairman.

Ms. Halliday, thank you and your team for the excellent work you've done and certainly informing our Committee of the problems. I guess my concern is, is that this mirrors and patterns many of the other hearings I've been to where we can't seem to get the electronic health record fixed year after year, and it looks like that security is a problem year after year. We just passed a bill in the House, CISPA.

Most of us in this room have been to classified briefings on the security risks that this country has from outside bad actors. And I've got to go home this weekend, as every member up here does, and when this information gets out, veterans are going to come to me, there are many veterans sitting right up here at this dais, and they are going to say, are my records secure? And I'm going to have to look them in the eye and say, no, they are not, from what I've heard. And that's not a very acceptable answer, especially after 10 years, and especially after we know the risks in the government.

You haven't looked at every other phase, but do other departments in the U.S. Government share these same problems? In other words, is this a systemic-wide problem across government or is this just VA specific? And you may not be able to answer that question.

Ms. HALLIDAY. I can't give you a definitive answer, but it is a problem for those agencies that are dealing with privacy-type information.

Mr. ROE. You know, we've been asked as a Congress, we've been instructed in private that it is a severe problem for business. We've been asked to look at some privacy issues about how you—and we have a department of government that's not even doing what we're asking business to do right now.

I think there are a couple of things that I would like to ask just briefly, and government-wide we don't know. How will we know that when we do go home, when can we say that this information will be secure? And we certainly know how when you steal private information, whether it is through somebody getting your debit card number or whatever, what it is used for, it is basically just to steal from you. So is that it, just mainly you think, or is it access to other government agencies through the VA? Is this the back door to some other agencies?

Ms. HALLIDAY. When we can say that the security of veterans information has been taken care of, I think will be at the point when VA addresses all the recommendations in the reports that we have made with regards to FISMA. We've given them a roadmap to fix things. It is such a decentralized organization that they have to bring a culture of accountability, personal accountability for every action, and they need to make sure they have a consistent implementation of the policies and procedures. We don't quite see that yet with the FISMA testing or the testing done as part of the consolidated financial statements.

Mr. ROE. Let's say you go to a VA medical center somewhere, and you mentioned that some of the software wasn't up to date, passwords, you can figure it out, 111, whatever, four 1s in a row, whatever. Who is responsible for that and what penalty is it if you don't do anything?

Ms. HALLIDAY. The responsibility lies with the CIO in the Department of Veterans Affairs and it tiers down through that organization.

Mr. ROE. Okay. When a breach occurs, what does VA do then? When you know you've been hacked or there is an attempt. Let's see you haven't been breached, but you know that your firewall has been pinged, what do you do?

Ms. HALLIDAY. You assess the severity of it based on the facts you can determine. You get a team together to look at how to fix whatever controls are needed to be fixed related to what happened. And VA has been trying to do that, but they have a significant number of security incidents.

Mr. ROE. And I'm thinking, I am a veteran, I'm sitting here thinking okay, we've lost a laptop computer with 20 million bits of information on it and the system is not secure now. That doesn't give me a lot of confidence if I go to the VA to hand over my Social Security number and all that.

Ms. HALLIDAY. Right. VA did mandate cybersecurity and privacy awareness training nationwide to bring down a level of personal accountability to every individual that's doing work and touching veteran-sensitive information to make sure it brought accountability to this process and requires individuals to sign a statement that they will protect the veteran's information. So that is a step in the right direction.

Mr. ROE. Ms. Halliday, thank you. And I think we have our marching orders, and we will hear from the other two panels. But I think in 12 months we should be able to sit here, or less, and be able to look our veterans in the eye and say to them that your information is as secure as we can do it. I understand there is nothing that's 100 percent, I got that. But it is relatively secure. Am I correct in that?

Ms. HALLIDAY. Absolutely. Both the prior VA Secretary and the current have asked for the gold standard in protecting VA's veterans information, and I think the expectation should be nothing less.

Mr. ROE. Thank you, Mr. Chairman. I yield back.

Mr. COFFMAN. Mr. Walz for 5 minutes.

Mr. WALZ. Thank you, Mr. Chairman.

Ms. Halliday and your team, thank you once again for coming.

Again, we have been through these hearings and we listen to them. I guess the part I'm getting at is, and many of us, myself included, I've been advocating for more sharing of data, especially between DoD and VA, been advocating for being able to get some of that information to some of our partners, like the county veteran service officers, to help with claim processing, been advocating for bringing private medical data into the system to help speed the claims process.

With that being said, with the VA and its research partners, how do they do the formal agreements between them? And I guess the point I'm getting at here is, is this issue we're addressing—and I would assume you have lots of contact with your private sector counterparts and best practices—this very same thing happens in the private sector, correct, but there's no requirement for them to report when there is a breach. Is that correct?

Ms. HALLIDAY. Pretty much, yes.

Mr. WALZ. How are these agreements done and if there's a breach at a research institution on the private sector side, how do we know they are reporting that breach back and who is ultimately responsible in those agreements?

Ms. HALLIDAY. Basically, you need a formal agreement that outlines the roles and responsibilities of both the external partner and VA. In that particular instance, we see some real inconsistencies and some of these agreements are not being put in place.

The second you would like to do is make sure that, whatever arrangement VA is entering into, that organization has commensurate controls with VA so that they can adhere to VA's policies and procedures.

Mr. WALZ. But they are not required to adhere to FISMA, is that correct, private entity?

Ms. HALLIDAY. Right. But you can establish those terms in these agreements.

Mr. WALZ. Okay.

Ms. HALLIDAY. And that's where you should do that. Because if you have one side, securing veterans' information very tightly and another handling it very loosely, you have a problem.

Mr. WALZ. Is it safe to say we then do not know the scope of the problem yet if those are lacking, because there are many, many of these agreements.

Ms. HALLIDAY. Absolutely.

Mr. WALZ. Okay. So we have no idea on the scope of that.

Ms. HALLIDAY. Right.

Mr. WALZ. When you look at this, where is the model? Is there an entity, an institution that's out there that is the gold standard of best practices, how should this be done? I mean, there are standards and protocols that should be implemented. Who is doing it on the scale of VA? Is Citibank doing it? Is Credit Suisse doing it? Who is doing it that it looks correct? Because the targets here aren't necessarily targets because they are veterans. They are targets because they are easy, is that correct, or they are trying to make it easy in many cases. Can you give me an example of who is the gold standard?

Ms. HALLIDAY. We can't give you an example.

Mr. WALZ. Is that for lack of your knowledge on what others are doing or is that because there might not be one?

Ms. HALLIDAY. I would say more lack of our having direct knowledge of who is actually performing specific practices. Some people might attest that they do have a gold standard, but when you look behind it and you see breaches and problems with that. We haven't looked at that so I can't really answer.

Mr. WALZ. If we had some of them here to talk to us about the problems they are having, that might help us get an understanding of this and let the VA bring some of those things in.

Ms. HALLIDAY. I think there's always an opportunity to bring in best practices from the outside and from other Federal agencies.

Mr. WALZ. Okay. So if we implement all the protocols that you've put out there, and I think you gave me the number of 4,000 potential weaknesses or vulnerabilities, if we implemented all of those and were able to do it, what's the cost associated with that? I understand what the cost of not doing it is great. It is a breach of trust and security of our veterans. What's the implication? Is that not something you factor in when you do your assessment?

Ms. HALLIDAY. Sir, I would not have that answer, but you should ask VA.

Mr. WALZ. Okay. Very good.

All right. Well, again, I thank you for your service. It is invaluable. As I always say, the more that we can do to support the IG, the better government we get out of it. So thank you.

Ms. HALLIDAY. Thank you.

Mr. COFFMAN. Mr. Huelskamp for 5 minutes.

Mr. HUELSKAMP. Thank you, Mr. Chairman. I appreciate you providing the opportunity for this hearing. And I must say I have a lot of words to describe my feelings, and embarrassed by the actions or lack thereof by the VA might be one of those. Shocked. Surprised. I guess I will probably be even more surprised by later testimony.

But if I understand correctly, one of the things that you did mention, that there was a violation or personal emails of the Secretary and high-level staff were compromised. And can you describe that a little bit further?

Mr. BOWMAN. My understanding is that when the domain controllers got compromised, they got access to the senior leadership email accounts, and there is information that indicates that those emails were exported outside the VA network.

The value of them is unknown. What they did with those emails is unknown. But whenever you compromise a domain controller, essentially you own the enterprise. That's the seriousness of it.

Mr. HUELSKAMP. I appreciate that. You own access to 20 million records, plus that of their dependents. What was the VA response when you brought that to their attention?

Mr. BOWMAN. It wasn't formally communicated to me. I heard it in a meeting that was discussed between the NSOC. And they probably were unaware I was listening in, but that is just what I heard, just by observing some of these meetings and VA describing these events.

Mr. HUELSKAMP. And this is very shocking, Mr. Chairman. I know we have a letter in front of us from a very high-ranking official at the VA that says, quote, "VA's security posture was never at risk." Was never at risk. And that's a quote from a high-ranking official. And I would guess that perhaps they used email to put this together. Can you imagine the thought that the folks that were hacking the system were actually reading this email as they were exporting 20 million private records. And you indicated we do have evidence potentially of external state-sponsored espionage that might be occurring to the VA. One of you had indicated that was a possibility?

Mr. BOWMAN. That's my understanding.

Mr. HUELSKAMP. Okay. And did you bring this to the VA's attention and what was their response?

Mr. BOWMAN. We haven't. With the FISMA work, we haven't specifically addressed that issue. We do get into incident handling and monitoring. And we identify every year there are network connections that aren't being monitored by VA. So the risk is that you could have systems compromised, data being transmitted externally, and VA could be unaware of it.

Mr. HUELSKAMP. They could be unaware that the information is actually leaving. And if asked, they could potentially, even under oath say we know of no such transmission, which if I understand correctly might absolutely be true and would suggest obviously when you've given up control of the system like you indicated you would have actually no idea of the threat then?

Mr. BOWMAN. That's correct.

Ms. HALLIDAY. Sir, one of the things that we do as part of our oversight is gain an understanding of what is happening in the VA environment, and then we send information to our contractor who is doing the actual FISMA assessment to put the right work steps in place to do full evaluations, to understand and properly assess the risks. That's all happening as part of the FISMA process.

Mr. HUELSKAMP. And I appreciate your work. You have a very difficult task of identifying the problems and hopefully providing

some solutions, but it is up to the VA, maybe after 10 years, to finally implement some of those.

The latest thing I see in your report is an incident from March 2013 in which sensitive, private, perhaps medical and personal data was transmitted over an unencrypted telecommunications carrier network. Can you tell me what happened when that personal data was transmitted unencrypted? Apparently VA did not know they were doing that. What's their response? You indicate that the management acknowledged this practice and formally accepted the security risk. Did they identify who was at risk, how they were at risk, and did they close this security gap?

Mr. BOWMAN. Yes, we received a hotline complaint discussing the transmission of unencrypted data between the medical centers and the community-based outpatient clinics using unencrypted protocols over a telecommunication carrier network. We went and discussed with the network engineers and various levels with VA, and they admitted that this is a common practice.

Mr. HUELSKAMP. They admitted this is a common practice.

Mr. BOWMAN. It is a common practice. But a mitigating factor is, is they logically segment that traffic from other customer traffic. The downside of that is it still needs to be encrypted, and there are technological solutions that can encrypt that traffic when it is outside of VA's span of control. Now, VA responded to that report by saying they plan to implement encryption controls, so that will improve that risk of losing that data as it leaves VA's span of control.

Mr. HUELSKAMP. I'm sorry, Mr. Chairman, one last question.

So they planned. Do you know if they actually have implemented the encryption to protect sensitive data?

Mr. BOWMAN. My understanding is that edge router encryption controls have not been implemented yet.

Mr. HUELSKAMP. I yield back, Mr. Chairman.

Mr. COFFMAN. Ms. Walorski for 5 minutes.

Mrs. WALORSKI. Thank you, Mr. Chairman.

I appreciate the report, I appreciate the information. I will tell you, when I was in the Indiana House, we did hold companies responsible for these massive breaches of identify theft, especially when a Social Security number was in the breach. And so we did have legislation and we still do, and I think 17 or 18 other States now have it as well, holding private companies responsible, and if there's a breach that the buck does stop with them for immediate information sharing, in some cases freezing credit reports.

So my first question is on this information as it is leaked to a veteran in my district, say their Social Security number was accessed, are any of those Social Security numbers redacted or is this just free-flowing raw data that's going out the door?

Mr. BOWMAN. Well, we don't have knowledge of any specific cases of data loss, other than the 2006 example, and in those cases VA is responsible for providing credit reporting services to the veterans who may have been harmed by this. But what we try to indicate, is that using unencrypted protocols, the risks remain, that the potential is there, and that VA needs to implement these proactive controls so these type of events do not occur going forward.

Mrs. WALORSKI. But in light of the answers to the various questions up here, there obviously has been more than just one incident

in 2006 when that information has been available. And so, you know, I think about this in my district. I have 52,000 veterans in my district and then their extended families, and I'm thinking, you know, if this happened in the private sector, automatically this would have triggered—just the suspicion and the not knowing would have triggered an automatic credit freeze to the people that would be living in my district.

So I'm looking at this from the standpoint of saying, you know, sending out an APB when I get out of here that says to the 52,000 vets in my district, better check your credit report because we have no idea that your information has not been breached, and to continually check that. And as we continue to tell people to go access their VSOs and go access their facilities because there's a long wait and the things we deal with on the veteran side, is how at risk they are with sharing that information in today's day with these violations.

In the private sector, this type of an entity would never survive. The lawsuits that would come would shut them down because of private information being at risk and being taken and nobody responsible. So it is absolutely baffling to me that in addition to some of the other things that we have heard in this report, that the buck stops with the CIO, and we have had nothing but turnover, as you've reported, in this entity of this area of the VA to begin with. Has anybody ever been disciplined based upon the findings of your reports?

Ms. HALLIDAY. We can only make a recommendation. It is up to the Department to take the administrative action. That's the extent of our authority.

Mrs. WALORSKI. Have any of your recommendations involved issues of employees or incompetence or training or things actually for the people who are actually working there taking this information?

Ms. HALLIDAY. Yes, I would say several, especially with our administrative investigations. It's looking at very specific personal accountability for actions.

Mrs. WALORSKI. And are you asking specifically that supervisors and managers and CIOs and these kind of people that have been in charge, where the buck stops with this information, that they be disciplined, if not terminated?

Ms. HALLIDAY. We make a recommendation for appropriate administrative action and then generally give a discussion with that—

Mrs. WALORSKI. And is the appropriate action usually termination? I'm not familiar with the protocol. What is the appropriate action on something like this large of a risk to this many people?

Ms. HALLIDAY. You would have to look at the severity of the incident, determine the exposure, determine what the accountability was. Was there intent? Was this a mistake that they may not have been able to prevent? And then when you do that, you apply the Douglas factors for discipline actions in the Federal Government?

Mrs. WALORSKI. But my understanding would be, in the last 10 years, based upon the previous questioning, that the 40 or so outstanding compliance issues that you have advocated that they follow, had those been followed in the last couple of years, we would

have remedied this situation. So there has to be some kind of accountability still, and disciplinary actions, and the buck stops someplace with this staff, correct?

Ms. HALLIDAY. We absolutely think the Department should have implemented many of the FISMA recommendations and tightened controls early, and they would have less security incidents.

Mrs. WALORSKI. Thank you.

Thank you, Mr. Chairman. I yield back.

Mr. COFFMAN. Thank you, panel. I appreciate your testimony. You are now excused.

I now invite the second panel to the witness table.

On this panel, we will hear from Mr. Stephen Warren, Acting Assistant Secretary for Information and Technology at the Department of Veterans Affairs. Accompanying Mr. Warren is Mr. Stan Lowe, Deputy Assistant Secretary for Information Security from the Office of Information and Technology at the Department of Veterans Affairs.

Before I recognize the panel, I ask that you please rise and raise your right hand.

[Witness sworn.]

Mr. COFFMAN. You may be seated.

Mr. Warren, you are now recognized for 5 minutes.

TESTIMONY OF STEPHEN W. WARREN, ACTING ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS, ACCOMPANIED BY STAN LOWE, DEPUTY ASSISTANT SECRETARY FOR INFORMATION SECURITY, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS

Mr. WARREN. Chairman Coffman, Ranking Member Kirkpatrick, Members of the Subcommittee, thank you for inviting me to testify regarding the Department of Veterans Affairs Information Technology Security Program. Accompanying me today is Mr. Stanley Lowe, Deputy Assistant Secretary for Information Security.

There is no higher priority than protecting the data that VA holds on our Nation's veterans. I, as well as the many IT employees at VA—over 56 percent are veterans themselves—take this responsibility very seriously.

As the Committee knows, the Department received a wake-up call from the stolen laptop incident in 2006. As a result, the VA consolidated its disparate IT functions into a single, unified IT organization. VA's consolidated IT organization is responsible for providing the tools, services, and systems that are necessary to protect veterans' information at 153 hospitals, 853 community-based outpatient clinics, 57 benefit processing offices, and over 160 cemeteries or memorial cites. Our network supports over 400,000 users and over 750,000 individual devices. We are committed to protecting the information we hold on millions of veterans, their beneficiaries, and more than 300,000 VA employees.

As we all know, IT security threats continue to evolve. To that end, we have implemented our continuous monitoring program, which continuously checks all IT systems and monitors every device attached to the VA network. VA launched the Continuous Readiness in Information Security Program, or CRISP, in 2012 to

proactively address process and policy deficiencies, as well as architecture and configuration issues.

As part of the CRISP effort, the VA conducts rigorous vulnerability scanning, continuous monitoring of patching and software inventory, implementing port security, anti-virus services, and encryption of nonmedical IT desktops and laptops.

Through Web Application Security Assessments, VA is able to identify critical vulnerabilities and potential exploits in VA systems. We protect the network infrastructure by identifying all network assets, critical database stores, all external connections, and provide the Trusted Internet Connection Gateways services.

In the past year, VA has measurably improved its security. The Department has ensured that over 98 percent of VA staff have received the mandatory security training they need to protect the information of veterans and their families. Only staff turnover prevents us from reaching 100 percent.

After the 2006 incident, VA worked to ensure its laptop computers were encrypted to provide another layer of protection. Currently, over 98 percent of VA's nonmedical IT laptops are encrypted. The Department aims to complete the encryption of the final 2 percent by June 30.

VA has a robust data breach notification process using a Data Breach Core Team. When the team determines that a potential breach may have occurred, they notify affected individuals and offer credit monitoring. VA also posts a monthly report of data breach notification on its Web site, and this report is provided to Congress, in addition to the required quarterly data breach report.

VA has become one of the very best large organizations of providing notification if a potential breach occurred. This law requires notification within 60 days. A review of VA's incident tracking system over the current fiscal year indicates that VA takes, on average, 25 days to provide notice. VA's standards and practices exceed even the strictest Federal, State laws and policies.

I would like to update you on our progress to extend VA's authority to operate, or ATOs. Before giving you this update, I would like to assure the Committee in the strongest terms that at no time was veterans' data placed at risk by this process. The signing of an ATO represents the final step in what is otherwise a continual process of security and management reviews.

As the Committee is aware, VA has been working to extend nearly 600 ATOs over the last several months. We have worked to assure that requirements for each ATO are properly conducted and documented. VA trusts the ATO validation process and the work of the information security officers, facility CIOs, and system owners to ensure system security. This paper-based process validates that critical steps are being taken to protect our veterans' data.

Mr. Chairman, VA places the highest priority on safeguarding veterans' and employees' personnel information. We are committed to information security. And although work remains, VA has made significant improvements in the last few years and strives to meet those highest standards in protecting our Nation's veterans' sensitive information.

Thank you for your continued support of veterans, their families, and our efforts to protect veterans and their information. I am pre-

pared to answer any questions by the Ranking Member, the Chairman, or the Members.

[THE PREPARED STATEMENT OF STEPHEN W. WARREN APPEARS IN THE APPENDIX]

Mr. COFFMAN. Mr. Warren, given your knowledge of visitors in the network since 2010, and understanding that there were significant security weaknesses, why would you insist on conveying the message that veteran data is not at risk?

Mr. WARREN. Thank you, Chairman. I think that that actually is a great question to ask within the construct of information protection.

I think it's very important to note that my partners in the Inspector General's Office used words such as could, might, potential, possible, is possible. When an audit takes place, when a review takes place, the focus is on what could happen. But remember, the existence of a risk is not the same as the removal of information out of the network.

Several things need to exist. What needs to exist is the potential, and we try to drive those down as quick as we can. There needs to be an actor who has access and the ability to get to where that risk is. They need to be able to do that in such a way that they are not seen, and then they need to be able to move the information out of the network through all the sensors and past the gateway, as well as past our partners in DHS who are watching outside our gateway, and then remove it. So the piece we need to be very careful of is, we're talking about potentials, we're not talking about actuals. And so the—

Mr. COFFMAN. I'm sorry. How do you define the difference between an actual and a potential? And I'm looking at an internal report on August 15, 2012, and it talks about an actual—at least it talks about that the network was penetrated. So how do you define actual versus potential?

Mr. WARREN. Sir, I don't have that report in front of me.

Mr. COFFMAN. Well, I'll make it available to you.

Mr. WARREN. And I will gladly respond to the record, sir, in terms of that specific incident.

Mr. COFFMAN. Sure. Okay.

Mr. COFFMAN. Please define the difference between actual and potential.

Mr. WARREN. Potential is—and we'll do as an example your home computer. So if you do not update your—

Mr. COFFMAN. How about we just stick with the VA system. Let's talk about that.

Mr. WARREN. Sure. We can talk about a desktop computer. Once a month Microsoft puts out a set of patches on Tuesdays. So every Tuesday, once a month, the first Tuesday Microsoft sends out a full set of patches. If we do not incorporate those patches into the system, the potential for somebody going to a Web site and the potential being exploited goes up. But the VA has a very aggressive program to make sure those desktop patches happen once a month as Microsoft puts it out. So if you don't do them and you don't do it over multiple months, the potential for the desktop to be compromised and the system itself to be compromised goes up.

Mr. COFFMAN. It's my understanding you have not instituted all the patches in the VA system. Is that correct?

Mr. WARREN. I'm sorry, I missed the first part.

Mr. COFFMAN. That you have not instituted all of the patches prescribed for the VA system.

Mr. WARREN. I would tell you, Mr. Chairman, that we have a very aggressive program to make sure the desktop computers are patched.

Mr. COFFMAN. You're not answering my question.

Mr. WARREN. The intent is not—

Mr. COFFMAN. To the VA system. Is it true that not all the patches have been applied as prescribed in the VA system? In the information network.

Mr. WARREN. Sir, there are about 750,000 devices in the network. So if you're asking does every single one of those devices have every single one of the patches that their manufacturers put out, the answer would be no because there are multiple times when that patch will actually break the application that you need to use, and therefore there is a waiver in place that says you don't patch that system because not working is actually worse than a potential risk within an environment which is—

Mr. COFFMAN. Mr. Warren, why did you not previously disclose to the Committee that VA has had serious and continuous compromises of systems and data by nation-state sponsored actors?

Mr. WARREN. With all due respect, I do not believe it is a true statement, as you laid it out, that the VA has been continually compromised by foreign nation states. We have a strong partnership with Homeland Security, which watches the boundary for the Department.

Mr. COFFMAN. Mr. Warren, has a foreign entity targeted and penetrated our network?

Mr. WARREN. I am aware of a single incident that our network operation center identified.

Mr. COFFMAN. And when was that?

Mr. WARREN. It was last year. I will need to get back for the record in terms of the specific date.

Mr. COFFMAN. Very well. And I will make this internal document available to you. And I think you can be informed that there actually have been quite a few breaches.

Ranking Member Kirkpatrick.

Mrs. KIRKPATRICK. Thank you, Mr. Chairman. I'd like to follow that line of questioning.

Mr. Warren, if a system is compromised, would you know? Or is it possible for it to be compromised and you to not know?

Mr. WARREN. I would tell you, with the controls that we emplace, with continuous monitoring, as well as the work that we do at our boundaries with Homeland Security and our NSOC, the probability of somebody being in the network and compromising a system without us knowing it is very, very low. But I can't argue the absolute.

Mrs. KIRKPATRICK. Can you provide for the Committee how many times the system has been hacked since the beginning of this year?

Mr. WARREN. I will gladly provide that for the record.

Mrs. KIRKPATRICK. Thank you. Was it your testimony that it takes you 25 days to notify the veteran that their personal information may have been compromised?

Mr. WARREN. Yes, ma'am. If I could expand on that.

Mrs. KIRKPATRICK. Would you expand on that, because that really concerns me. In 25 days everything could be wiped out for that person.

Mr. WARREN. Certainly, ma'am. What happens is as soon as—and VA has a 1-hour reporting requirement—as soon as an employee believes the potential of something happening, they're supposed to notify our NSOC, and it is part of the reporting we do. At that point, we pull the team together and we ask the question: What and why? Is it real? And if it turns out we have an issue, the Data Breach Team—which meets once a week, which is made up of career staff who are outside the chain of command—they do the analysis of that potential breach and they determine if the potential was high enough that data had left. And normally, if there is just a little potential, the Department goes ahead and reaches out to all of those veterans with credit monitoring for a year. And the 25-day period is the time for the notification to the NSOC, the establishment of the team, the analysis of the data to make sure what was reported was actual. And in many cases—in fact, in most cases—it's the potential that is reported, and we reach out to veterans anyway and we offer that credit reporting.

Mrs. KIRKPATRICK. How many times have you had to notify veterans within the last year?

Mr. WARREN. Ma'am, I will get you that for the record in terms of the number of times that we notified veterans and offered credit reporting as a result of a potential data breach.

Mrs. KIRKPATRICK. Thank you. And was it also your testimony that by June 30 of this year your system will be encrypted?

Mr. WARREN. Actually, my testimony, ma'am, was that for all nonmedical IT laptops. So the ones that are under my responsibility, we will have the last of those encrypted.

Mrs. KIRKPATRICK. But the medical laptops will not be encrypted?

Mr. WARREN. No, ma'am. And, Ranking Member, the difficulty we have with medical devices is they're constrained by their certification from the FDA. And the concern is by putting encryption on that laptop, a medical device that has a laptop in it, you will actually impede the ability of that medical device to do its job.

And so we've had lots of conversations with the FDA to figure out how you can do that. But when a device is certified that has a medical device in it, the condition of the device at the time of certification constrains what you can do afterwards. And so to handle that, we actually have a separate area, an isolated area in the VA network where we put those medical devices that are based on IT equipment. And we also go further by working with our partners in VHA where we start testing those devices to see if there is an impact to its job in terms of delivering care, or if we impact their certification boundary. And in cases where it isn't—and there is a tool called bar-code medication, which is what the nurses move through the wards—we are able to show that there was no impact, those medical device laptops are now encrypted. And so we work

our way through that with our partners in the health administration and the biomed folks.

Mrs. KIRKPATRICK. I have one last question. Are you familiar with or have you heard the Inspector General talk about the fact there has been excessive turnover in key leadership positions and there's a lack of human resources in the IT departments? Do you agree with that statement?

Mr. WARREN. I would tell you that an organization going through transformation is a difficult place to work because everything is moving around you. And so we have had transition of staff. We've had transition of staff going out and coming in. This year, I believe I am 100 folks below my ceiling of about 8,500 individuals.

Mrs. KIRKPATRICK. Do you have a strategy to address that so you have adequate human resources?

Mr. WARREN. We do active recruiting. We work with the HR organization to figure out how do I do pools so I can make sure I've got project managers lined up, to make sure I have individuals lined up to bring them in.

We also have a very strong focus on veterans. As an example, last year, 75 percent of my new hires were veterans, because that's very important to me, as a veteran, to make sure we're bringing our clients, if you will, into the organization to help us do a better job.

Mrs. KIRKPATRICK. Thank you, Mr. Warren. I yield back.

Mr. COFFMAN. Mr. Warren, please be reminded that during the course of this oversight hearing and Committee investigation, it is a Federal crime, pursuant to 18 United States Code section 1001, in pertinent part, knowingly and willfully to falsify, conceal, or cover up a material fact, or to make any materially false, fictitious or fraudulent statement.

Mr. Lamborn, you have 5 minutes.

Mr. LAMBORN. Thank you, Mr. Chairman.

Mr. Warren, members of the previous panel testified under oath that foreign state actors have accessed sensitive information of veterans within the last 2 years and that the VA does not know how much information was stolen. Would you agree with that statement?

Mr. WARREN. I would say, Congressman Lamborn, there is that potential. I would tell you that, working with our partners at Homeland Security in terms of where they watch our gateway—so it's not just the VA connected to the world and everything happens, we have Homeland Security, if you will, at the gate. So I have our team on our side and Homeland Security on the other side. And between the two of us, we watch all the traffic going back and forth.

So the ability of material to move, yes, there is always a potential. We referred to a particular incident that the Inspector General talked about. I was aware of that incident. So I would tell you that one, we know happened. With the other ones, it's still the potential and the probable, in terms of—

Mr. LAMBORN. And of the one that you will admit has happened, we don't know how much information was taken because it was encrypted before being exported. Isn't that correct? So we don't know how little or how much the data was that was stolen?

Mr. WARREN. Sir, my recollection of that report—and what I'd like to do is go back and review that report to give you the answer in terms of what came out and what the report was able to tell us given the conditions that existed.

Mr. LAMBORN. What kind of dependent information is put into some veterans' files?

Mr. WARREN. I would tell you, Congressman Lamborn, the veteran files are held in many locations in the VA, in many systems, whether in the electronic health record or whether in the new—used as part of the new VBMS system, as well as all the other systems. So the information necessary to provide benefits or services is what we—

Mr. LAMBORN. So it can include the names and Social Security numbers of dependents.

Mr. WARREN. If that's required as part of the claim or service process, sir.

Mr. LAMBORN. Another problem I have is—and this happened to me recently. I got a credit card in the mail. It turns out that my credit card issuer had been compromised, so everyone had to get a new credit card. And we had to go back and change the numbers on all our accounts. It was a big hassle. Fortunately, nothing was stolen that I know of. But what happens when a Social Security number is stolen? You can't replace that. I mean, we're talking about something really serious here. Are you aware of how serious this is?

Mr. WARREN. Congressman Lamborn, we take any potential incident and any incident very seriously. I take it personally. It's one of the reasons why the VA offers credit monitoring. So even when there is a potential, we reach out to the veteran and we offer them that credit monitoring for a year. We also have a 1-800 number that we've made available to veterans if they have any questions so that they can reach out to us if by chance something does happen, so we can help them, walk them through that process.

Mr. LAMBORN. You said earlier that we place the highest priority on protecting this information, and yet members of the OIG indicated that for more than 10 consecutive years, independent public accounting firms under contract with OIG have identified information technology security controls in the VA as a material weakness. How can that condition have persisted for 10 years if that's your highest priority?

Mr. WARREN. Congressman Lamborn, thank you for that question. I would tell you that material weakness is actually a financial term. It's the same type of term used as part of Sarbanes-Oxley in terms of laying those financial controls on the organization. So the material weakness says there is a question about whether the financial data in the system is secure or not.

So material weakness, yes. I will tell you that, as an organization, the Department wasn't going, we've got a material weakness, move on. Every year we took the inputs—and I've only been with the VA for 7 of those 10 years—every year I've been there we took those inputs and we laid out what we needed to do. We laid the resources on it. We put focus on training. And I will tell you it wasn't enough. And so 2 years ago, this major effort of doing CRISP, of taking the whole organization—not just the IT organiza-

tion, but taking the whole organization, because information protection is not just an IT thing.

Mr. LAMBORN. Well, I'll agree with one thing you've just said when you said it wasn't enough. I certainly agree with that.

And how do we know that there isn't going to be some kind of document dump by a foreign actor, you know, WikiLeaks or something like that? I mean, there are so many things—health care records. There is such sensitive information in health care records. So we're not just talking about Social Security numbers, there's health care records. We shouldn't be here today, and I am sad that we are at this juncture right now.

Mr. Chairman, I yield back.

Mr. COFFMAN. Thank you, Mr. Lamborn.

Mr. O'Rourke.

Mr. O'ROURKE. Thank you, Mr. Chairman.

For Mr. Warren, I'm not as conversant in the details of these issues and the different systems and protocols involved as I would like to be, but I think it's fair to say that the picture you paint of the VA's IT system and the vulnerabilities is very different than the one that we just heard from, from Ms. Halliday. And I think you heard many of us say that what we heard presented was unacceptable in terms of the vulnerabilities, unacceptable in terms of the amount of time that the VA has known about those vulnerabilities without successfully addressing them, some concerns about when information was reported to this Committee and others in terms of breaches to the system and retrieval of information by foreign actors.

Can you just, so in general terms that I can understand, address that discrepancy from what we just heard to what you're presenting? You seem to be saying that things are generally under control.

Mr. WARREN. I would tell you the state of security and the work we need to do is something that I wrestle with all the time. Am I satisfied with where we are? No, I'm not. Can we do better in terms of fixing the things that our partners in the IG and the audit community have identified? Yes. And we are dedicated to doing that.

But the difference that you are hearing from myself versus the audit community is, they have to deal with potential: Is there a chance? Is there any opportunity for something like that to happen? And the answer will always be yes. It will always be yes, that there is a potential. So if you ever ask me, or even if you ask me today, can I guarantee that everything is perfect and wonderful? I could not give you that guarantee because it's constantly changing, the technology constantly changes.

So my focus is more of a very pragmatic operational person whose job is to try and make sure we continue to deliver those benefits and services in a way that has the least risk, the one that does not put our veterans' information at risk while we do that. And again, is it where I want it to be? No. Do we continue to drive on getting it to where we need to be? Yes.

Mr. O'ROURKE. In terms of the 32 recommended steps that need to be implemented—and I asked the IG's Office about what the

timeframe would be to implement those—do you agree that it's a 12-to-18-month implementation timeframe?

Mr. WARREN. Yes, sir. And in fact, when the report gets published, you will find there is a departmental response. And it actually lays out what it is that we have in place and what we are going to do. And I believe the latest date I have when I signed out that document with all the different organizations was September 2014 for some of the longer items. And I believe that fits within that 12-to-18-month period.

But there are many things that are happening now. We have some significant things coming online at the end of August. There are things taking place between now and August. But the longer, harder ones take that extra time to get there.

Mr. O'ROURKE. And so there are no fundamental differences between your office and the IG's report in terms of what they just described to us in their findings, their vulnerabilities, and the seriousness of those vulnerabilities and threats?

Mr. WARREN. I will tell you, there were many reports referred to in the prior panel. You will find that if you look at the report and you look in the appendix, the place where the Department did not agree with the findings, you will find a statement in there that says—again, we always thank our partners to come in. We see them as part of the team. They give us that outside view. But where we disagreed with what their observations were, we normally state that in the document.

So, given the Chairman's reminder, I need to make sure that where the Department did not agree, we stated in the report. And we also state what it is we're doing as a result of what they find and what our plan of actions are. And then we give a quarterly update to all of the things that we said we are going to do. And as the Acting Assistant Secretary, I sign off on every one of those quarterly reports in terms of what we said we were going to do, what did we do to ensure that we are responsive not only to what the Inspector General identified, but ensuring that we're doing everything we need to do to protect our veterans data.

Mr. O'ROURKE. Let me ask one more question. You've used the terms "possible," "probable" and "actual" several times in response to our questions. A question I asked of the previous panel, can you tell us of an actual incident where, because of a security vulnerability, private information from a veteran was retrieved by someone to negatively impact that veteran, whether they stole their Social Security number or other personal data that was then used to harm that veteran?

Mr. WARREN. I am aware of several incidents, and I will describe one for you. It's an individual who accessed—he was a system administrator—again, not foreign, but domestic—accessed the database and used the information to do identity theft. When identified, we refer those to the IG and they bring in criminal investigations. So, in that regard, there was an individual who breached the system. It is always referred to law enforcement. It is always referred to law enforcement. And then we provide credit monitoring, and we also work with the law enforcement folks to make sure that they have full access to do what they need to do.

So I will tell you, large organization, lots of people, there are going to be folks who do bad things. As we find them, we refer them to law enforcement for them to take action. And then we just keep, as a result of what we saw—what then do we do, right; how did that person get in there. So you will see there is a very strong personal accountability program the Department is bringing onboard to go ask the question, are we hiring the right people? Do they have the right credentials? Are there flags here on their personnel records such that we really shouldn't be putting them into a position of trust—not an IT thing, but the broader aspect of how you hire folks and how you make sure you're bringing in the right folks.

Mr. O'ROURKE. Thank you.

Thank you, Mr. Chairman.

Mr. COFFMAN. Just real quick. When the OIG, in their report, said that your system got hacked by foreign actors, do you refute that as part of your response?

Mr. WARREN. So, again, I believe you're referring to that August report. Let me just make sure what you're referring to, Mr. Chairman, if I can. I don't have enough information to answer your question, sir.

Mr. COFFMAN. So you're not aware—in the OIG report, in their testimony, when they were up here, they referenced that your system got hacked by foreign actors. First of all, do you acknowledge that?

Mr. WARREN. I believe I already have in my testimony, Mr. Chairman.

Mr. COFFMAN. Yes or no?

Mr. WARREN. Yes.

Mr. COFFMAN. Very well.

Dr. Poe for 5 minutes.

Mr. ROE. Thank you, Mr. Chairman.

And a couple of questions that Congressman Lamborn talked about.

One of the reasons that, the way I understand this from listening this afternoon, that you might not know what information is going out is that the information that people were after was not encrypted. But on the way out the door it was encrypted, so you couldn't read what was gone. So you could truthfully sit there and say we don't know what's been stolen because you really don't know. And it should just have been the other way around; we should have had the data encrypted so that nobody could have gotten a hold of it or done anything with it. Am I right or wrong with that? Did I misunderstand?

Mr. WARREN. No, Congressman Roe, you are actually laying it out appropriately. And again, with the report that we're referring to, glad to do a private briefing to the Committee with the details because of some of the issues around it.

I will tell you that the area where the individuals were, were in the email area, in terms of pulling emails out. The one compensating controller, the thing we do as well, is many of our emails are encrypted. So the reference to unencrypted is information in databases. This particular information—which I believe has been referred to—deals with folks who went after email packages. In

many cases, those are encrypted such that it would be difficult to read them. But again, because, as you rightfully pointed out, the data left the network encrypted, it's hard to say yes or no what it was.

Mr. ROE. I understand that now. And let me ask, would any of this other information, since you-- do you cover the part of the VA involved in contracting? Is that data—not just personal information, but is contract data? In other words, if I'm bidding on a project out here, would a foreign competitor know what that contract was? Because we certainly have seen that in other areas. Is that possible?

Mr. WARREN. Sir, I can't refute the possible of any scenario in terms, again, there are no absolutes in information security. We strive to make sure there aren't any—

Mr. ROE. Let me stop you. I've heard that before. This August 15th, there is an Office of Information Security, and you stated you heard—at least were known of one time that—I think that I understood this—that you had been hacked or pinged. March 10th and onward the DeepDive Analysis has been tracking activities of well-funded cyber-espionage teams that regularly target VA. Over the past 31 months, the DDA—that's the Direct Dive Analysis—has identified eight of these teams as part of our threat program. Each team is assigned a name—I won't go through that. Assigning a common nomenclature has allowed them to contribute each of their campaigns and see which one of them is the most effective. And it goes through how they were doing it. I'm sure you're aware of that.

Mr. WARREN. Yes, sir. The key reporting and the fusion technology team—so the individual whose report you're reading from—is an initiative that I started in terms of asking folks to go out and start pulling data and understand what was going on. What I think what you will see—

Mr. ROE. Help clear me up because you said you only heard of one—you only knew of one incident, and yet you started this, which there are eight different teams that are looking. And it appears from this information we have—which it makes sense that they most like to hack us during holiday times, which makes sense, your defenses are down, Thanksgiving, Christmas, those times when we would be less—our defenses are up less.

Mr. WARREN. I think what you'll find, sir, if you read into that report, it's targeting. So the report, again, it's a very aggressive defensive policy in terms of through our network security folks is trying to identify where the threats are. Now, again, the August report we talked about, the specific instance where we saw the material leaving and some of the things that we did as a result of that, you will find there are reports like that that are published probably a couple times a month from the fusion team saying this is what we're tracking, this is what we're monitoring, this is what we're doing about it.

Mr. ROE. But you wouldn't be tracking those if they weren't active.

Mr. WARREN. Sir, there are things known as honey pots, black holes, where the individual may try to come in. And what you do is you set up your perimeter so it looks like they're actually getting

into data, but they're not. You're actually tracking and capturing them.

The other piece, if I could, is there are actors you see inside, but you also set it up on the outside, where if they are trying to send data out, you basically put a trash can where the data goes versus leaving the Department.

Mr. ROE. I have some more questions on that to see how many times that has happened. There is a note here I have that says over 400,000 systems in VA's network do not even have a basic security baseline installed. Is that correct or incorrect?

Mr. WARREN. Sir, I would need to basically validate where that report is coming from, and I will take that for the record.

Mr. ROE. And lastly, just one quick question: Who are the state-sponsored actors that we're dealing with? You haven't called any names, but who are they?

Mr. WARREN. I would tell you, sir, that my preference is to do that in a closed session; otherwise I would put my clearance at risk, as well as the fines and penalties.

Mr. ROE. That's fine. That's fine. I yield back.

Mr. COFFMAN. Mr. Walz for 5 minutes, please.

Mr. WALZ. Thank you, Chairman.

Thank you, Mr. Warren.

Your data is on those computers too, correct, as a veteran?

Mr. WARREN. Yes, it is, sir.

Mr. WALZ. Okay. And you were over at FTC and DOE?

Mr. WARREN. Yes, sir. I was at the Federal Trade Commission, where I did the national Do Not Call Registry, something I'm very proud of, as well as annual credit monitoring that you can get, and then at the Department of Energy with the Weapons Clean Up Program.

Mr. WALZ. How does your knowledge over there—does the current job you're in correspond with you having a knowledge of those organizations and their ability to provide security over data? Because I'm assuming both of those have very sensitive data, especially DOE, in terms of state secrets and things like that. So is there a comparison there? Can you tell us how they function or how VA's system is in terms of robustness compared to those?

Mr. WARREN. I would tell you, sir, we are all facing the same threats. And we all put the protections in place and we work with each other. In fact, we have a very aggressive outreach program with the folks in the other organization. And there is also a larger effort through the Federal CIO Council to learn from each other and use our best practices because we are all facing that threat today.

Mr. WALZ. I agree. And this is what I'm trying to get at. And I think the gentlewoman from Indiana brought up a good point. States are trying to tackle this as they go. And I'm looking through, there's a Privacy Rights Organization Clearinghouse that, as we speak, in realtime is listing this: Health Information Trust of Frisco, Texas, 111 record compromised. A dentist in Rochester, New York, on June 3, theft of a laptop, 13,806 records.

One, though, that comes in here—and I think it brings to the point of what we're trying to get at—is Hampton Roads Health System, Newport News, Virginia, talked about employees accessing

information incorrectly. And it even notes in this that they were fired for that. And then of course there's malicious content and all that.

The point I'm trying to figure out here is, when you do this, is data security an all-or-nothing, zero-sum proposition? Is it an impenetrable firewall, or it's open access, or are decisions made in the business community as well as you that risk assessment and what is acceptable risk is in that?

I'm assuming in the private sector now—and listening to Ms. Walorski brought up a very good point—is there is a huge market in identity theft insurance, data breach insurance on that. Those insurance underwriters must be drawing some guidelines on what is acceptable risk and what is not. Does that pertain to what you're doing? Is the VA doing that very same risk analysis based on best practices of those underwriters?

Mr. WARREN. Yes, sir. We apply those same rules. It is baked into the standards that we follow. The National Institute of Standards and Trust applies those to us.

And to your question about, is there an all or nothing? I think our partners at DoD found out with WikiLeaks, in a secure system, you still could not guarantee the material would not—

Mr. WALZ. Well, what I guess I'm asking for is, is it worth—and I'm going to come to this question is: What's the cost, have you figured, to implement OIG's recommendations? Is there a cost factor that takes into this? Say, for example, depending on where I'm at, versus a high crime versus a low crime neighborhood, I might not invest in the most robust security system, taking and thinking into—there hasn't been a crime in my neighborhood in 75 years. Those are things that we work in. Now, if I always want to be absolutely sure, I could go to the top of the line every time and implement that security. How do you view that at VA when you make those decisions?

Mr. WARREN. Sir, great question. Thank you for that question. We look at what the risk is. Is it something at the perimeter or is it something inside? Is the data inside something that has the highest level of need or something that is just transactional data? And the amount of resources we apply and the controls we put in place are actually tailored to the information that's in the system and the potential risk.

Mr. WALZ. Does OIG take that into consideration when they put out their recommendations, that you are doing—what you're telling me is, you are doing a risk analysis, a cost-benefit analysis. Is OIG asking or saying this is the ultimate perfect world, what it looks like in security? Are they factoring that in?

Mr. WARREN. I believe my partners in the Inspector General Office are taking that into consideration. But I will tell you they've done a fair appraisal, in terms of the FISMA audit, of areas where we need to continue our attention and focus. And I will tell you the one thing that tells me that we're on the right path is we did this massive program last year called CRISP, which was more than just IT, it was the leadership of the organization—the VHAs, the VBAs, the NCAs. So they got engaged from the senior levels of what do we need to secure the enterprise. And we are seeing the critical

things dealing with personal attitude by non-IT folks as well as IT folks is changing to where it needs to be.

Mr. WALZ. Well, if I heard that right, OIG did say they didn't give an assessment based on it hasn't run its whole course yet. So what your assessment is, is at the end of this, when you go back and look at what CRISP did, we're going to see a change across the spectrum, culturally and robustness of security.

Mr. WARREN. Yes, sir. We are seeing that change. And I will tell you the change will need to continue from here on out because we know that threat evolves with our change.

Mr. WALZ. I'm going to use my last 25 seconds here. You're not going to get the opportunity to do this, but following you, Mr. Davis is going to speak and there's going to be some questions of how things came out or why they came out. Is there anything you'd like to address? I'm out of time here. You know the situation, the memorandum and how things are going to play out, and I think it's only fair that you be able to respond.

Mr. WARREN. I would tell you, sir, I was perplexed by what happened and how it went down. I was troubled by the fact that there are two memos in circulation, a memo dated 29 January that I and leadership received, and the one that we received from the Committee that was signed on the 28th of January that we were not aware of the existence of it until Friday, when the Committee staff gave it to us. And the memos are almost identical except for one paragraph, and that paragraph says: "Clear and present danger."

I will tell you, if anyone tells me there's a clear and present danger, I pick them up and I walk them over to the IG and say, tell them what it is that I am missing here. I actually did that on the 29th with the memo received. That memo I took to the IG.

On Friday, when I learned of the existence of a second memo different than the one the Department received, I took both of those memos and I reached to the IG and said, I need you to help me figure this out because I cannot figure out why the Department would get one memo with four paragraphs and the Committee would get a different memo with five paragraphs and the difference is "clear and present danger." That was not communicated in the memo we received. And I'll tell you, I am still perplexed on why that would exist.

Mr. WALZ. Mr. Chairman, I thank you for indulging the extra time.

Mr. COFFMAN. Ms. Walorski for 5 minutes.

Mrs. WALORSKI. Thank you, Mr. Chairman.

Mr. Warren, can you guarantee that the veterans in my district, in Indiana's Second District, have not suffered a security breach?

Mr. WARREN. Ma'am, I'd be lying to you if I made that guarantee. Again, it is all about what the risks are. And we try our darnedest—in fact, we do more than try our darnedest.

Mrs. WALORSKI. But you can't guarantee that.

Mr. WARREN. I can't—and in fact, nobody—if someone sat here and guaranteed, you should haul them out of here—

Mrs. WALORSKI. All right. Do you personally, sir, do you personally feel responsible for the fact that we have a Nation of veterans that are vulnerable?

Mr. WARREN. I care deeply that we are not further—

Mrs. WALORSKI. Do you feel personally responsible, when you leave and check out at night and go home, do you feel responsible for the fact that there are various security breaches and our whole Nation's veterans are at risk?

Mr. WARREN. Ma'am, I go home tired every night for all the things that I do.

Mrs. WALORSKI. Do you feel responsible for all the things that we talked about here today?

Mr. WARREN. Ma'am, I'm personally responsible for the organization as the Acting CIO.

Mrs. WALORSKI. Thank you.

I yield back my time to Dr. Roe.

Mr. ROE. Just a couple of questions, and maybe I got to this before. But are the state actors, is that classified information? Because I've seen published reports. I mean, we've just had the Chinese in every headline in the world here saying, oh, it's not a big deal, it's not a big. We know it's a big deal. So who are the state actors?

Mr. WARREN. Sir, as a young lieutenant, one of the first briefings I got when I came onboard was that just because something is published in the press, if you receive a briefing that says it's classified, until the classifying authority says it's clear, it's classified no matter what you read.

Mr. ROE. The briefings you've had, I mean, what you've got done right here, when you determine with what you're doing that somebody is trying to breach your firewalls and get into data that's in the VA system, that's classified information, you can't come here to this Committee and say, this is what happened?

Mr. WARREN. Sir, actually, you had asked me a different question, which was the naming of the actors. We work with Homeland Security on our boundary, so they are in constant communication with us. They are telling us when they see stuff. We are telling them when we see stuff.

Mr. ROE. We want you to tell us when you see stuff. What's the problem with that? I thought that we all work for the American people.

Mr. WARREN. As do I, sir.

Mr. ROE. Well, I include you. I said we all. You, me, everybody in this room who's here who's a public servant works for the American people. They have a right to know who's trying to get into their personal information. I would like to know who's trying to get into the veterans that I serve, the 70-something thousand of them that live in northeast Tennessee.

Mr. WARREN. Congressman Roe, we would be glad to come up and give you that private briefing with all of the material you would like.

Mr. ROE. I guess my question is—second question is—why is that classified? Why wouldn't that be public? When people are trying to steal from you, we ought to let the people in our country know who's trying to steal our own veterans' information, I think. I think that's very important to be public. Why are we hiding that? And that's above where you are, I understand that. But that's a philosophical question.

The next question is, is that, when we come back a year from now—I've been here now 4-1/2 years, and I see problems that linger on and on and on. Are we going to come back 1 year from now and have the same conversation? And I totally agree with you, Mr. Warren, when you were saying you couldn't absolutely guarantee. I've had people come to me when I'm taking them to the operating room and say, will you guarantee that I'm going to live through the surgery? Well, I can't guarantee that. I got that. I understand that. But with as good a system, can we say a year from now that the IG, in fact, who gave a very good report, you will have met those metrics that you agree with, and then you all work out if you don't agree with them?

Mr. WARREN. Sir, I would like to take the 12 to 18 months the IG identified. But the intent is to clear as many of those as we can in the 12 months with the schedule we've given them, and to keep moving through those until we've cleared them all.

Mr. ROE. I yield back.

Mr. COFFMAN. Thank you, Mr. Chairman.

Mr. Huelskamp.

Mr. HUELSKAMP. Thank you, Mr. Chairman.

Mr. Warren, the IG's testimony outlined some pretty serious deficiencies in the Office of Information and Technology. And according to the evidence, VA's network has been accessed by foreign state actors since March 2010. And in that fiscal year, and since then, you've received a grand total of more than $87,000 in bonuses. Can you explain how you merit such a large amount in bonuses?

Mr. WARREN. Sir, as you're aware, the way the compensation system works in the Federal Government is a performance plan is laid on an employee, as in myself. A supervisor sits down and lays out what I expect from you in the year. And based upon how you do, there is an appraisal given.

Mr. HUELSKAMP. So how you did was worthy of $87,000 in bonuses? Is that your understanding?

Mr. WARREN. I believe, as a result of me exceeding the performance expectations that my leadership have laid on me, I was recognized with performance awards of that amount.

Ms. HALLIDAY. Okay. I'd like to ask a question as well, that you did state there were no absolutes in your mind in security. But we do have a letter here, a very absolute statement from your boss, the Secretary, that says, quote, "To be clear, VA's security posture was never at risk."

Is that a true or false statement?

Mr. WARREN. I would tell you, sir, as the person who ghost wrote that memo, in terms of doing the staff work for the Secretary, I was not clear in my language and I take ownership of that.

Mr. HUELSKAMP. Is it true or false?

Mr. WARREN. It is true with respect to the ATO process, which this memo was trying to answer. With respect to the broader question, as we've already talked about today, there always is some risk. And so again—

Mr. HUELSKAMP. Is this a false statement then?

Mr. WARREN. I would not say it was a false statement, sir.

Mr. HUELSKAMP. It's an inadequate statement? A mistake?

Mr. Lowe, let me ask you a question: Have you ever brought to Mr. Warren's attention that there are significant security issues that need to be addressed?

Mr. LOWE. Congressman, thank you.

Have I ever brought attention to Mr. Warren that there are significant security issues that need to be addressed? No, sir, I have not.

Mr. HUELSKAMP. You have not?

Mr. LOWE. I have not.

Mr. HUELSKAMP. Usually, I try to anticipate an answer. And to anticipate an answer that in your job you have never identified a single security risk really strains credibility. Your own testimony.

So you've never sent an email, never made a statement to Mr. Warren or his superiors that there are any security risks in the IT system at the VA?

Mr. LOWE. I brief Mr. Warren and the Secretary frequently on security risks for the organization.

Mr. HUELSKAMP. Do you know how many foreign state actors have been identified as perhaps intruding upon the system?

Mr. LOWE. I know that there are foreign state actors that are—

Mr. HUELSKAMP. Do you know how many have you identified? Is there one or more?

Mr. LOWE. Individual state actors?

Mr. HUELSKAMP. The Individual states. It's a pretty clear question.

Mr. LOWE. Yes, sir.

Mr. HUELSKAMP. Have you identified more than one?

Mr. LOWE. Yes, sir.

Mr. HUELSKAMP. How many more? Mr. Warren said there was only one, in his earlier testimony. How many more were identified?

Mr. LOWE. How many more state actors that are actively trying to penetrate the network or actors that have penetrated—

Mr. HUELSKAMP. I'm guessing there will be a second round of questions, so it probably doesn't help to try to stall. Would you answer the question? How many more?

Mr. LOWE. Sir, I have been in this position for approximately 90 days. I'm still trying to ascertain the state of the organization.

Mr. HUELSKAMP. Have you seen any memos that would identify more than one?

Mr. LOWE. More than one—

Mr. HUELSKAMP. State actor. You believe there's more than one. Mr. Warren stated there was only one. You believe there's more than one. I am asking how many more?

Mr. LOWE. I don't know the answer off the top of my head, sir. If I could get back to you on the record, I would appreciate it.

Mr. HUELSKAMP. Well, I will note for the Committee I've had a grand total of, I believe 23 questions. I've been waiting for 264 days for your agency to respond. As Dr. Roe mentioned, we're supposed to be working for the American people. And when your agency, your bosses refuse to answer questions, it looks like you're covering things up. When you say there's one state actor, he says there's more, he's only been here for 90 days, we've got a report from the people that work for you, Mr. Warren—you know this report. You know there's eight actors identified on here. And you claimed

there's only one in your earlier testimony. I think that's embarrassing. It's not only embarrassing, you're sworn under oath. So I'm going to ask you one more time, how many state actors have you identified or believe are out there that have accessed the system for 20 million veterans and their dependents?

Mr. WARREN. Congressman Huelskamp, I believe that question is directed to myself?

Mr. HUELSKAMP. Is your name Mr. Warren? Answer the question, please. Let's get on with it. We're doing the business of answering questions. Please answer them. I come from Kansas. We don't go through all this trying to act like we don't know what the question is. I asked your name. Answer the question.

Mr. WARREN. I would tell you that the Department, through the NSOC, is aware of multiple state actors who are trying to take action against the Department.

And I will tell you it is more than just state actors. It is very known in the community that it is more than countries. There are syndicates who have this as a money-making activity. And I believe that's also in the open press in terms of it's not just countries, it's individuals, it's groups of individuals. And it is not just veteran data they're going after, they go after your home, your home computer, Web sites you go to. And there is a very aggressive effort, and I know that Congress is engaged in terms of what's notification, what you should notify, how we share, and how do we do all those things.

Mr. HUELSKAMP. But you're comfortable with the current security risk?

Mr. WARREN. I am not comfortable with the current security risk, sir. And again, I will tell you the safest computer is the one you don't hook up to the Internet.

Mr. COFFMAN. Mr. Huelskamp, we'll do a second round.

Mr. HUELSKAMP. Thank you, Mr. Chairman.

Mr. COFFMAN. Mr. Warren, so we know that we've been hacked by a foreign actor, we know that, the VA system. We know that they encrypted their way out, exiting. So we don't know what they took. We know that the system contains the personal identification information for about 20 million veterans. So isn't it possible that they could have taken all of that—that there is an entity, having hacked our system, that has all the personal identifying information for all our 20 million veterans? Isn't that correct?

Mr. WARREN. Sir, I am very concerned about stringing all those facts together and stating a causality. In other words, this, this, this, this means.

Mr. COFFMAN. Well, okay, let's walk through it then.

Number one, our system has been hacked, correct?

Mr. WARREN. We are aware of incidents—

Mr. COFFMAN. That's right. Number two, that they encrypted—that they penetrated the system, and they encrypted on their way out, so we don't know what files they took. Is that correct?

Mr. WARREN. In the incident referred to, there was data removed that was encrypted, yes, sir.

Mr. COFFMAN. So we don't know what files they took, correct?

Mr. WARREN. We do not know what files they took out of the VA.

Mr. COFFMAN. Had access to information pertaining to our 20 million veterans, did they not?

Mr. WARREN. I would tell you, sir, that is the point where I diverge, because it's not clear where they had access, right. So you're assuming the VA is a small place with one computer.

Mr. COFFMAN. You're right, we don't know. That's the problem. We don't know. That's right. And so the fact is that they had access to the 20 million veterans. Aren't you concerned about that?

Mr. WARREN. Sir, I am concerned any time veterans' data is put at risk.

Mr. COFFMAN. Don't you feel that the veterans of this country—I being one of them, and there are some other veterans on this Committee—ought to be warned of that fact?

Mr. WARREN. I believe you are accomplishing that through this hearing, sir.

Mr. COFFMAN. Should you have accomplished that?

Mr. WARREN. To what end, sir? To drive veterans away from the health care they need, the mental health care they need?

Mr. COFFMAN. To inform them that they need to watch out, the fact their—that the system had been compromised, just as any private entity that had been compromised would notify the consumers that they serve. You, in fact, had an obligation to notify the consumers that you serve. That's the men and women that served this Nation in uniform.

Mr. WARREN. Yes, sir, as I did. And any time there is the potential where we believe there is the potential of a breach, we offer credit monitoring—

Mr. COFFMAN. There was a breach.

Mr. WARREN. We offer credit monitoring for a year. We have a hotline to provide those services to individuals. In the past, we have received emails from Homeland Security—

Mr. COFFMAN. Ranking Member Kirkpatrick.

Mrs. KIRKPATRICK. I yield back.

Mr. COFFMAN. Mr. Lamborn.

Mr. LAMBORN. Thank you, Mr. Chairman, and once again, thank you for your leadership on this issue.

Mr. Warren, it was testified under oath by the previous panel that when you own the domain controls you own the network and that that is what happened at the VA. Would you agree with that statement?

Mr. WARREN. I would tell you, sir, that when you have the domain controllers you can go where you would like. That is not necessarily the same as owning the network. Owning the network means you control what anybody does or anybody can do and where all the traffic goes. That is not the case.

Mr. LAMBORN. But if you are looking for information and you can go wherever you want to go, that is a pretty bad situation.

Mr. WARREN. As I believe I have—yes, sir.

Mr. LAMBORN. Can you tell me about the APO process, the certification process? I hope I am using the right terminology.

Mr. WARREN. Yes, sir. The authority to operate process is something that was established I think approximately in 2002 by the E-Gov Act. It was a paper process that was used, very routine eyes, very checklist focused, very document oriented, to if you are bring-

ing a system online, are you putting it in a box and controlling all of the boundaries on the box in such a way that it was worth the risk to the organization for the system to run.

Mr. LAMBORN. Okay, thank you. So if you go to a vendor or if you go to someone in the VA and say I want you to certify that everything is working properly and is secure, how long would it normally take them to do that?

Mr. WARREN. So that the ATO process is actually an ongoing process. Multiple documents are on different schedules on when they are generated and when they are updated. As an example, COOP/COG, which deals with what do you do if a system breaks, that gets checked and exercised on an annual basis, and in fact every year the IG comes in and looks at have you done that? That is a part of that. There is a system security plan which is the description of it. There is the security controls in terms of what you are doing. There are the management controls in terms of what you put in place because technology can't do it. And there is a whole list of documents that you run through. Each of those are on a different schedule. So when you talk certifying, there are multiple steps in the process.

Mr. LAMBORN. Okay. What would be a normal range of high-end and low end of how long that certification would take?

Mr. WARREN. Sir, if you are referring to the last two steps, which I take it you are, which is the individual looking at all of the material that exists and asking is it relevant and correct and then recommending authorization, I believe you can do that in 2 weeks to 30 days if you have a well-run organization.

Mr. LAMBORN. Two weeks to 30 days.

Mr. WARREN. For the last two steps of the process. As I said, all of the other ones are ongoing. Those last two steps are validating that the individuals below, the information security officer, the system owner, the facility, have actually done all the things and certified, attested that all of the information is correct, that it is current. So that certification process is not a go do a lot of work. It is make sure all the folks below you, all the processes you are responsible for, have happened.

Mr. LAMBORN. So if you accepted certifications like that in that 2 weeks to 30 days or 2 months process, then you would also be trusting that everything before those last two steps had been accomplished on an ongoing and regular basis?

Mr. WARREN. Yes, sir. You count on the signature of the individual and the attestation they have done their job. And I will tell you, when we did that first cycle, of the 268 documents that were signed, I rejected over 40 percent because when I looked at the underlying documentation, which is how I do things, it did not meet the standard and I sent them back to be redone. So the certifier said yep, it is ready, but when I did that first set, 44 percent did not meet it.

Mr. LAMBORN. So you would not accept an ATO without all of the previous steps having been done on an ongoing basis up to the last two steps and then reviewing it once again for those last two steps?

Mr. WARREN. Yes, sir.

Mr. LAMBORN. And you would not rush something through just to look good or something like that?

Mr. WARREN. Sir, my signature means a heck of a lot to me, so when I sign something saying that I am accepting the risk, I am accepting that risk. So I believe I laid out a responsible time period for something to be done and I had an expectation that the individual would have done all the things necessary such that when it got to me that it needed to be done. And in fact the action was given in November in a meeting where the individual accepted the responsibility to do the job by February. It had been talked about prior to that in multiple meetings about the need to fix that process. I was expecting at the end of the process that all of the things they were responsible for had happened. And even though they were, I still checked and rejected the ones that did not meet the standard.

Mr. LAMBORN. All right. Thank you.

Mr. COFFMAN. Mr. Warren, a quick question. Did you mislead the Secretary of Veterans Affairs when you had inserted the language in the letter that was sent to me on May 14th, "To be clear, VA security posture was never at risk." Did you mislead the Secretary?

Mr. WARREN. Mr. Chairman, I did not intend to mislead the Secretary.

Mr. COFFMAN. But you did?

Mr. WARREN. I don't believe I did.

Mr. COFFMAN. You did?

Mr. WARREN. I believe my answer was within the context of the question which was dealing with the ATO process.

Mr. COFFMAN. Dr. Roe.

Mr. ROE. Just very briefly. Mr. Warren, one of the things that is most important I think at the VA or with anyone in health care is trust. You have to trust not only the person that is seeing you, providing the care, but you have to trust that that information will be protected. Because many times it could be very embarrassing if something had occurred to you years ago that maybe current family members, other people don't know about, right now the relationships you have had, issues that come along, mental health care issues. That is why it is so—not just money, but that is why that is important.

And I guess a question that I have, and the VA has not done an exemplary job, in 2006 with the laptop it took forever to notify people. Secondly, when the issue came along with the colonoscopies, that wasn't handled very well by the VA. And I don't think that veterans right now understand, as a matter of fact I guarantee you they won't until they see this hearing today and the word gets out among the veteran community that all of their personal information potentially is at risk.

I guess the question I have for you is, are you concerned at all about your data in the VA, if you go to the VA, about your own personal information, you?

Mr. WARREN. Sir, I have no reservation about using VA benefits or services, placing the data, my data in the veterans' hands, into my staff's hands, into the rest of the VA. I believe we would be doing a disservice to our veterans by telling them, hey, there is a disproportionate risk and therefore you should not be coming to the VA for those services or benefits.

We know health care, and as you have already talked about in other settings about mental health care and making sure our veterans get that, I would hate that this, the potential to drive folks away from the services and the benefits not only that they have earned but they need.

Mr. ROE. But equally just as bad is to have that information once she have shared it with somebody, shared with the world, I think Mr. Lamborn said in a WikiLeak drop. I think the most compelling thing you said, and I have to agree with you the more I hear in these hearings I go to, is don't hook up a computer to the Internet if you don't want somebody to know about it. Apparently if you can't protect it, I mean that is what you said just a minute ago, whether you said that just out of exasperation or fact, but I think when you hook it up, you may be now, you may be an open book.

Mr. WARREN. I would tell you, sir, and it is a great area where we focus and it is the training of our workforce, our greatest asset and our greatest risk is our employee base, because if you do something without thinking, if you do not think about where you go—in other words, if you go out to the Internet and you say "free car," and you go to that Web site to get that free car, you are actually downloading probably malicious software.

Within the VA, we protect against that. But when you are at home, if you go to the wrong place or your child goes to the wrong place or a visiting sibling or niece, you are putting that computer at risk, right? And one of the programs that we have at the VA is, we don't allow you to hook your personal commuter up to the VA. We actually allow you to come into the VA through a virtual environment so you don't bring any of the things you have on your home computer.

In fact, at the Federal Trade Commission before the virtual technology had really matured, we paid for anti-virus protection for individuals' personal computer because we knew if they had to use it to get into the VA through remote or into the Federal Trade Commission.

At the VA we don't have to do that because we protect by doing virtual. But the behaviors that we build at the VA we want them to take home, because if you are at home dealing with identity theft because you did a bad thing unintentionally, you really can't do your job at the VA as a result of it.

Active aggressive education. Posters. Some of the things that we have been exploring with, and we did it at the Federal Trade Commission, is you do spooks, right? You send individuals email at work intentionally, bad stuff, right, and you want them to basically do it. And you pop up and say don't do this for real, because this, if this had been a real one, you would have just compromised your system.

Mr. COFFMAN. Mr. Walz.

Mr. WALZ. I yield back my time, Mr. Chairman.

Mr. COFFMAN. Mr. Huelskamp.

Mr. HUELSKAMP. Thank you, Mr. Chairman. I apologize for my emotion earlier. I have a 95-year-old veteran uncle, a Purple Heart recipient who is facing some medical problems and the thought that his records might be at risk is particularly worrisome to me.

But I have a few more follow-up questions for Mr. Warren and his assistant on some budget issues.

If I understand correctly, the VA intends to transfer almost $69 million to various IT efforts. Is any of that money destined for IT security?

Mr. WARREN. Sir, so I can make sure I am answering the question appropriately, is that referring to a reprogramming action that was sent up to the Hill, or is this something else?

Mr. HUELSKAMP. That would be a reprogramming.

Mr. WARREN. This would be the reprogramming. I need to go back and confirm which accounts were being moved. I do not believe—in fact, I am pretty sure that that transfer would not be degrading any of the efforts we are doing in information security; that the work that we need to do to continue CRISP and to support the work on the material weakness that the IG has identified—

Mr. HUELSKAMP. Is it enhancing your IT security efforts?

Mr. WARREN. I would tell you every day we are working on enhancing our—

Mr. HUELSKAMP. With this transfer, are you moving money to enhance the IT security?

Mr. WARREN. The primary purpose of those dollars, sir, that transfer, is to move accounts, move dollars out of different accounts—

Mr. HUELSKAMP. Are you using it for enhancing IT security? Yes or no.

Mr. WARREN. I will need to go back and confirm if we are moving funds into the information security accounts. I can't tell you that directly here, but I will get back to you, sir.

Mr. HUELSKAMP. The second budget question would be, it is my understanding under your direction, the VA spent $14 million for a conference room, approximately $14 million for a conference room in Martinsburg, Virginia. Is that accurate?

Mr. WARREN. Sir, I would need to take that one for the record. The number I believe is high, but I need to go back and pull the records up to confirm.

Mr. HUELSKAMP. When you say high, is that in the ballpark? Roughly? I appreciate getting the actual figures, but your best guess is how much was spent on this conference room?

Mr. WARREN. Sir, the reason I would like to take the question for the record is Martinsburg is a facility that has multiple conference facilities in it. It is a place where we have the NSOC in terms of our security group. So I don't know if it is facilities we built for them. There is a location for the Secretary and the leadership team. I don't know if it refers to that. We also have a command post for the IT organization in case we deploy there. So I don't know which one you are speaking to, so that is why I would like to take it for the record.

Mr. HUELSKAMP. There is one here. It would be the one room that has a plaque on the wall with your name on it. And I don't know if we have a copy of that. That would be the plaque that is on the wall. So if you are going to look for the room—is it customary in the VA to put your name on a plaque on a wall?

Mr. WARREN. Sir, that is actually the plaque to the building, and I was the responsible official that worked with the Congress to get

the funding for that location. And I believe if you look in any new building that has been built, the names of the individuals responsible normally appear on the plaque.

Mr. HUELSKAMP. I would say actually say put about 300 million taxpayers on there as the ones responsible for the building.

The last thing I want to ask you about, you mentioned credit monitoring services.

Mr. WARREN. Yes, sir.

Mr. HUELSKAMP. Who do you provide those to?

Mr. WARREN. We provide those in any case where we believe there is the potential for the release of veterans data.

Mr. HUELSKAMP. So you do that on an individual—

Mr. WARREN. On an individual basis. A letter is sent out to each of the veterans where—

Mr. HUELSKAMP. Do you know how many you have provided this for?

Mr. WARREN. I will take that for the record and get it back to you, sir.

Mr. HUELSKAMP. Okay. So you actually have identified individuals you believe their data is at risk and provided them credit monitoring services if they so choose?

Mr. WARREN. Any time we believe there is the potential of the information being released, we offer the credit monitoring protection to those veterans.

Mr. HUELSKAMP. Okay. And I understand you don't believe anything is actual, you don't have actually any loss of data. It is all potential.

Mr. WARREN. I will tell you, sir, we go the extra distance by offering that. We actually have a lower threshold for offering than anybody else because we want to be sure—

Mr. HUELSKAMP. You know that how?

Mr. WARREN. Based upon our communication with the industry and conversations with folks who offer credit monitoring. I am not sure you will find other government agencies who offer credit monitoring if there is the potential of a risk. I think the VA is unique in that regard.

Mr. HUELSKAMP. I look forward to that information, the exact numbers of folks you have identified potentially at risk.

Mr. WARREN. Yes, sir.

Mr. HUELSKAMP. Thank you, Mr. Chairman. I yield back.

Mr. COFFMAN. Potentially, I think that number is about 20 million. Mr. Warren, thank you so much for your testimony today. Mr. Lowe, you are excused, both of you. Thank you. Stay around. I think if we have time we will do that classified setting after Mr. Davis gives testimony.

On the last panel today is Mr. Jerry Davis, former Deputy Assistant Secretary for Information Security for the Office of Information and Technology at the Department of Veterans Affairs.

Before I recognize you, Mr. Davis, I ask that you please rise and raise your right hand.

[Witness sworn.]

Mr. COFFMAN. Please take your seat and you will be recognized for 5 minutes, Mr. Davis.

STATEMENT OF JERRY L. DAVIS, FORMER DEPUTY ASSISTANT SECRETARY FOR INFORMATION SECURITY, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS

Mr. DAVIS. Chairman Coffman, Ranking Member Kirkpatrick, and Members of the Subcommittee, thank you for the opportunity to convey my concerns to you regarding the protection of information systems and information, which includes sensitive veteran data at the Department of Veterans Affairs.

From August 2010 until February 2013 I have served as the Deputy Assistant Secretary Information Security and Chief Information Security Officer at the VA. As the DAS IS, I served as the most senior civil servant staff member within VA with responsibility for oversight and accountability and the protection of VA information, VA privacy, records management, and the Freedom of Information, FOIA, Act process.

At that time, the time of my departure from VA in early February 2013, I was one, if not the longest serving chief information security officer in the Federal Government, with nearly a decade of service in that role spread across multiple Federal agencies. I am also a Marine veteran, having served in combat with distinction during the first Gulf War, so the appointment to the position as the VA CISO had special meaning. It was a position that I did not take lightly and I was and I still am extremely proud to have had an opportunity to serve our country, and equally proud to have had an opportunity to serve the veteran community.

My time at VA was largely filled with a great sense of pride because of the purpose and mission of VA and because of my role, which had a direct and positive impact on the veteran community. However, there came a time at the end of my tenure where my pride turned to serious consternation, and that consternation remains to this day.

In nearly 20 years of building and managing security programs across government and private industry, I have never seen an organization with as many unintended security vulnerabilities. Upon my arrival in late August 2010, I inherited results of more than 15 continuous years of an unintended and documented material weakness in IT security controls. This material weakness included more than 13,000 uncompleted IT security corrective actions. These 13,000 corrective actions will require more than 100,000 sub-actions to fully remediate and manage IT security vulnerabilities and improve the VA security posture. In early September 2010, I was also advised that nearly 600 VA systems' Authority to Operate had expired and there was no plan in place to bring these systems into compliance.

Despite the voluminous number of uncompleted corrective actions and expired ATOs, the most concerning issue was a conversation I had with the VA Principle Deputy Assistant Secretary Steph Warren, who told me shortly after my arrival that we have uninvited visitors in the network. Further discussion with the VA network security operations team indicated that VA became aware of a serious network compromise in March 2010 and these uninvited visitors were nation-state sponsored attackers.

Over the course of time while working with the VA NSOC and external agencies I learned that these attackers were a nation-state sponsored cyber espionage unit and that no less than eight different nation-state sponsored organizations had successfully compromised VA networks and data or were actively attacking VA networks, attacks that continue at VA to this very day.

These group of attackers were taking advantage of weak technical controls within the VA network. Lack of controls such as encryption on VA data bases holding millions of sensitive records, web applications containing common exploitable vulnerabilities, and weak authentication to sensitive systems contributed to successful unchallenged and unfettered access and exploitation of VA systems and information by this specific group of attackers.

During my tenure, I consistently ensured that each instance of attack or compromise by these group of attackers was documented and communicated to the VA OIT leadership through specialized reporting called Key Investigative Reporting performed by the NSOC Deep Dive analysis team and biweekly security meetings with the VA Principle Deputy Assistant Secretary, Mr. Steph Warren.

From late August 2010 until my departure in early February 2013, I planned for and executed with support from various sub offices within OIT a series of initiatives and activities needed to improve network and system security with the particular focus on defending the network against sophisticated and targeted attacks levied by nation-state sponsored organizations. Some of these initiatives included a web application security program, the VA software assurance program, continuous monitoring and diagnostics of VA information systems, mandating encryption of all VA databases, and supported the reduction of the total number of VA databases hosting sensitive veteran information.

During my tenure as CISO, with the support of VA as a whole, we were able to close more than 10,000 of the 13,000 security corrective actions. In all, VA personnel executed more than 100,000 sub actions. While these actions did improve security from a compliance perspective, there still existed a problem of fully implementing adequate technical security controls needed to defend network systems and system information from nation-state sponsored attackers.

The heart of selecting the proper technical controls meant fully understanding the threat actors, their tactics, techniques and procedures, and along with systems and network vulnerabilities in implementing a program that could continuously report on and remediate identified vulnerabilities in a near realtime fashion.

Over time, the Office of Information Security worked to enhance a comprehensive program called Continuous Monitoring and Diagnostics that would provide adequate security of VA systems and networks by continually evaluating certain technical controls in a near realtime fashion. There is proof that a good CMD program monitoring the correct controls can significantly improve information security and is consistent with the direction that the Federal Government is taking in securing Federal systems. It is also significantly superior to even a good paper-based ATO process.

It is my testimony that at the time of my departure from VA that the process required for the DAS IS to make an attestation that VA systems were adequately secure was completely faulty and improper and implementation of the process veteran systems and VA information to further risk of compromise. It was confirmed to me by the VA information security staff charged with executing the process that it was flawed, provided no value, and that providing a positive attestation to the adequacy of security controls would seriously compromise the integrity of the VA security program. I subsequently conveyed this message to the Assistant Secretary and the PDAS by formal memorandum and in conversation to the PDAS between January 15, 2013, and January 23, 2013.

VA Handbook 6500.3 states that the DAS is responsible for reviewing all C&A packages and making a decision recommendation to the authorizing official to issue an IATO, ATO or Denial of Authorization to operate; and providing an IATO extension in the event local management can demonstrate continuous monitoring and security due diligence are being provided.

In accordance with VA information security policy and following VA information security procedures as a DAS IS, I elected to recommend a denial of Authority to Operate and also elected to recommend movement of VA systems over the course of eight months into an enhanced continuous monitoring program where systems technical controls can be centrally managed and evaluated in a near realtime fashion. I based my decision on the guidance provided by the information security team on the fact that the paper-based process would not keep highly sophisticated nation-state sponsored attackers from further compromising VA data.

Furthermore, as each VA system was transitioned into the continuous monitoring program, additional specific critical controls would be evaluated for adequacy before being fully granted a full ATO. These additional critical controls are proven to slow and repeal sophisticated nation-state sponsored attackers from compromising information systems and data. This was an agreed upon process with the VA information security team and a process that had been briefed by me to the Director of IT Audits and Security within the VA Office of the Inspector General several weeks before the process implementation.

Despite the authority granted to the DAS IS, to make the recommendation to deny authorization, the VA OIT PDAS made a concerted effort to circumvent my authority and influence my decision to make a recommendation to the accrediting official that 545 VA systems be given an interim authority to operate. Furthermore, VA handbook and policy 6500.3 and VA policy 6500 provides no role or authority for the PDAS, OIT with regard to the program or processes governing authority to operate.

To this end, I would recommend to this Subcommittee some recommendations. Review all key investigation reports and Deep Dive analysis reports and Web Application Security Program reports to assess the damage and depth of exposure, extent of compromise to VA systems and compromise to Veteran information, and regularly report to the House Committee on Veterans Affairs on progress made with respect to mitigating access to VA systems and veteran information by nation-state sponsored organizations.

Assess previously identified web application exposures and assess for potential compromise of veteran data, both PII and PHI.

Include web application exposures as part of the Data Breach Core Team evaluation process.

Assess the potential compromise to non-VA networks sharing an interconnection with VA's networks.

Designate the VA network as a compromised environment and establish controls that are effective and support the reclamation of control back to VA from nation-state sponsored organizations.

Move the VA systems into a full continuous monitoring and diagnostics program with near realtime situation awareness of a security posture with a focus on the 20 critical controls.

Increase VA funding for VA security programs and number of information security officers supporting VA field offices and facilities.

Move reporting lines for the DAS Information Security directly to the Assistant Secretary OIT or to the Office of the Secretary, VA.

Assess the past and present practices of the OIT leadership with regard to decisions made in the protection of VA systems and information.

I would like to thank the Members of the Subcommittee for your time today and I look forward to any questions you may have.

[THE PREPARED STATEMENT OF JERRY L. DAVIS APPEARS IN THE APPENDIX]

Mr. COFFMAN. Thank you, Mr. Davis. Mr. Davis, in your experience, what would be the intended use for their access once these actors gained access into the network?

Mr. DAVIS. The actors, once they get inside a network, depending on what their goals and objectives are, could be a number of things. So initially, once they get inside a network they establish a foothold and that foothold is actually meant and designed to allow them access into the network at another given time. So basically what they do is, they install backdoors into the network. Once they are inside the network and they have established those backdoors, they then attempt to move laterally throughout the network by compromising passwords, user names and things of that nature, and elevating their privileges so they can further move throughout the network and start looking at systems to potentially compromise.

Their long-term objective is to maintain a presence inside the network for whatever they need to do. So by maintaining the presence means that they will attack multiple systems, they will continue to steal passwords, user names, things of that nature, so they can maintain their presence, and then essentially take whatever data that they deem may be important for them.

Mr. COFFMAN. Mr. Davis, can you elaborate on these nation-state attackers?

Mr. DAVIS. So within VA I saw—we dealt with approximately eight different types of attackers or groups or organizations. In looking at reporting that was put out by industry experts, particularly a report in February of 2013, Mandiant, they identified attackers coming from the People's Republic of China, the People's Liberation Army, and in information that I had at the time and looking back when we did the analysis on those individuals, we

identified that it was also the same groups. One the groups we called were the Comment Crew, and they are known to be sponsored by the People's Liberation Army.

Mr. COFFMAN. Mr. Davis, how does an organization defend against these sophisticated attackers once they are in the network?

Mr. DAVIS. Once they are in the network, once you understand that they are in the network, you have to do something which I call is, you are in a compromised environment. So there is a number of things that you need to do to understand how do you reclaim that environment.

The first thing you need to do is identify which systems were compromised, do a forensics evaluation if you can on what was actually taken, remove users from resources around the network and then do things such as look at what we call indications of compromise.

So this is basically digital fingerprints that we would have of different groups who have compromised other environments and we now have their fingerprints. You will look for these indications of compromise and then basically go back and remediate all of those areas where you believe the compromise took place or where you know the compromise took place.

So if you know that the compromise was a missing patch, you have to start patching past the systems. The problem is, is that once you realize that the individuals are in the network, on average, they have already compromised the environment for generally up to a year by the time you figured out they have been in the network. So you may go back and patch a particular system, but they have already established backdoors elsewhere in the network. So it becomes sometimes chasing your tail around and around in circles in trying to identify where they are. So you may patch, but they will pop up again somewhere else. So it takes over time a number of years, months to years, to go through the organization systematically and plug these holes.

DoD puts out a very good document, it is not classified, it is sensitive but it is the not classified, that is called Operating in a Compromised Environment, and it teaches organizations, it is instructions on how you actually operate in a compromised environment and reclaim that environment.

Mr. COFFMAN. Mr. Walz.

Mr. WALZ. Thank you, Chairman. Mr. Davis, thank you. Thank you for your service both in uniform and after.

I am going to try and go back at this issue because I think the issue of security and veterans security is paramount. The accusations that have been laid out, I am going to get at this and try and figure it out. Can you tell me, was this issue over you pointing out that there were problems, did that lead to your departure from VA?

Mr. DAVIS. The problems at VA didn't lead to my departure. Like I said earlier, we had worked through a tremendous number of corrective actions. You know, as I said earlier, I worked through about—of the 13,000, we had gotten through about 10,000 of them. At that time I felt that the work that I was doing at VA, some other opportunities came up. I had an opportunity to move back to the West Coast where I am from originally and be closer to my

family out there, was part of the reason why I elected to move back.

Mr. WALZ. Because you signed off, if I am right here, in August 31 of 2011 you did the extensions on the ATOs.

Mr. DAVIS. That is correct.

Mr. WALZ. And then again you met with Mr. Warren on November 29th about the expiring ATOs, and then on December 21st you informed him of your resignation. It is just personal timing on all this, is why this hit like this?

Mr. DAVIS. Yes, it was the timing. I had actually notified the previous Assistant Secretary Mr. Baker before November that I would be departing. I had just had a one-on-one with him and said that I have an opportunity to go back to the West Coast. I don't have anything in writing but there has been a formal offer. When I get a formal offer—

Mr. WALZ. This was all prior to December 31st on the expiring ATOs.

Mr. DAVIS. That is correct.

Mr. WALZ. Why would they have asked you when they knew you were leaving, you had already signed on to these, do you think it was appropriate at that time? Now, you say, the thing that I am going at is under duress. What did they do or ask you to do that violated your conscience on this to sign these things?

Mr. DAVIS. The process to do the Authority to Operate, it is a sign-off that says—that gives my attestation that the systems are adequately secure. The process is pretty involved and very extensive. So the problem that I had was that the process was asked to be short-circuited. In other words, an email had come out from the OIT front office indicating that Mr. Warren wanted all the authorities who operate to be signed by the time I left, and that was 2 weeks. This is January 11th. So my team forwarded that to me—

Mr. WALZ. Why didn't you just say no and walk away? Because what you are asking here is signing off on a system that is going to possibly lead to the breach of this. You knew it wasn't working. You knew that there were violations made. But by putting your name on it, it gave the authorization to move it forward. You were already leaving your job and had notified them, and then a month later a memo is sent, and I am going to get to that in a minute, two different ones, and I find out about it here for this hearing. I am still trying to get at this.

Mr. DAVIS. Yes, sir. At that point, I did say no in writing, in memorandum form to Mr. Baker, and that would have been on or about January 15th, immediately after I became aware that I was needed to sign these before I had departed. In the memorandum that I sent to Mr. Baker, I said that this is improper because all of the activities that are needed to make a decision on authorities to operate can't be done in 2 weeks. I said there is going to be errors and omissions and that it was improper, we would jeopardize the integrity of security.

Mr. WALZ. Did someone threaten you?

Mr. DAVIS. I wouldn't say—no one threatened me, but basically I was told that I would not be getting—be given a transfer date, a transfer date would not be given to the agency that picked me up until I signed off on the documentation.

Mr. WALZ. Who told you that about the transfer?

Mr. DAVIS. Mr. Warren.

Mr. WALZ. Mr. Warren said you would not be given a transfer date if you wouldn't sign on a document that your conscience told you was wrong?

Mr. DAVIS. That is correct. And that was—I contacted the senior executive HR because the new organization was contacting me and asking me when was I going to be coming on board, because I had told them back in December that I would give VA 30 days to work through whatever I had left to do and I would be coming on board. At this point they are contacting VA. They are asking when am I going to get a release date. I contacted HRHCS and I was told that Mr. Warren said that you would not be given a release date because you still had a project to finish.

Mr. WALZ. Did he miss this last paragraph in the memo you gave him? The one I have here says I attest that there is a clear and present danger and risk of exposure and compromise of the sensitive data.

He testified under oath that he never got that, that this was added to the letter that was sent to Congress on January 28th, and on January 29th he got the letter without that there.

Mr. DAVIS. He did indeed, sir, get a different copy.

Mr. WALZ. Why a different copy?

Mr. DAVIS. Let me explain what happened. I originally—that was the original letter that I had written, and that letter was on an internal—a letter that was going to VA internally and it had concurrently copied all the Members of Congress. My business office came back to me, because we were putting it through the official VA system, my business office came back to me and said we don't concurrent copy Members of Congress on letters of this type. They get an individual memorandum. So I said okay.

So they went ahead and drafted the individual memorandum in the background. Meanwhile, what I did was, I had someone look at the letter and they said they didn't like the language. They said I don't like the language. They said you probably should change this language at the bottom. It sounds a little bit dramatic and that sort of thing.

Mr. WALZ. Well, when I read this letter, the most important paragraph is the last one.

Mr. DAVIS. Yes. It was—someone told me that I asked to—the person I asked to look at it thought it was overly dramatic. I said, you know, this is a dramatic thing, but maybe it is. So I did change the letter. But what had happened was I sent that inside, but then later on before I left, I had gotten copies of the original letters that came up here to the Members of Congress and those had went out.

Mr. WALZ. Okay, I will yield back. We will wait if there is a second round of questions.

Mr. COFFMAN. Mr. Lamborn.

Mr. LAMBORN. Thank you, Mr. Chairman.

Continuing on these ATOs, Mr. Warren testified that in a well run organization you can finish up the last two steps prior to signing off on an ATO in as little as 2 weeks. Now, you did not feel that that was appropriate though, and why not?

Mr. DAVIS. Because the team that was putting together, which was the security team that worked under me that runs the what we call assessment and authorization process, they looked at the process—they put together the process, looked at it, brought it to me and said, sir, do not sign these, the process is not good. But I already knew that just by looking at what was coming up to me for me to sign that it wasn't a good process.

Mr. LAMBORN. So in an ideal situation, if it was a well run organization you could do that. So you are saying it wasn't a well run organization?

Mr. DAVIS. The ATO process that was taking place at the very end was not the general ATO process that we had done in the 2-1/2 years that I had been there. It was cut short, very abbreviated, to make this 2-week timeframe. And I said there is no way you can certify and accredit 600 systems in a 2-week timeframe by going through all the controls.

The bigger problem that I had was there is a checklist, and some individuals have already testified to this. That on that checklist we were asking people out in the field to validate that the controls had not changed. My team that came back to me in reaching out to the field, one of the reasons they told me not to sign the document is because the individuals who were supposed to sign off on the checklist delegated the authority down, down, down into the organization to hurry up and meet the timeframe.

So you had individuals that had no concept about the security posture of the system checking off on this checklist and then sending them up to me for signature, and I just refused to sign them.

Mr. LAMBORN. Thank you. That is very illuminating, and I am sorry that we are even in this posture today. I am sorry that we have to have this hearing.

You mentioned encryption and others have talked about that. Was it a negligent practice or a deficient practice not to have veterans' personal information encrypted so that one of these, up to eight state actors or state sponsored or outside actors, had they accessed it, it would have been not usable to them?

Mr. DAVIS. That is correct. Encryption of any sensitive data is a general policy. When I got to VA and we started looking, the VA policy, which is Directive 6500, encryption on databases was basically optional. So in 2012, I said absolutely not. I am mandating that all databases be encrypted because of the issues of individuals being in the network who could quite—pretty simply, once you got into the database you had everything that you needed.

Mr. LAMBORN. Now, those of us, some of us anyway on this panel have been concerned about what would have been able to be accessed. Am I correct in assuming that this would include, of the 20 million veterans on the system, Social Security numbers and names, ages and possibly Social Security numbers of dependents and sometimes personal health information?

Mr. DAVIS. Sure. Some of the systems that were compromised, if they had that information in them obviously they would take that. In some of the studies that my organization did when we were looking at web applications, and web applications that have a database connected to the back end it has veterans' information, my team will run security software tools and it will tell them if that

application is vulnerable to attack and how easily it is vulnerable and exploitable.

My team at that time found a number of applications that had veteran information, 30 million instances of veteran information that was exploitable, and they exploited the system to show that it was exploitable inside those systems; Social Security numbers, date of birth, so on and so forth.

Mr. LAMBORN. And what about, and I don't know if there is going to be a second round or not, I may have to pursue this later, but what about access to other networks? Like, I know DoD and VA interact a lot, at least in the health care issue. What possible access could this allow if someone was controlling VA or at least had domain control to get into other networks?

Mr. DAVIS. As we talked about earlier, the team did these key investigative reports, so specifically looking at the nation-state sponsored attackers. And one of the compromises that they picked up on, this report was right as I was leaving, this came out on January 9th, 2013, there was an incident that took place where the team, and I will just kind of read it, it says the teams in turn simply gains initial access to an enterprise via spear pfishing by moving laterally previously through compromised trusted networks.

I will jump forward in this report, and what they have said is that—has targeted and compromised one or more systems within the Silver Spring office site code, many of which are virtual private network users. Based on information collected from open source intelligence and interviews of targeted users, the Deep Dive analysis team considers the Bidirectional Health Information Exchange Program to be a high value target for this team. The BHIE program is a joint information technology data exchange initiative between the Department of Defense, DoD, and VA. The team may be interested in the data residing in the system and the network interconnections between the VA and DoD allowing this program to function or both.

Mr. LAMBORN. Thank you.

Mr. COFFMAN. Dr. Roe.

Mr. ROE. Thank you. A couple of things I want to just go over very quickly and then yield my time. In March 2010, these uninvited visitors were nation-state sponsored attackers. Over the course of time, while working with the VA, the NSOC team and external agents learned that these attackers were a nation-state sponsored cyber espionage unit and that no less than eight different nation-state sponsored organizations had successfully compromised VA networks or data or were actively attacking, not necessarily compromised but attacking VA networks, and attacks continue to VA to this day. Is that a correct statement?

Mr. DAVIS. That is correct.

Mr. ROE. So to this date, to date perhaps these attacks are taking place. The other question I have is, that I think you just stated, and you said the PLA without any hesitation. I guess I would have to ask Mr. Warren, why couldn't he say the PLA? He didn't mention that. It is not any big secret to anybody.

Mr. DAVIS. It is in the public domain.

Mr. ROE. Yes, it is.

Mr. DAVIS. And that is what I am going off. I am going off the report that came out in the public domain that listed these groups of individuals, organizations, and based on that information that is in this public domain report, we could accurately say that those are the same individuals. Even the nomenclature is the same.

Mr. ROE. And I am not a technical person so stop me if I am off base, but you mentioned that once that system has been compromised, that piece of malware is in the system, there are ways you can operate around it.

Mr. DAVIS. Yes.

Mr. ROE. But would encryption work once you have been compromised? Once that malware—do you follow me?

Mr. DAVIS. Right. So it depends on what exactly the malware is that they put on the system. Your encryption would be of little value to you if—once the malware is on the system, the malware can then go out and call down other tools into the environment. And some of the tools that they do remotely is they pulled down keystroke logging. So if they have those types of tools, a keystroke logger on that system, when you go to log in to decrypt, they have the decryption password for that system.

Mr. ROE. So they get your password that way.

Mr. DAVIS. That is correct.

Mr. ROE. And do you know that that has happened? When you have got the system up now, let's say you are back there, would you know that has happened to you, that they swiped the password?

Mr. DAVIS. We know that the way these individuals work that it is a typical tactic for them to, if they compromise something such as a domain controller as was said earlier, or particularly the domain controllers, the domain controller has a file on it called the SAM file and that file is the securities accounts manager. In that file are all the password accounts for the users in the network. So if they have got the domain controller, they will grab the SAM file. When they encrypt the information, generally, if it is going out and it is encrypted, I know they hit a domain controller. I guarantee they probably took the SAM file. They are going to go back, crack it later and are going to take every password that was on that system.

Mr. ROE. So you better change your password pretty often?

Mr. DAVIS. Yes, you would have to change all the—but the problem is, if you have compromised the domain controller, you have to change the password to the domain controller as well because they are on a controller. If you are just changing passwords without changing the domain controller, they are just grabbing that as it goes along.

Mr. ROE. Well, I want to thank all of the people here today, Ms. Halliday, certainly your team and every one of you. I have learned a lot today, and I think we will continue.

Mr. Chairman, thanks for holding this hearing.

Mr. COFFMAN. Mr. Huelskamp.

Mr. HUELSKAMP. Thank you, Mr. Chairman. I just want to follow up on a statement that Dr. Roe mentioned in which he stated that you learned about these attackers were a nation-state sponsored cyber espionage unit with no less than eight different nation-state

sponsored organizations. Who told you this, how did you determine that, and was that common knowledge in the IT network?

Mr. DAVIS. It was put together through information that the VA Information Security Team, they are called the Enterprise Network Defense Team, they put that information together because they track, as Mr. Warren stated earlier, they track all these issues across the network. They produce these reports. They would send them to me and Mr. Warren and a couple other folks and I would read through them and work out a plan of action or strategy to work through this.

Mr. HUELSKAMP. So the report you mentioned, which I believe we have a copy of, both reports, did Mr. Warren receive these reports as well?

Mr. DAVIS. Yes, he was on that email distribution list. I think it was only Mr. Warren, myself and maybe one other person. There is like three people.

Mr. HUELSKAMP. Did you discuss this issue of nation-state sponsored organizations with Mr. Warren?

Mr. DAVIS. We did from time to time initially when I first came on board at VA. He told me that we have uninvited visitors in the network. I pretty much knew what that meant. I had dealt with it before. And then going on in subsequent talks, from time to time I had a biweekly security meeting with Mr. Warren. It would come up about these attackers in the network. If we had an incident it might be the topic of the day that we had an incident and we are trying to work through it. So, yes, we definitely talked about it.

Mr. HUELSKAMP. And above Mr. Warren, did you discuss with any of his superiors about that or did you just leave it in his hands?

Mr. DAVIS. I generally—my reporting line was to Mr. Warren, so generally, I didn't have a great opportunity to talk to folks above Mr. Warren.

Mr. HUELSKAMP. Did you ever email them with the information or include them on an email distribution about this issue?

Mr. DAVIS. No. I just worked directly with Mr. Warren on those things.

Mr. HUELSKAMP. Okay. I think you were here earlier, but a statement from Mr. Shinseki indicates that, again to be clear, VA security posture was never at risk. Your opinion on that, Mr. Davis. Is that an accurate statement?

Mr. DAVIS. I would say that is not an accurate statement.

Mr. HUELSKAMP. Okay. Did Mr. Warren ever tell you that was an inaccurate statement? Did you ever discuss something along those lines?

Mr. DAVIS. At the time when we were doing the ATOs in the memorandum and at the time when he visited my office, I believe it was January 22nd, I said that, you know, that the process was just bad and basically, as I wrote in the memo, I repeated the words that it jeopardized the integrity of the security program.

Mr. HUELSKAMP. Lastly, I didn't get a chance to ask questions on this issue, but recently it has come up that numerous other Secretary and high level individuals in Washington have at times used private apparently non-secure email systems to communicate and to conduct business. Do you know if that was occurring at the VA?

Mr. DAVIS. I couldn't say definitely. I would suspect that people do do that, but I have no direct knowledge that anybody was doing it. I was not asked to investigate or anything like that.

Mr. HUELSKAMP. Okay. Were there any VA policies about doing that?

Mr. DAVIS. I believe there is a VA policy. I believe it would be more on the—possibly on the HR side of the house, but it may also be in the security policy, that official business you have to conduct using VA provided email systems and things of that nature. But I don't know the exact policy that that would be. But I am pretty sure that it is in policy.

Mr. HUELSKAMP. And then lastly and I will yield back, Mr. Chairman, I wasn't trying to figure out what you were doing on personal time, but the testimony you have given sometimes has not matched up with earlier testimony as I understood that. Do you have any printed out emails or anything in your possession that would help establish the veracity of some of the discussions today, or is that all retained entirely by the Department?

Mr. DAVIS. Anything that I have with me, it is free to go to the Committee. It is a lot—some of this is off the public Internet and some of them are internal VA documentation and email systems information, things like that, that—some of them I would be concerned that where there are system compromise—or system issues, exposures of data, that it identifies the particular vulnerability in the system. So I would ask that the system piece of it be stripped out.

Mr. HUELSKAMP. I understand. Last, Mr. Chairman, Mr. Davis, as I understand it, you have 20 years of experience in the private and public sector dealing with system security and it still is your recommendation that the VA network should be designated as a compromised environment. Is that still your—

Mr. DAVIS. That is correct.

Mr. HUELSKAMP. Thank you, Mr. Chairman. I yield back.

Mr. COFFMAN. Thank you, Mr. Huelskamp. Does anybody have any questions they would like to ask?

Very well. Our thanks. Mr. Davis, thank you very much for your testimony today. You are now excused.

It is obvious from what we have heard here today that VA needs to take action to improve its IT security. The Subcommittee looks forward to working with VA to address these serious deficiencies and ensure that all steps are being taken to safeguard the information of our veterans. In that vein, I ask that in 30 days VA provide this Subcommittee a specific plan to address all of its IT vulnerabilities.

I ask unanimous consent that all Members have 5 legislative days to revise and extend their remarks and include extraneous material. Without objection, so ordered.

Mr. Weaver, the Committee will be in touch with you to establish a date and time for a separate meeting for a classified brief—

Mr. WARREN. Warren.

Mr. COFFMAN. Mr. Warren, I am sorry. I was looking at you. Mr. Warren, okay.

I would like to once again thank all of our witnesses and audience members for joining us today in conversation. This hearing is now adjourned.

[Whereupon, at 5:40 p.m., the Subcommittee was adjourned.]

A P P E N D I X

Prepared Statement of Hon. Mike Coffman, Chairman

Good afternoon. I would like to welcome everyone to today's hearing titled "How Secure is Veterans' Private Information?"

Reports from VA's Office of Inspector General, private sector consultants brought on by VA, and this Subcommittee's own investigation have revealed tremendous problems within VA's Office of Information and Technology.

Some of these issues have been made public in Inspector General reports which outlined mismanagement of human resources and the lack of much needed technical expertise. Other issues have been less publicized, such as those captured in the Deloitte ("deep dive" that identified gaps in OI&T's organizational structure and a poorly executed business model.

The latter report recognized the growth of VA by thirty-three percent since 2006; growth that is mirrored by the expansion of VA's computer network. Unfortunately, there has not been a comparable growth in the technical personnel needed to manage security of VA's sprawling network.

These failures have created problems for both the Department and for veterans.

The Inspector General substantiated that VA was transmitting sensitive data, including personally identifiable information and internal network routing information, over an unencrypted telecommunications carrier network—both violations of Federal regulation and basic IT security. The IG also noted that VA has not implemented technical configuration controls to ensure encryption of sensitive data despite VA and Federal information security requirements.

Similarly, it is evident that software patches are not up to date across the network, too many users have Administrator access, security software is not up to date on older computers, and computer ports are not properly secured. There is little to no security of file transfer protocol, and web pages are vulnerable allowing unauthorized access to veterans' unprotected personal information within the system.

While these issues alone give cause for grave concern, this Subcommittee's investigation has identified even greater problems. The entire veteran database in VA, containing personally identifiable information on roughly 20 million veterans, is not encrypted, and evidence suggests that it has repeatedly been compromised since 2010 by foreign actors, including in China and possibly in Russia.

Recently, the Subcommittee discussed VA's Authorization to Operate, a formal declaration that authorizes operation of a product on VA's network which explicitly accepts the risk to agency operations, and was told that "VA's security posture was never at risk."

In fact, VA's security posture has been an unacceptable risk for at least three years as sophisticated actors use weaknesses in VA's security posture to exploit the system and remove veterans' information and system passwords. While VA knew foreign intruders had been in the network, the Department was never sure what exactly these foreign actors took, because the outgoing data was encrypted by the trespassers.

These actors have had constant access to VA systems and data, information which included unencrypted databases containing hundreds of thousands to millions of instances of Veteran information such as veterans' and dependents' names, social security numbers, dates of birth, and protected health information.

Notwithstanding these problems, VA has waived or arbitrarily extended accreditation of its security systems on its network. It is evident that VA's waivers or extensions of accreditation only "appear" to resolve material weaknesses without actually resolving those weaknesses.

VA's IT management knowingly accepted the security risks by waiving the security requirements even though such waivers are not appropriate. This lapse in computer security and the subsequent attempts by VA officials to conceal this problem are intolerable and I look forward to a candid discussion about these issues.

I now yield to Ranking Member Kirkpatrick for her opening statement.

Prepared Statement of Hon. Ann Kirkpatrick

Thank you, Mr. Chairman.

As the Department of Veterans Affairs works hard to serve the needs of today's veterans they must work equally hard to protect their personal information.

Today's hearing is an attempt to determine whether a veterans' private information is secure. Mr. Chairman, veterans need to know that when they ask VA for the services and benefits they have earned, the information they submit in order to get those benefits will not be compromised under any circumstances.

I hope that the VA came prepared today to provide assurances to Congress and veterans that that all their information technology systems are secure. We expect VA to also answer our questions directly and honestly. As we get questions from veterans in our districts we want to provide complete and honest answers to them.

Congress received a letter from Mr. Jerry L. Davis, now a former employee at VA, who states that "there is a clear and present danger and risk of exposure and compromise of the sensitive data." I share the Chairman's concern on whether VA is following the required government practices and policies regarding the monitoring and remediation of system risk.

In addition, two OIG reports from 2012 and 2013 raise additional concerns. The 2012 report questions whether the agency has the proper Strategic Human Capital Management program to meet mission-critical system capabilities as VA moves in the 21st century. The second 2013 OIG report faults VA for failing to ensure private information by not encrypting health data transmitted to outpatient clinics and external business partners. The VA must address the concerns raised and assure veterans who come to VA for assistance that their personal information is secure.

I want to thank everyone for being here today. I would also like to thank the witnesses for their testimony and for answering our questions about the security of veterans' private information at the Department of Veterans' Affairs.

Thank you Mr. Chairman. I yield back.

Prepared Statement of Hon. Jackie Walorski

Mr. Chairman and Ranking Member, it's an honor to serve on this Committee.

I thank you for holding this hearing on such an important issue affecting our veterans and their sensitive personal information.

There are over 22 million veterans who have proudly served this country and who we are indebted to for their selfless call to protect the freedoms which we cherish. [1] The fact that the personal information of many of these veterans may have been compromised is completely unacceptable.

The VA's Office of Information and Technology has proven inept at securing the Department's information systems and has consequentially exposed veteran information.

Our veterans are comprised of an exceptional group of men and women, including their families, who should not live in fear of their private information getting into the wrong hands.

I look forward to working my colleagues and our panelists to establish an immediate plan of action that will address this serious problem.

Thank you.

Prepared Statement of Linda A. Halliday

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General's (OIG) work regarding the securing of veterans' private information by VA. I am accompanied by Ms. Sondra McCauley, Deputy Assistant Inspector General for Audits and Evaluations, and Mr. Michael Bowman, Director, OIG's Information Technology and Security Audits Division.

BACKGROUND

Secure systems and networks are integral to supporting the range of VA mission-critical programs and operations. Information technology (IT) safeguards are essen-

[1] Veteran population estimates, as of September 30, 2012, are produced by the VA Office of the Actuary (VetPop 2011). *http://www.va.gov/vetdata/Veteran—Population.asp.*

tial due to the wide availability of hacking tools on the internet and the advances in the effectiveness of attack technology. Lacking proper safeguards, IT systems are vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. VA has at times been the victim of such malicious intent. In the past, VA has reported security incidents in which sensitive information has been lost or stolen, including personally identifiable information (PII), potentially exposing millions of Americans to the loss of privacy, identity theft, and other financial crimes. The need for an improved approach to information security is apparent, and one that senior VA leaders well recognize.

In response to the need to improve security controls, VA has made progress defining policies and procedures supporting its Department-wide information security program. However, VA continues to face significant challenges implementing effective access controls, configuration management controls, and contingency planning to protect mission-critical systems from unauthorized access, alteration, or destruction. VA has taken positive steps to safeguard personal and proprietary information used by VA employees and contractors. Key actions have included:

- Mandating cyber security and privacy awareness training to ensure that VA and contract employees are familiar with applicable laws, regulations, and policies.
- Reviewing the accuracy of position sensitivity level designations for VA and contract employees.
- Strengthening its policies and procedures for identifying and reporting incidents involving information management and security violations to ensure that the incidents are promptly and thoroughly investigated.
- Establishing a clear chain of command and accountability structure for information security.

These were good first steps toward improving information security; however, more needs to be done. Over recent years, the OIG has conducted a series of reviews to help VA overcome its information security challenges by identifying the underlying causes for VA's security vulnerabilities and deficiencies. These include our statutory work, reviews of complaints to the OIG Hotline, and proactive reviews of internal controls. Our report findings have disclosed a pattern of ineffective information security controls that expose VA's mission-critical systems and sensitive data to unnecessary risk. We believe our corresponding audit recommendations provide a roadmap for VA to improve the effectiveness of its information security program and safeguard the sensitive data needed to support delivery of benefits and services to our Nation's veterans.

STATUTORILY–REQUIRED REVIEWS

For more than 10 consecutive years, independent public accounting firms under contracts with the OIG identified information technology security controls as a material weakness as a result of their annual audits of VA's Consolidated Financial Statements. Work on these audits supports our annual Federal Information Security Management Act (FISMA) assessments. FISMA requires agencies to develop, document, and implement agency-wide information security risk management programs and prepare annual reports. FISMA also requires that each year, the OIG assess the extent to which VA complies with FISMA's information security requirements, information security standards developed by the National Institute of Standards and Technology, and the annual reporting requirements from the Office of Management and Budget.

In the middle of FY 2012, while our annual FISMA assessment was ongoing, VA instituted the Continuous Readiness in Information Security Program (CRISP) to ensure continuous monitoring year-round and establish a team responsible for resolving the IT material weakness. As our FISMA work progressed, we noted more focused VA efforts to implement standardized information security controls across the enterprise. We also saw improvements in role-based and security awareness training, contingency plan testing, reducing the number of outstanding Plans of Action and Milestones (POA&Ms), developing initial baseline configurations, reducing the number of IT individuals with outdated background investigations, and improving data center web application security. However, the CRISP initiative was not launched until March 2012 and the improved processes had not been implemented for an entire fiscal year with the opportunity to demonstrate sustained improvements in information security.

For FY 2012, we provided a draft report to VA for review and comments and we expect to issue our report in June 2013. The report will discuss control deficiencies in four key areas:

Configuration Management Controls are designed to ensure critical systems have appropriate security baseline controls and up-to-date vulnerability patches implemented. However, we found:

- Systems including key databases supporting various applications were not timely patched or securely configured to mitigate known and unknown information security vulnerabilities.
- Baseline configurations, including implementation of the Federal Desktop Core Configuration, were not consistently implemented to mitigate significant system security risks and vulnerabilities across the facilities.
- Change control policy and procedures for authorizing, testing, and approval of system changes were not consistently implemented for the networks and mission critical system hardware and software changes.

Access Controls are designed to ensure that password standards are consistently implemented across the enterprise and that user accounts are monitored to enforce minimal access privileges necessary for legitimate purposes and to eliminate conflicting roles. Our FISMA assessment revealed that:

- Password standards were not consistently implemented and enforced across multiple VA systems, including the network domain, databases, and mission critical applications. In addition, multi-factor authentication for remote access had not been implemented across the agency.
- Inconsistent reviews of networks and application user access resulted in numerous generic, system, and inactive user accounts that were not removed and/or deactivated from the system, and users with access rights that were not appropriate.
- Proper completion of user access requests was not consistently performed to eliminate conflicting roles and enforce principles of least system privilege.
- Lack of monitoring of access in the production environment for individuals with elevated application privileges for a major application.

Security Management is designed to ensure that system security controls are effectively monitored on an ongoing basis and system security risks are effectively remediated through corrective action plans or compensating controls. We will report that:

- Security management documentation, including the risk assessments and System Security Plans, were outdated and did not accurately reflect the current system environment or Federal standards.
- Background reinvestigations were not performed timely or tracked effectively. In addition, personnel were not receiving the proper level of investigation for the sensitivity levels of their positions.
- Scheduled completion dates for POA&Ms were updated without written justification and supporting documentation was not adequate to justify POA&M closures.

Contingency Planning Controls ensure that mission-critical systems and business processes can be restored in the event of a disaster or emergency. However, we determined that:

- Contingency plan documentation had not been updated to reflect lessons learned from the contingency and disaster recovery tests, and detailed recovery procedures for all system priority components had not been documented and/or did not reflect current operating conditions.
- Backup tapes were not encrypted prior to being sent to offsite storage at selected facilities and data centers.

More importantly, we continue to identify significant technical weaknesses in databases, servers, and network devices that support transmitting sensitive information among VA's Medical Centers, Data Centers, and VA Central Office. Many of these weaknesses are due to inconsistent enforcement of an agency-wide information security program across the enterprise and ineffective communication between VA management and the individual field offices. Therefore, VA needs to improve its monitoring process to ensure controls are operating as intended at all facilities and communicate security deficiencies to the appropriate personnel to implement corrective actions.

We have identified and reported deficiencies where control activities were not appropriately designed or operating effectively. The dispersed locations, the continued reorganization of VA business units, and the diversity in applications adversely affected facilities and management's ability to consistently remediate IT security deficiencies agency-wide. For example, VA's complex and dispersed financial system ar-

chitecture had resulted in a lack of common system security controls and inconsistent maintenance of IT mission-critical systems. Consequently, VA continues to be challenged by a lack of consistent and proactive enforcement of established policies and procedures throughout its geographically dispersed portfolio of legacy applications and newly implemented systems. In addition, VA lacks an effective and consistent corrective action process for identifying, coordinating, correcting, and monitoring known internal security vulnerabilities on databases, web applications, and networks infrastructures.

Our FY 2012 FISMA report will include 27 current recommendations to the Acting Assistant Secretary for Information and Technology for improving VA's information security program. The report also highlights five unresolved recommendations from prior years' assessments for a total of 32 outstanding recommendations. Overall, we are recommending that VA focus its efforts in the following areas:

- Addressing security-related issues that contributed to the IT material weakness reported in the FY 2012 audit of the Department's consolidated financial statements.
- Remediating high-risk system security issues in its Plans of Action and Milestones.
- Establishing effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments.

We continue to evaluate VA's progress during our ongoing FY 2013 FISMA audit and acknowledge increased VA efforts to improve information security, but we are still identifying repeat deficiencies, albeit to a lesser extent. This fall, upon completion of our FY 2013 FISMA testing and related work, we will make a determination as to whether VA's improvement efforts are successful in overcoming the IT material weakness.

OTHER REPORTS RELATED TO INFORMATION SECURITY

Over the past 2 years, we have issued a series of audits and reviews that have identified VA's information security controls deficiencies. Our reports disclosed a number of issues, including ineffective management of systems interconnections and sensitive data exchanges, delayed contractor background investigations, and inadequate access controls that placed sensitive veterans' data at unnecessary risk.

Review of Alleged Transmission of Sensitive VA Data Over Internet Connections

In March 2013, we substantiated an allegation made through the OIG Hotline that VA was transmitting sensitive data, including PII and internal network routing information, over an unencrypted telecommunications carrier network. VA Office of Information Technology (OIT) personnel disclosed that VA typically transferred unencrypted sensitive data, such as electronic health records and internal internet protocol addresses, among certain VA Medical Centers and Community Based Outpatient Clinics using an unencrypted telecommunications carrier network. OIT management acknowledged this practice and formally accepted the security risk of potentially losing or misusing the sensitive information exchanged.

VA has not implemented technical configuration controls to ensure encryption of sensitive data despite VA and Federal information security requirements. Without controls to encrypt the sensitive VA data transmitted, veterans' information may be vulnerable to interception and misuse by malicious users as it traverses unencrypted telecommunications carrier networks. Further, malicious users could obtain VA router information to identify and disrupt mission-critical systems essential to providing health care services to veterans.

VA acknowledged transmitting PII over privately segmented networks to support service to veterans. VA concurred with our recommendations to improve the protection of sensitive data transmitted over the unencrypted carrier networks and implement configuration controls to ensure encryption of such data. VA clarified that it employs an industry telecommunications carrier network to provide a segmented network for transmitting PII, but noted that these network links are not currently employing encryption controls to protect sensitive data.

VA did not agree with the assertion that PII and internal network routing information were being transmitted over unsecured internet connections. However, based on interviews with OIT personnel at VA Medical Centers as well as information provided by the OIG Hotline complainant, we maintain that PII and router information were being transmitted unencrypted through a telecommunications carrier that also provided internet services to customers outside of VA. Nonetheless, we commend OIT for performing a review of the locations associated with the Hotline complaint and inspecting communication networks to ensure proper segmentation of VA net-

works from internet connections. We recognize that industry telecommunications carriers can segment data traffic from unsecured Web connections. However, we believe the risk remains that sensitive VA data and router information can be compromised when it is transmitted across unencrypted telecommunications carrier networks outside of VA's span of technical control. More specifically, the network alone does not provide encryption, integrity, or authentication protections for the transmission of sensitive data and such services may be vulnerable to denial of service or sniffing attacks by malicious users. The Assistant Secretary for Information and Technology acknowledged these information security risks by stating OIT will review technical network communications practices across the enterprise and take corrective actions without hesitation.

Audit of VA System Interconnections With Research and University Affiliates

In October 2012, we reported on the effectiveness of VA's management of network interconnections and sensitive data exchanges with its research and university affiliates. Our audit disclosed that VA has not consistently managed its systems interconnections and data exchanges with its external research and university affiliates. Despite Federal requirements, VA could not readily account for the various systems linkages and sharing arrangements. VA also could not provide an accurate inventory of the research data exchanged, where data was hosted, or the sensitivity levels. In numerous instances, we identified unsecured electronic and hardcopy research data at VA Medical Centers and co-located research facilities.

We determined that VA's data governance approach has been ineffective to ensure that research data exchanged is adequately controlled and protected throughout the data life cycle. VA and its research partners have not consistently instituted formal agreements requiring that hosting facilities implement controls commensurate with VA standards for protecting the sensitive data. The responsible Veterans Health Administration program office's decentralized approach to research data collection and oversight at a local level has not been effective to safeguard sensitive VA information. Because of these issues, VA data exchanged with its research partners was considered to be at risk of unauthorized access, loss, or disclosure.

VA has the opportunity to further serve veterans by supplying the patient and medical data needed to achieve advancements in medical research and health care services. However, providing such sensitive data through electronic or hard copy means without effective information security controls and oversight has left the data susceptible to unauthorized access, loss, or disclosure. Leaving hosting facilities responsible for data governance at the local level without coordinated involvement of all stakeholders has proven ineffective and improvements are needed.

Establishing formal information security agreements is one method of documenting data sharing agreements and ensuring that hosting facilities institute information security controls commensurate with VA standards. Further, a centralized data governance and storage approach would ensure researchers effectively control and securely manage sensitive VA research information over the data life cycle. Such measures are key to protect veterans' PII and personal health information and promote continued advancements in medical research now and for the future. VA generally concurred with our report recommendations. VA is taking corrective actions, however, all recommendations remain open as full implementation has not occurred.

Review of Alleged Incomplete Installation of Encryption Software Licenses

In October 2012, we substantiated a Hotline allegation that OIT had not installed and activated an additional 100,000 licenses purchased in 2011. As of July 2012, OIT officials stated they had installed and activated only a small portion, about 65,000 (16 percent), of the total 400,000 licenses procured. OIT did not install and activate all of the licenses due to inadequate planning and management of the project. Specifically, OIT did not allow time to test the software to ensure compatibility with VA computers, ensure sufficient human resources were available to install the encryption software on VA computers, and adequately monitor the project to ensure encryption of all VA laptop and desktop computers.

As such, 335,000 (84 percent) of the total 400,000 licenses procured, totaling about $5.1 million in questioned costs, remained unused as of 2012. Given changes in VA technology since 2006, VA lacked assurance the remaining software licenses were compatible to meet encryption needs in the current computer environment. Further, because OIT did not install all 400,000 encryption software licenses on VA laptop and desktop computers, veterans' PII remained at risk of inadvertent or fraudulent access or use.

We recommended the Assistant Secretary for Information and Technology complete an assessment of the encryption software project to determine whether the

software was compatible with VA's operating systems and still met VA needs. Based on the assessment, we recommended that VA terminate the project or develop a plan, including adequate human resources and project monitoring, to ensure installation and activation of the remaining encryption software licenses. The Assistant Secretary for Information and Technology concurred with our finding and recommendations and is taking steps to move forward with the software implementation.

Review of Alleged Delays in VA Contractor Background Investigations

In September 2012, we reported on the merits of a complaint regarding ineffective VA management of its contractor background investigations. We substantiated that VA could improve management of its contractor background investigations. Specifically, VA had a backlog of 3,000 contractor background investigations as of April 2012, despite process improvements and a reduction in pending cases in recent months. VA also inappropriately prohibited contractors from working on awarded contracts although VA policy only requires initiating, not fully completing, investigations before contractors could start work.

According to VA officials, delays occurred due to ineffective management within VA's program office which is responsible for initiating and adjudicating background investigations; staff misunderstanding VA's personnel security requirements and investigative processes; and no effective centralized system to monitor progress in addressing the backlog. In the absence of a system linking contractors needing background investigations with underlying contracts, we could not determine whether VA unnecessarily paid for contractors not yet authorized to work on awarded contracts. Nonetheless, VA officials said the backlog adversely affected their ability to fully staff major IT initiatives.

Our report provided several recommendations for improving procedures to reduce the backlog of contractor background investigations and implementing a central case management system to monitor contractor status and associated costs during the background investigation process. VA generally concurred with our findings and recommendations and has reported corrective actions to address them.

Review of Alleged Mismanagement of the Systems To Drive Performance Project

In February 2012, we reported that VA's Office of Management did not effectively manage the Systems to Drive Performance (STDP) project. We substantiated that VA did not adequately protect sensitive VA information from unauthorized access and disclosure. Specifically, we determined that more than 20 system users had inappropriate access to sensitive STDP information. On a specific note, VA's National Data Systems Group did not consistently approve requests for user access. Furthermore, project managers did not report unauthorized access as a security event, as required by VA policy. Security deficiencies occurred because STDP project managers were not fully aware of VA's security requirements for system development and had not formalized user account management procedures. Inadequate Information Security Officer oversight also contributed to weaknesses in user account management and the failure to report the granting of excessive user rights as security violations. As a result, VA lacked assurance of adequate control and protection of sensitive STDP data.

VA concurred with our findings and recommendation to ensure that employees assigned to the STDP project receive the role-based security training needed to address the issues highlighted in the report. Additionally, VA agreed to assign an Information Security Officer to the project to ensure VA's information security requirements are met. Corrective actions have been taken and these recommendations are now closed.

Review of Alleged Unauthorized Access to VA Systems

In July 2011, we reported on the merits of an OIG Hotline allegation that certain contractors without proper security clearances gained unauthorized access to VA networks and Veterans Health Information System and Technology Architecture (VistA) systems at multiple VA medical facilities. Our review substantiated the allegation and found that contractors improperly used other employees' Virtual Private Network user accounts to gain unauthorized access to VA systems and networks. The review also substantiated that contractor personnel did not obtain appropriate background security clearances before gaining access to VA systems and networks. Contractors admitted to sharing two of their employees' user accounts to access VA networks on a number of occasions for maintenance and monitoring of contractor systems. Further, contractors could not provide evidence that it readily initiated actions to terminate user accounts after the employee's separation date.

VA policy specifically prohibits the sharing of user accounts and requires the closing of user accounts as part of proper user account management. Further, VA policy requires VA personnel to regularly review user account access for inappropriate or unusual activity and take necessary actions. Contractors stated they did not fully understand VA's information security requirements regarding user account access and did not believe additional user accounts were needed. Additionally, VA did not actively monitor user account activity or readily communicate with contractors the need periodically to identify and terminate unnecessary user accounts. Without effective controls to prevent unauthorized access by contractors, VA information systems and sensitive veterans' data are vulnerable to increased risks of compromised availability, integrity, and confidentiality. The lack of individual accountability over user accounts provides ample opportunities to conceal malicious activity such as theft or misuse of veterans' data. VA concurred with our findings and recommendations. However, the report remains open because a key recommendation regarding contractor security controls and practices has not been implemented almost 2 years after we issued the report.

CONCLUSION

Well-publicized information security incidents at VA demonstrate that weaknesses in information security policies and practices expose mission-critical systems and data to unauthorized access and disclosure. Through its CRISP initiative, VA has strengthened its efforts to define policies and procedures supporting its agency-wide information security program. However, its highly decentralized and complex system infrastructure poses significant challenges to implementing effective access controls, system interconnection controls, configuration management controls, and contingency planning practices that adequately protect mission-critical systems from unauthorized access, alteration, or destruction. Until VA fully implements key elements of its information security program and addresses our outstanding audit recommendations, VA's mission-critical systems and sensitive veterans' data remain at increased and unnecessary risk of attack or compromise.

Mr. Chairman, this concludes my statement. We would be happy to answer any questions you or other Members of the Subcommittee may have.

Prepared Statement of Stephen W. Warren

Introduction

Chairman Coffman, Ranking Member Kirkpatrick, Members of the Subcommittee: thank you for inviting me to testify regarding the Department of Veterans Affairs' (VA) Information Technology (IT) security strategy. I appreciate the opportunity to discuss VA's plans, actions, and accomplishments in IT security.

Protecting the data that VA holds on Veterans is as important as the Veterans themselves. As the committee knows, the Department received a wakeup call from the incident in 2006 involving a stolen laptop which contained unencrypted information on over 19 million Veterans. As a result of this incident, VA consolidated its disparate IT functions into a single, unified IT organization. This consolidation has benefited VA in many ways, especially in terms of strengthening its information security posture. VA's consolidated IT organization is responsible for protecting Veteran information at 153 hospitals, 853 community-based outpatient clinics, 57 benefits processing offices, and 131 cemeteries and 33 soldier's lots and monument sites. Our network supports over 400,000 users, and over 750,000 devices.

We remain committed to protecting the information we hold on millions of Veterans and their beneficiaries and more than 300,000 VA employees by providing round-the-clock security of VA's enterprise and infrastructure. The Department fully supports the White House's information security initiatives such as two-factor authentication using HSPD–12 compliant PIV cards, which the VA is in the process of implementing. The Department continues to improve the security posture of the VA network through our Visibility into Everything initiative, which allows VA to see and manage all of its devices and network components in real time. The continuous monitoring program is responsible for checking IT systems and monitoring every desktop and laptop computer attached to the VA network.

To reinforce our commitment to information security, we are fostering a culture change to ensure that all users on our system follow all necessary and required IT and privacy protection rules. VA launched the Continuous Readiness in Information Security Program (CRISP) in 2012 to proactively address process and policy deficiencies and architecture and configuration issues. As part of the CRISP effort, VA conducts rigorous vulnerability scanning, continuous monitoring of patching and

software inventory, implementing port security, anti-virus services, and encryption of non-medical IT laptops.

Through Web Application Security Assessments, VA is able to identify critical vulnerabilities and potential exploits in VA applications that store millions of records of sensitive data. The network infrastructure is protected through identification of all network assets and critical database stores, identification of all connections, and providing the Trusted Internet Connection Gateways services for mail, content filtering, name resolution and firewall protection.

In the past year, VA improved its security posture. The Department has ensured that over 98 percent of VA staff have received the mandatory information security training they need to protect the information of Veterans and their families. We have also completed a number of business impact assessments for contingency planning.

After the 2006 laptop incident, VA worked to ensure its laptop computers were encrypted to provide another layer of protection. Currently, over 98 percent of VA's non-medical IT laptops are encrypted. VA has around 2,500 unencrypted laptops remaining and, with the exception of laptops with specific waivers (specific medical uses, research laptops using software where encryption would disable the device, service/maintenance laptops that do not connect to VA's network or store sensitive information, and laptops purchased by VA and given to Veterans as part of a A rehabilitation program) the Department expects to complete encryption of all laptops by June 30, 2013.

Data Breaches

The Department has worked hard to regain the trust of Veterans after the stolen laptop incident in 2006. VA now has a robust data breach notification process, using a Data Breach Core Team (DBCT), which provides advance planning, guidance, analysis, and direction regarding the potential loss of Protected Health Information (PHI), Personally Identifiable Information (PII), or both. The DBCT serves as the decision making body between the functional area(s) affected, VA organizations, and external stakeholders.

The DBCT is made up of representatives from across nearly every part of the VA enterprise. When the DBCT determines that a breach is reportable, notification is made to the affected individuals and credit monitoring is extended. VA also posts a monthly report of data breach notifications on its Web site and holds a press call with reporters to discuss the contents of the report. The report is also provided to Congress, in addition to a quarterly data breach report.

VA has become one of the very best large organizations at providing notification when a breach occurs. For example, while the HITECH Breach Notification Rule requires covered entities to provide notification within 60 calendar days after discovery of the breach, and the strictest state laws require notice within 45 days after discovery of a breach, VA policy requires notification within 30 days. A review of VA's incident tracking system over the current fiscal year indicates that VA takes, on average, 25 days to provide notice. VA's standards and practices exceed even the strictest Federal and state laws and policies.

Conclusion

Mr. Chairman, VA places the highest priority in safeguarding Veterans' and employees' personal information. We are committed to information security, and although work remains, VA has made significant improvements made in the last few years and strives to meet the highest standards in protecting sensitive information. Thank you for your continued support of Veterans, their families, and of our efforts to protect Veterans and their private information. I am prepared to answer any questions you and other Members of the Subcommittee may have.

Prepared Statement of Jerry L. Davis

INTRODUCTION

Chairman Coffman, Ranking Member Kirkpatrick and members of the Subcommittee, thank you for the opportunity to convey my concerns to you regarding the protection of information systems and information, which includes sensitive Veteran data at the Department of Veterans Affairs (VA).

From August 2010 until February 2013, I served as the Deputy Assistant Secretary, Information Security (DAS IS) and Chief Information Security Officer (CISO) at the VA. As the DAS IS, I served as the most senior civil service staff member within VA with responsibility for oversight and accountability in the protection of

VA information, VA privacy, records management and the Freedom of Information Act (FOIA) process. At the time of my departure from VA in early February 2013, I was one, if not the longest serving Chief Information Security Officer (CISO) in the federal government with nearly a decade of service in that role spread across multiple federal agencies. I am also a Marine Veteran having served in combat with distinction during the First Gulf War, so the appointment to the position as the VA CISO had special meaning. It was a position that I did not take lightly and I was and I still am extremely proud to have had an opportunity to serve our country and equally proud to have had a great opportunity to serve the Veteran community.

My time at VA was largely filled with a great sense pride because of the purpose and mission of VA and because of my role, which had a direct and positive impact on the Veteran community. However there came a time at the end of my tenure where my pride turned to serious consternation and that consternation remains this very day.

SECURITY POSTURE IN 2010: VA's COPROMISED ENVIRONMENT

In nearly 20 years of building and managing security programs across government and private industry, I had never seen an organization with as many unattended IT security vulnerabilities. Upon my arrival in late August 2010 I inherited the results of more than 15 continuous years of an unattended and documented material weakness in IT security controls. This material weakness included more than 13,000 uncompleted IT security corrective actions. These 13,000 security corrective actions would require more than 100,000 sub actions to fully remediate and manage IT security vulnerabilities and improve the VA security posture. In early September 2010, I also was advised that nearly 600 VA systems' Authority to Operate (ATO) had expired and there was no plan in place to bring these systems into compliance.

Despite the voluminous number of uncompleted corrective actions and expired ATOs, the most concerning issue was the conversation I had with the VA Principle Deputy Assistant Secretary (PDAS), Stephen Warren, who told me shortly after my arrival that "We have uninvited visitors in the network". Further discussion with the VA Network Security Operations (NSOC) team indicated that VA became aware of a serious network compromise in March 2010 and these "uninvited visitors" were nation-state sponsored attackers. Over the course of time while working with the VA NSOC team and external agencies, I learned that these attackers were a nation-state sponsored cyber espionage unit and that no less than eight (8) different nation-state sponsored organizations had successfully compromised VA networks and data or were actively attacking VA networks; attacks that continue at VA to this very day. These groups of attackers were taking advantage of weak technical controls within the VA network. Lack of controls such as encryption on VA databases holding millions of sensitive records, web applications containing common exploitable vulnerabilities and weak authentication to sensitive systems contributed to the successful unchallenged and unfettered access and exploitation of VA systems and information by this specific group of attackers.

During my tenure, I consistently insured that each instance of attack or compromise by these group of attackers was documented and communicated to the VA OIT leadership through specialized reporting called Key Investigative Reporting (KIR) performed by the NSOC Deep Dive Analysis (DDA) team and biweekly security meetings with the VA Principle Deputy Assistant Secretary (PDAS), Mr. Stephan Warren.

MITIGATION ACTIVITIES 2010–2013

From late August 2010 until my departure in early February 2013, I planned for and executed with support from various sub offices within OIT a series of initiatives and activities needed to improve network and systems security with a particular focus on defending the network against sophisticated and targeted attacks levied by nation-state sponsor organizations. Some of these initiatives included the Web Applications Security Program (WASP), the VA Software Assurance Program, Continuous Monitoring and Diagnostics (CMD) of VA information systems, and mandating encryption of VA databases, and supported the reduction of the total number of VA databases hosting sensitive Veteran information.

During my tenure as CISO, with the support of VA as a whole, we were able to close more than 10,000 of the 13,000 security corrective actions. In all, VA personnel executed more than 100,000 sub actions. While these actions did improve security from a compliance perspective, there still existed a problem of fully implementing adequate technical security controls needed to defend networks, systems and sensitive information from nation-state sponsored attackers. The heart of selecting the proper technical controls meant fully understanding the threat actors, their tactics, techniques and procedures (TTPs) and along with system and network

vulnerabilities and implementing a program that could continuously report on and remediate identified vulnerabilities in a near real time fashion.

Over time, the Office of Information Security (OIS) worked to enhance a comprehensive program called Continuous Monitoring and Diagnostics (CMD) that would provide adequate security of VA systems and networks by continually evaluating certain technical controls in a near real time fashion. There is proof that a good CMD program monitoring the correct controls can significantly improve information security and is consistent with the direction that the federal government has taken in securing federal systems. It is also significantly superior to even a good paper based ATO process.

OIT LEADERSHIP DEVIATES FROM ATO PROCESS

It is my testimony that at the time of my departure from VA that the processes required for the DAS, IS to make an attestation that VA systems were adequately secure was completely faulty and improper and the implementation of the process exposed Veteran systems and VA information to further risk of compromise. It was confirmed to me by the VA information security staff charged with executing the process that it was flawed, provided no value and that a providing a positive attestation to the adequately of security controls would seriously compromised the integrity of the VA security program. I subsequently conveyed this message to the Assistant Secretary and the PDAS by formal memorandum and in conversation to the PDAS between January 15, 2013 and January 23, 2013.

VA Handbook 6500.3 states that the DAS, IPRM (now called DAS,IS) is responsible for:

(3) Reviewing all C&A packages and making a decision recommendation to the AO to issue an IATO, ATO or Denial of Authorization [emphasis added] to operate; and

(4) Providing an IATO extension in the event local management can demonstrate continuous monitoring and security due diligence are being provided . . . .

In accordance with VA information security policy and following VA information security procedures, As the DAS, IS, I elected to recommend a denial of an authority to operate and also elected to recommend movement of VA systems over the course of eight (8) months into an enhanced continuous monitoring program, where systems technical controls could be centrally managed and evaluated in a near real time fashion. I based my decision on the guidance provided by the information security team and on the fact that the paper based process would not keep highly sophisticated nation-state sponsored attackers from further compromising VA data. Furthermore, as each VA system was transitioned into the continuous monitoring program, additional specific critical controls would be evaluated for adequacy before being granted a full ATO. These additional critical controls are proven to slow and repel sophisticated, nation-state sponsored attackers from compromising information systems and data. This was an agreed upon process with the VA information security team and a process that had been briefed by me to the Director of IT Audits and Security within the VA Office of the Inspector General (OIG) several weeks before the process implementation.

Despite the authority granted to the DAS, IS to make a recommendation to deny authorization, the VA OIT PDAS made a concerted effort to circumvent my authority and influence my decision to make a recommendation to the Accrediting Official (AO) that 545 VA systems be given an IATO. Furthermore, VA handbook 6500.3 and VA policy 6500, provides for no role or authority for the PDAS, OIT with regard the program or processes governing Authority to Operate.

RECOMMENDATIONS

To this end, I would recommend that this subcommittee:

1. Review all VA Key Investigative Reports (KIRs) and Deep Dive Analysis (DDA) reports and Web Application Security Program reports (WASP) to assess the damage and depth of exposure, extent of compromise to VA systems and compromise of Veteran information; and

2. Regularly report to the House Committee on Veteran Affairs on progress made with respect to mitigating access to VA systems and Veteran information by nation-state sponsored organizations;

3. Assess previously identified web application exposures and assess for potential compromise of Veteran data, both PII and PHI;

4. Include web application exposures as part of the Data Breach Core Team (DBCT) evaluation process;

5. Assess the potential compromise to non VA networks sharing an interconnection with VA's network;

6. Designate the VA network as a "compromised environment" and establish controls that are effective and support the reclamation of control back to VA from nation-state sponsored organizations;

7. Move the VA systems into a full continuous monitoring and diagnostics program with near real time situational awareness of its security posture with a focus on the 20 critical controls;

8. Increase VA funding for information security programs; and number of Information Security Officers (ISOs) supporting VA field offices and facilities

9. Move reporting lines for the DAS, IS directly to the AS, OIT or to the Office of the Secretary, VA

10. Assess the past and present practices of the OIT leadership with regard to decisions made in the protection of VA systems and information.

I would like to thank the members of the subcommittee for your time today and I look forward to any questions you may have.

Executive Summary

At the Department of Veterans Affairs (VA), the Deputy Assistant Secretary for Information Security (DAS, IS) is responsible for information security and privacy strategy, management, policy, procedures, oversight and reporting. VA handbook 6500.3, Certification and Accreditation (C&A) of VA Information Systems, Holds the DAS, IS responsible for;

Reviewing all final C&A packages and making a decision recommendation to the AO to issue an IATO [Interim Authority to Operate], ATO [Authority to Operate], or Denial of Authorization to operate ... " and "Providing an IATO extension in the event local management can demonstrate continuous monitoring and security due diligence are being provided ... "

Beginning in early 2010 and continuing through late 2012, VA systems had been under repeated attacks and data compromised by no less than eight (8) groups of well organized and sophisticated nation-state sponsored actors who appear to have had unfettered and at times, unchallenged access to VA networks, systems and information. Internal reporting by the Office of Information Security (OIS) to the Principle Deputy Assistant Secretary (PDAS), Office of Information and Technology (OIT) kept the PDAS informed of the condition regarding exposures of Veteran dated in information systems. This reporting further confirmed to the PDAS by his own admission in late 2010 that "uninvited visitors were in the [VA] network" and thus continued to be a persistent threat and risk to VA systems and sensitive information and other interconnected non-VA networks.

Security enhancements and programs put into place by the DAS, IS beginning in late 2010 through early 2013, revealed over time that significant amounts of Veteran data was exposed to potential compromise by any attacker from both the Internet and from within the VA network infrastructure.

Because of unfettered access to VA systems and information by sophisticated attackers and lack of adequate controls to ensure protection of Veteran information, in January 2013, the DAS, IS operating under the authority of VA policy and FISMA, determined that the newly derived C&A process was not proper and inadequate for securing VA systems holding sensitive information. Despite the recommendation from the DAS, IS to the Assistant Secretary, OIT to reconsider an IATO using the inadequate process, the PDAS used his official position to influence the DAS, IS to sign an attestation that systems were adequately secure for more than 250 ATOs, and essentially exposing VA systems and sensitive data to further risk of compromise and exposure.

Questions For The Record

Letter From: Hon. Mike Coffman, Chairman, Subcommittee on Oversight & Investigations, To: VA

October 22, 2013

The Honorable Eric K. Shinseki
Secretary

U.S. Department of Veterans Affairs
810 Vermont Avenue, NW
Washington, DC 20420

Dear Mr. Secretary:

Please provide written responses to the attached questions for record for the Oversight and Investigations Subcommittee hearing entitled "How Secure is Veterans' Private Information" that took place on June 4, 2013.

In responding to these questions for the record, please answer each question in order using single space formatting. Please also restate each question in its entirety before each answer. Your submission is expected by the close of business on July 25, 2013, and should be sent to *Ms. Bernadine Dotson at Bernadine.dotson@mail.house.gov.*

If you have any questions, please call Mr. Eric Hannel, Majority Staff Director of the Oversight & Investigations Subcommittee, at 202–225–3527.

Sincerely,

Mike Coffman
Chairman
Subcommittee on Oversight & Investigations

MC/hr

Questions for the Record from Subcommittee Chairman Mike Coffman

1. The OIG indicates that IT security has been a material weakness at VA for more than 10 years. Why did VA OI&T wait until 2012 to institute a proactive initiative like the Continuous Readiness in Information Security Program (CRISP) to try to address this issue?

2. The OIG's more recent Semiannual Report states that OI&T has 11 reports open containing 60 recommendations with 14 open for more than year. Can you explain why you concur with OIG recommendations but can't seem to complete the actions necessary to close the recommendations?

- For example, one report will be open for 2 years come July and yet the most significant recommendation remains open – which deals with reviewing contractor security controls and practices to ensure compliance with VA's information security requirements.

3. What steps is VA taking to eliminate the IT Material weakness in FY 13?

4. Why does VA have so many repeat findings and recommendations from the OIG's FISMA work? Why has VA not made any significant progress towards eliminating these long standing recommendations?

5. What actions is VA taking to eliminate the use of clear text protocols used to transmit medical information between the VAMCs and the CBOCs over external service provider networks?

6. Based on the information provided in the Deloitte's deep dive report detailing inefficiencies in OI&T operations, what steps will the CIO take to improve delivery of IT services?

7. How will the issuance of the PIV badge affect the ability of the Department to respond to Congressional requests, litigation demands, and other similar requests to search, decrypt, and release bulk volumes of VA emails? Does the planned roll-out of the PIV badge tied to automatic encryption hinder timely responses to such requests in any way?

8. Why is it that the PMAS processes only focuses on meeting milestones and schedule but there are no metrics around quality, functionality and customer satisfaction?

9. The VA regulations on Information Security Matters at 38 CFR Part 75 appear to authorize an accelerated response with notice to the subjects of a data breach and/or an offer of credit protection services. How many times has credit protection service been offered to veterans for FY 2008–2012 and for each such instance, to how many veterans were such services offered? Please provide the annual cost for credit services for each year between FY 2008–2012.

10. Under the regulations at 38 CFR Part 75, if the Secretary determines that individual notice is not warranted for a data breach, then an independent risk analysis is required to be performed. How many risk analyses have been performed in accordance with these provisions for FY 2008 to present? Please describe each occurrence of such analysis including the findings and conclusions. Please also indicate each date and instance in which a data breach was reported to OMB and/or to Congress within FY 2008 to present.

11. By letter to the committee dated May 14, 2013, you stated: "To be clear, VA's security posture was never at risk." Please explain how this statement is true given the admissions uncovered in the hearing that systems and networks had been breached by foreign state actors and the testimony of OIG that, at one point, there were 4000 open vulnerabilities. If the statement was untrue when made (as it certainly appears), please describe what disciplinary action is being taken for the subordinates responsible.

12. Reports indicate that VA became aware in January, 2013, of an incident where attackers used a spearphishing attack to gain access to a joint VA–DoD network dealing with health data. How many instances have hackers tried to use VA networks to gain access to Defense Department computer systems? Please describe each instance and what corrective actions were taken in response.

Questions for the Record from Congressman Tim Huelskamp

1. I reiterated in my questioning during your testimony, if you could please communicate with the appropriate individual my request for answers to the letters I sent to the Department of Veteran Affairs on September 23, 2012 and October 3, 2012? If you need a copy of those questions, my office would be happy to provide those to you.

2. Your explanation for receiving $87,000 in bonuses was that you met the performance expectations laid out for you by your leadership—could you please provide further explanation of those expectations to my office?

3. Can you please provide information on how data security at the Department of Veteran Affairs compares with industry standards outside the federal government? Specifically, please describe the current data encryption process used by the Department of Veteran Affairs.

4. It was stated during the hearing that outside foreign agents have had access to information in the Veterans Affairs database. Could you please provide to me detailed information on who has accessed the data, the date(s) it was accessed, and what the Department of Veteran Affairs has done to prevent future compromises to the system?

Questions and Responses From: U.S. Department of Veterans Affairs

Questions for the Record from Subcommittee Chairman Mike Coffman

1. The OIG indicates that IT security has been a material weakness at VA for more than 10 years. Why did VA OI&T wait until 2012 to institute a proactive initiative like the Continuous Readiness in Information Security Program (CRISP) to try to address this issue?

VA Response: VA has been taking proactive steps to strengthen IT security for many years. Prior to 2006, information technology (IT) at the Department of Veterans Affairs (VA) was decentralized. Among other implications, this decentralization made securing the vast VA enterprise information systems, and thus ending the material weakness, virtually impossible. The lack of an ability to address the material weakness in IT was one of the primary reasons the Department, with the help of Congress, began to consolidate IT functions into the Office of Information and Technology (OIT) in 2006. As a result of IT consolidation, all governance, funding, and implementation of IT programs and security controls are managed out of VA Central Office (VACO). VA's consolidation of OIT was not completed until 2009.

After consolidation, VA managed its information security posture as an IT concern. Prior to 2012, information security was seen by some as only an IT issue. Today, VA recognizes information security is a Department-wide concern and responsibility of every single VA employee. In order to bring leadership and field-level

focus on the goal of ending the material weakness, the Continuous Readiness in Information Security Program (CRISP) was formed in 2012 under a new innovative management methodology. The CRISP effort consolidates all of the disparate material-weakness related initiatives under the leadership of one focused team across VA. Moreover, CRISP is more than just a program, but rather is a culture change to be embedded throughout the agency. CRISP is steered by VA executive leadership and executed by two OIT co-managers. This collaborative approach with senior leader oversight allowed for more consistent communication, implementation, and consolidation of tasks downstream, more accurate reporting and oversight upstream, and meant a more agile governance of the program.

2. The OIG's more recent Semiannual Report states that OI&T has 11 reports open containing 60 recommendations but can't seem to complete the actions necessary to close the recommendations?

- **For example, one report will be open for 2 years come July and yet the most significant recommendation remains open – which deals with reviewing contractor security controls and practices to ensure compliance with VA's information security requirements.**

VA Response: VA appreciates the work conducted by the Office of Inspector General (OIG) to ensure that the Department is following the correct path in working to serve Veterans. VA takes OIG's recommendations seriously, and where we concur with the recommendations, we work to implement the recommendations to OIG's satisfaction as quickly as possible.

VA's OIT acknowledges that it has several outstanding recommendations over a year old. Many of these recommendations have either been submitted to OIG for closure, or are in the process of being implemented. VA will continue to work with its OIG partners to implement and close all outstanding recommendations.

VA has furnished OIG with what it believes to be responses sufficient to close the open recommendation for its oldest reports.

3. What steps is VA taking to eliminate the IT Material weakness in FY 13?

VA Response: VA's OIT has made strides to improve its information security program. While many of the changes in fiscal year (FY)2012 were recognized by OIG during the FY 2012 audits, those changes were not in place long enough to assure auditors a permanent process had been firmly established. In FY 2013, VA focused on the four major areas of repeat material weakness findings which are: Configuration Management, Access Controls, Security Documentation, and Contingency Planning. The CRISP team and VA leadership are optimistic that the progress made from FY 2012 have been sustained, and when coupled with the early audit results this year, will show positive improvements during the remainder of FY 2013 audit results. FY 2013 also includes the introduction of a new office which focuses on patch management and baseline configuration management. While this program is new to FY 2013, it is demonstrating promise in its effectiveness.

FY 2014 continues to bring other significant changes in working towards security improvement. Some examples of major initiatives include the Department-wide implementation of a Governance, Risk, and Compliance (GRC) tool (begun in

FY 2013) which will aid in the assessments of the overall security posture within VA as well as the funding approval for a Security Information and Event Management (SIEM) tool to provide an audit log and event management oversight capability.

All of these efforts are in conjunction with VA's 18-month plan in response to OIG's Federal Information Security Management Act (FISMA) Audit. The plan, provided to OIG and part of their FISMA report, addresses each and every OIG recommendation with a plan to remediate the recommendation at various intervals, but no later than 18 months. This plan includes work to complete implementation of a risk governance structure, completion of a process for better documenting Plans of Actions and Milestones, update system security plans, finish implementing strong password requirements on all computers, continue reviewing user accounts for correct level of user access, implement a mechanism for ensuring antivirus definitions are installed and up to date, and others.

4. Why does VA have so many repeat findings and recommendations from the OIG's FISMA work? Why has VA not made any significant progress towards eliminating these long standing recommendations?

VA Response: As stated above, VA takes OIG's recommendations seriously and is working to implement the recommendations with which VA concurs as quickly as

possible, including several targeted efforts as outlined in the 18-month plan to address recommendations in OIG's FISMA report. Many of the recommendations are technical in nature and require extensive research, and detailed implementation plans spanning more than a year in order to request closure of the recommendation by OIG. All findings have remediation plans either currently in development or execution which will position VA to address OIG's FISMA recommendations.

5. What actions is VA taking to eliminate the use of clear text protocols used to transmit medical information between the VAMCs and the CBOCs over external service provider networks?

VA Response: OIT does not agree with the conclusion reached by OIG in its recent report regarding data transmission. In its final report, OIG acknowledges that VA does not send unencrypted sensitive information over the public Internet. However, VA does not agree with OIG's assertion in its final report that the manner with which VA transmits data over its network necessarily exposes sensitive data to non-VA personnel.

Although OIT does not agree with OIG's findings in the OIG final report, we concurred with the recommendation to immediately conduct a comprehensive review. The information contained in the OIG report is incorrect for the specific network links cited in Veterans Integrated Service Network 23, and is inaccurate of the network as a whole.

VA takes a defense-in-depth approach to the protection of data in flight. Encryption is being deployed at the network layer as well as means to encrypt data in flight at the application layer. The Department is already approximately two thirds done with deployment of a Transmission Control Protocol/Internet Protocol (TCP/IP) Layer 3 bulk encryption solution for wide area network (WAN) links to its major facilities including medical centers, regional offices, and data centers. This would eliminate the passing of "clear text" across those VA WAN links regardless of the use of private external service provider networks as an underlying transport. Encryption for the links to major facilities is scheduled to be completed by the end of the calendar year and the same solution is being extended to the Department's Community-Based Outpatient Clinics.

In addition to the bulk WAN encryption, there is encryption at the application layer in some instances related to the transmission of medical and other sensitive data. For terminal emulation sessions to its hospital information systems (VistA), for instance, VA uses secure shell which encrypts all traffic transmitted between the end user client and the VistA system. For the bulk transmission of VistA data, the VistA systems end user clients and other VA servers have the capability to use secure file transmission protocol which encrypts the data in flight. For other types of sensitive transmissions, VA staff and systems have standard public key infrastructure (PKI) capabilities to digitally sign and encrypt any transmissions and, for document encryption and user-based controls, VA has Rights Management Services (RMS). RMS encrypts documents regardless of where and how they are transmitted and controls how the recipient is permitted to handle the document (e.g., whether they are permitted to forward it, print it, store it, etc.). VA also uses secure socket layer and transport layer security, which encrypts sensitive http transmissions. All of these methods are in place and encrypt data transmissions independent of whether or not the underlying network is, itself, encrypted.

6. Based on the information provided in the Deloitte's deep dive report detailing inefficiencies in OI&T operations, what steps will the CIO take to improve delivery of IT services?

VA Response: VA is working hard to position its IT organization as a product and service delivery organization focused on providing quality customer service. VA asked for the Deloitte survey to be conducted specifically to help address any existing issues in order to meet the goal of improving customer service. As part of our culture of constant measurement and evaluation against goals and objectives, leadership asked for a tough and thorough analysis to evaluate the effectiveness of the Service Delivery organization.

Since the delivery of the Deloitte deep dive report, we have worked on expediting initiatives already in place designed to improve service delivery and have begun two related efforts to address customer service and communications issues. We are currently exploring ways of accelerating the implementation of the National Service Desk, which we believe will streamline and improve our efficiency in capturing issues facing our customers so they can be addressed and resolved more quickly and analyzed more comprehensively so as to enable proactive efforts to do IT preventive maintenance interventions, where necessary.

In terms of new efforts, we established a Customer Advisory Tiger Team in April 2013, comprised of members of field-based employees from the Veterans Health Administration (VHA) and OIT as recommended by the Assistant Deputy Undersecretary for Health and the Acting Assistant Secretary for Information and Technology. This tiger team is tasked to explore the impact of OIT organizational initiatives, such as the establishment of regional service lines. Recommendations resulting from the work of this committee were presented to the Acting Assistant Secretary for OIT in August 2013. In addition, we have begun an effort toward enhancing field communications and dialogue between VACO and the field through direct meetings, mostly via teleconferencing, with field leadership in the Veterans Benefits Administration (VBA) regional offices, VA medical centers, and National Cemetery Administration offices, working to identify and solve issues identified through focus group dialogues and intervention by our customer service improvement council. Using the October 2013 VA-wide customer satisfaction survey as a launching point, this program of structured interviews will identify six issues to address nationwide on a quarterly basis. The first of several quarterly reports is due at the end of this month, and the six initial issues we seek to address were identified in August 2013. The investigation process will continue with additional interviews in the next two quarters.

OIT leadership is actively working with field staff to keep communication lines open as changes to the organization are developed and implemented. The Acting Assistant Secretary for OIT conducts weekly calls with IT field leadership to keep them informed and involved in this significant initiative to transform service delivery at VA. VA will keep the committee informed after recommendations are selected for adoption and the initial set of six customer concern issues are selected for resolution.

7. How will the issuance of the PIV badge affect the ability of the Department to respond to Congressional requests, litigation demands, and other similar requests to search, decrypt and release bulk volumes of VA emails? Does the planned roll-out of the PIV badge tied to automatic encryption hinder timely responses to such requests in any way?

VA Response: The issuance and use of Personal Identity Verification (PIV) cards will improve the security posture of VA by ensuring only authorized employees have access to general information systems by requiring a higher level of assurance through using multi-factor authentication. Multi-factor authentication and hard PKI certificates associated with the PIV card will improve network access and help secure VA and Veteran's information. The use of PIV cards with hard PKI certificates to encrypt/decrypt email complicates the response to e-Discovery request. We have several efforts underway to improve our response times when dealing with emails encrypted with a hard PKI certificate, as VA understands the importance of complying with such requests.

8. Why is it that the PMAS processes only focuses on meeting milestones and schedule but there are no metrics around quality, functionality and customer satisfaction?

VA Response: The Project Management Accountability System (PMAS) is an evolving IT project development methodology and management oversight system. From the very inception of PMAS, VA leadership planned to systematically expand the scope and function of PMAS over time. PMAS was initially implemented to ensure on-time delivery of IT capabilities. PMAS' initial focus on schedule was the most impactful to reviving the IT delivery rate at VA. However, PMAS continues to evolve and now also includes quality, functionality and customer satisfaction elements.

PMAS Guide 4.0, dated November 7, 2012, establishes current PMAS policy. PMAS mandates that IT customers be engaged in the process of identifying the functionalities and capabilities that new IT projects are to deliver. Before development of a new IT project begins, as well as during the development process, the customer is intricately involved and their satisfaction is a critical element in the ability of that project to continue development. In addition, PMAS requires direct and continual participation by the customer across the entire life cycle of project development via the Integrated Project Team. Specifically, PMAS policy mandates that the Project Manager and the customer agree not only on the IT capability to be delivered, but also on the schedule by which the new IT capability is to be developed.

At the conclusion of each development period, called increments, the customer must approve of the capabilities which were delivered. Without this measure of customer satisfaction being achieved, the project cannot continue development. To deliver on time, the capability must be delivered to a production environment by the

scheduled increment delivery date, and the customer must agree that the capability meets desired functionality and schedule goals.

Recently, measuring functionality (scope) has also been added to PMAS by capturing function points delivered in an IT project's increment. Function points measure an amount of business functionality delivered by the IT system to its users. By capturing these metrics, analysis can be conducted to also measure the effectiveness and efficiency of functionality delivered to the VA enterprise.

In addition to measuring functionality, PMAS is now able to capture costs per increment by integrating data from the Budget Tracking Tool and PMAS data to achieve a cost per increment.

The PMAS program will continue to mature; the near-future will focus on: ???(1) increasing customer satisfaction by assisting the customer in determining and measuring the business value the increment delivers; (2) recognizing and verifying the progress toward achieving the customers' strategic goals and objectives; and (3) determining the quality of the code delivered to production.

9. The VA regulations on Information Security Matters at 38 CFR Part 75 appear to authorize an accelerated response with notice to the subjects of a data breach and/or an offer of credit protection services. How many times has credit protection service been offered to veterans for FY 2008–2012 and for each such instance, to how many veterans were such services offered? Please provide the annual cost for credit services for each year between FY 2008–2012.

VA Response: The following table demonstrates the number of credit monitoring offers extended by VA, and the cost to the agency.

FY	Issued	Cost
FY 2009	20,287	97,519
FY 2010	28,369	148,367
FY 2011	26,980	74,908
FY 2012	16,160	39,498
FY 2013*	11,485	25,156

*so far through July

VA has reached out to Veterans Service Organizations to help encourage Veterans who are offered credit monitoring to accept the service.

10. Under the regulations at 38 CFR Part 75, if the Secretary determines that individual notice is not warranted for a data breach, then an independent risk analysis is required to be performed. How many risk analyses have been performed in accordance with these provisions for FY 2008 to present? Please describe each occurrence of such analysis including the findings and conclusions. Please also indicate each date and instance in which a data breach was reported to OMB and/or to Congress within FY 2008 to present.

VA Response: The results of several contracted Independent Risks Analysis' (IRA) VA has conducted are below. The costs for each IRA are at least $29,000 and as much as $67,000. In 2012 alone, there were 4,724 incidents. Conducting an IRA for each incident would have cost the Government over $136 million. The costs are not justified by the results from the IRAs. Of note, VA's OIG has declined to conduct IRA's as authorized by 38 U.S.C. § 5724(a).

In order to protect our Nation's Veterans, VA uses a very low threshold for offering credit protection services when a Veteran's sensitive personal information is the subject of a data breach. All reported incidents are triaged by VA's Incident Response Team and forwarded to the Department-wide Data Breach Core Team (DBCT) to determine when credit monitoring or notification letters are required. The DBCT team performs the same function as the IRA at a much lower cost.

Additionally, the Department routinely performs other monitoring activities to ensure information is protected and has not been compromised, including conducting

quarterly generalized data breach analysis on the 20 million Veterans names in the Beneficiary Identification Record Locator Subsystem to determine if any anomalies indicating identity theft warrant intervention on behalf of the Veteran. If such anomalies are detected, individual Veterans are notified by mail. This proactive data breach analysis identifies both potential identity theft that may be the result of undetected VA data breaches and identity theft unrelated to VA experienced by the Veteran population.

1. April 2008 – An Independent Risk Analysis (IRA) was completed on an incident that involved unaccounted for IT Equipment Inventory losses across VA. A reasonable risk of harm was not found. Approximately $53,000.

2. June 2008 – An IRA was completed on an incident that involved lost CD's at VBA regional offices. A reasonable risk of harm was not found. Approximately $29,000.

3. October 2009 – An IRA was completed on an incident that involved contracted transcription services done for various facilities within VHA. A reasonable risk of harm was not found. Approximately $67,000.

4. April 2011 – An IRA was contracted regarding an OIT employee in Fayetteville, North Carolina, who was stealing identities. The contract was cancelled in September 2011, after the employee was convicted and the OIG determined the investigation was complete. Credit protection services were provided due to reasonable risk of harm.

11. By letter to the committee dated May 14, 2013, you stated: "To be clear, VA's security posture was never at risk." Please explain how this statement is true given the admissions uncovered in the hearing that systems and networks had been breached by foreign state actors and the testimony of OIG that, at one point, there were 4000 open vulnerabilities. If the statement was untrue when made (as it certainly appears), please describe what disciplinary actions is being taken for the subordinates responsible.

VA Response: As has been previously explained to the committee on July 12, 2013, this statement came in the context of a response to an inquiry on a particular topic. On April 25, 2013, VA received a letter from Congressman Coffman asking how VA will renew its "Authorizations to Operate" (ATO) various IT systems "without compromising system security." The Secretary responded to this question in a letter on May 14, 2013, outlining the ATO process and stating that through this process, "VA's security posture was never at risk." As the Acting Assistant Secretary for OIT, Mr. Stephen Warren indicated in the testimony at the June 4, 2013, Subcommittee hearing, that specific phrase in the letter was and is clearly referring to the context of the letter: The process to approve "Authorizations to Operate" did not "compromise system security." The line did not – and was not meant to—imply that normal operation of VA systems were never at risk based on other factors. Further, as you know, Mr. Warren indicated in the hearing that his office drafted that letter for the Secretary's signature and that in retrospect Mr. Warren believes he could have been more clear. Regardless, the sentence is within the context of the ATO situation and responds to Congressman Coffman's request for assurance that the process of renewing ATOs would not put VA systems at risk.

12. Reports indicate that VA became aware in January, 2013, of an incident where attackers used a spearphishing attack to gain access to a joint VA–DoD network dealing with health data. How many instances have hackers tried to use VA networks to gain access to Defense Department computer systems? Please describe each instance and what corrective actions were taken in response.

VA Response: A response to this question was provided in a briefing to Committee staff on July 12, 2013. VA is bound by agreements with outside agencies to not reveal information they report to the department in public documents or settings. This has been explained to committee staff several times.

Questions for the Record from Congressman Tim Huelskamp

1. I reiterated in my questioning during your testimony, if you could please communicate with the appropriate individual my request for answers to the letters I sent to the Department of Veteran Affairs on September 23, 2012 and October 3, 2012? If you need a copy of those questions, my office would be happy to provide those to you.

VA Response: VA provided a response to Congressman Huelskamp's October 3, 2012, letter on January 24, 2013. A response to Congressman Huelskamp's September 23, 2012, letter will be provided as soon as it is available.

2. Your explanation for receiving $87,000 in bonuses was that you met the performance expectations laid out for you by you leadership—could you please provide further explanation of those expectations to my office?

VA Response: Mr. Warren met and exceeded the performance expectations set by his supervisors. As a Senior Executive, Mr. Warren was responsible for meeting the executive core requirements of leading change, leading people, being results-driven, exercising business acumen, and building coalitions. Mr. Warren has excelled in these areas as reflected in the performance appraisals.

3. Can you please provide information on how data security at the Department of Veteran Affairs compares with industry standards outside the federal government? Specifically, please describe the current data encryption process used by the Department of Veteran Affairs.

VA Response: Effectively comparing data security at VA to industry standards largely depends on what sector of industry is being used for comparison. VA is on par with health care providers in terms of data security based on publicly available data regarding Health Insurance Portability and Accountability Act reports to the Department of Health and Human Services. VA has made great strides in encrypting laptops and desktops, having completed approximately 99.6 percent encryption of laptops and 70 percent encryption of desktops, with the remainder of desktop encryption to be completed by the end of the calendar year.

4. It was stated during the hearing that outside foreign agents have had access to information in the Veterans Affairs database. Could you please provide to me detailed information on who has accessed the data, the date(s) it was accessed, and what the Department of Veteran Affairs has done to prevent future compromises to the system?

VA Response: A response to this question was provided in a briefing to Committee staff on July 12, 2013. VA is bound by agreements with outside agencies to not reveal information they report to the department in public documents or settings. This has been explained to committee staff several times.

○