VA'S LONGSTANDING INFORMATION SECURITY WEAKNESSES CONTINUE TO ALLOW EXTENSIVE DATA MANIPULATION

HEARING

BEFORE THE

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

ONE HUNDRED THIRTEENTH CONGRESS

SECOND SESSION

TUESDAY, NOVEMBER 18, 2014

Serial No. 113–90

Printed for the use of the Committee on Veterans' Affairs

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

U.S. GOVERNMENT PUBLISHING OFFICE
96–133 WASHINGTON : 2015

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

COMMITTEE ON VETERANS' AFFAIRS

JEFF MILLER, Florida, *Chairman*

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

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

JON TOWERS, *Staff Director*
NANCY DOLAN, *Democratic Staff Director*

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

Tuesday, November 18, 2014

VA'S LONGSTANDING INFORMATION SECURITY WEAKNESSES CONTINUE TO ALLOW EXTENSIVE DATA MANIPULATION

Tuesday, November 18, 2014

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON VETERANS' AFFAIRS,
Washington, D.C.

The committee met, pursuant to notice, at 1:41 p.m., in Room 334, Cannon House Office Building, Hon. Gus M. Bilirakis [vice chairman of the committee] presiding.

Present: Representatives Lamborn, Bilirakis, Roe, Benishek, Huelskamp, Coffman, Wenstrup, Cook, Walorski, Jolly, Michaud, Brown, Takano, Brownley, Kirkpatrick, Ruiz, Kuster, O'Rourke, and Walz.

OPENING STATEMENT OF VICE CHAIRMAN GUS M. BILIRAKIS

The CHAIRMAN. The committee will come to order. Good afternoon. I want to welcome you to today's full committee hearing. For at least the last 18 months this committee has held hearings, conducting briefings and participating in discussions in a bipartisan manner. I am sure you will agree with that. The committee is seeking corrective action on longstanding issues in the VA's Office of Information and Technology.

On May 29th, 2014 the VA Office of the Inspector General noted that VA's information technology is still plagued by material weaknesses for the 16th straight year, unacceptable as far as I am concerned. Looking back nearly 18 months Mr. Warren testified to the committee that he had an 18-month plan to resolve the problems in VA's network. However, as GAO's report released yesterday tells us there are continued problems. Of great concern, VA could not provide supporting material for at least one of the serious problems it claimed to have resolved. The weaknesses in VA's network have contributed to the data manipulations related to the recent wait times scandal. Today we want to discuss these issues.

As you probably noticed, Chairman Miller is attending another congressional, he has got congressional business on the steering committee. Therefore I would like to submit his written statement for the record. Hearing no objections, so ordered.

OPENING STATEMENT OF RANKING MEMBER MICHAEL MICHAUD

The CHAIRMAN. Thank you all once again for being here. With that, I will yield to the Ranking Member Mr. Michaud for as much time, at least five minutes, thank you.

Mr. MICHAUD. Thank you very much, Mr. Chairman. As a committee we could have had a week of hearings to thoughtfully get to the bottom of the many issues that will be raised by the witnesses this afternoon. The Department of Veterans Affairs has many longstanding IT security problems, these problems that have been raised time and again by the Inspector General and the GAO. It is time that the VA address these issues quickly and effectively. Today we need to have a frank and open discussion about our expectation of VA's IT security and whether or not the VA has the resources, capabilities, and the leadership to meet these expectations. One of the biggest challenges we will discuss today is scheduling software used by the VHA. In their testimony VA indicated these problems of an antiquated scheduling system is recognized and being addressed. I look forward to hearing what VA is doing to address these problems and when we can discuss the solutions to be implemented.

I would also like to hear from VA how they are ensuring that veterans' personal data and information is uncorrupted and protected. Federal IT security laws require a balance among security, mission, and cost. We must also keep in mind that IT is not the end, but rather the means by which VA accomplishes its missions. This recognition should not blind us to the real, very real, IT security issues facing the VA. It does not, is not an excuse of ongoing security problems that should have been addressed a long time ago, but recognizing the need for balance will better enable us to figure out what the VA needs to do today and down the road.

In February the administration needs to submit a budget that gives the department all of the necessary resources to address these IT security issues once and for all. And I hope all of my colleagues here today will continue to fight to give VA those needed resources. And I hope that they will fight to ensure these resources are used properly as well. At the end of the day the American people must have confidence that VA's ability to keep veterans' data and information safe and secure and I am hopeful that today's hearing will begin that establishment of that credibility on some issues and show us that we are still able to work together.

For a number of years there has been a growing level of frustration and distrust between the VA and Congress. Within that climate we sometimes lose sight of the need to work together to deliver the promises we made to our veterans. IT security is critical and we simply must do all that we can working together to ensure that veterans' personal information is protected and that data is credible and that the VA has the tools it needs to do its job.

It is clear to me that our recent hearings and the change in VA leadership is having a positive effect. We have seen more open senior leader engagement and more responsiveness from the department and I want to thank you and appreciate all of that. I am hopeful that these changes can expand to VA and Congress working together to address IT security issues and that today's con-

versation is the first step of this process in this new environment. So I want to thank you all for coming here today. I look forward to your testimony. And I want to thank you, Mr. Chairman, for having this very important hearing. And with that I yield back the balance of my time.

[The prepared statement of Michael H. Michaud appears in the Appendix]

The CHAIRMAN. All right, very good. We will now begin with today's hearing with our first and only panel of witnesses who are already seated at the witness table. Joining us from the Department of Veterans Affairs is Mr. Stephen Warren, Executive in Charge and Chief Information Officer. Mr. Warren is accompanied by Mr. Stan Lowe, Deputy Assistant Secretary, Office of Information and Technology; and Ms. Tina Burnette, Executive Director for the Enterprise Risk Management. Joining us from the Department of Veterans Affairs Office of the Inspector General is Ms. Sondra McCauley, Deputy Assistant Inspector General for Audits and Evaluations. Ms. McCauley is accompanied by Mr. Michael Bowman, Director, Information Technology and Security Audit Office. Finally, joining us from the Government Accountability Office is Mr. Greg Wilshusen, who is the Director of Information Security Issues. Thank you all for attending today. And we will begin with our testimony and we will start with Mr. Warren. Please proceed with your testimony, thank you.

STATEMENTS OF MR. STEPHEN WARREN, EXECUTIVE IN CHARGE AND CHIEF INFORMATION OFFICER, OFFICE OF INFORMATION AND TECHNOLOGY, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY MR. STAN LOWE, DEPUTY ASSISTANT SECRETARY, OFFICE OF INFORMATION AND TECHNOLOGY, OFFICE OF INFORMATION SECURITY, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND MS. TINA BURNETTE, EXECUTIVE DIRECTOR FOR ENTERPRISE RISK MANAGEMENT, U.S. DEPARTMENT OF VETERANS AFFAIRS; MS. SONDRA MCCAULEY, DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDITS AND EVALUATIONS, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS; ACCOMPANIED BY MR. MICHAEL BOWMAN, DIRECTOR, INFORMATION TECHNOLOGY AND SECURITY AUDIT OFFICE, OFFICE OF INSPECTOR GENERAL, U.S. DEPARTMENT OF VETERANS AFFAIRS; AND MR. GREGORY WILSHUSEN, DIRECTOR OF INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE

STATEMENT OF STEPHEN WARREN

Mr. WARREN. Thank you, Chairman Bilirakis, Ranking Member Michaud, and members of the committee. Thank you for the opportunity to appear before you today to discuss the Department of Veterans Affairs and how we endeavor to find the appropriate balance between information protection and the delivery of care, services, and benefits to our nation's veterans.

Before proceeding I would like to recognize the valuable role of the Office of the Inspector General and the General Accountability Office for forming and offering insights that validate actions and ef-

forts underway, or as important identify areas where we need to improve or redouble our efforts. Though there are times when we may not agree on specific findings, conclusions, or statements, that does not diminish the great weight I give to their contributions as we take on the difficult to deal with challenges of this organization.

Securing veterans' data in an enterprise as large and as complex as VA is a dynamic and constantly involving process that includes contributions from the OIG and the GAO. I am disappointed that in spite of the significant efforts by our employees over the past year that the OIG maintained an IT material weakness. I am committed to redoubling our efforts to put in place the processes and disciplines to address these issues, building upon the extensive layered in depth strategy that we already have in place. To that end after receiving the findings from the OIG last week, I have directed an additional $60 million to be added to our information security efforts this year. This will provide additional resources to our facilities to implement configuration management as well as vulnerability remediation. In February we will reevaluate and if significant progress has not been made additional resources will be applied.

We should not overlook that VA faces the same threats as departments and many businesses. We believe we are taking responsible actions to deal with these persistent threats. My written testimony contains information on the many actions completed and significant milestones achieved in the past year. But instead of repeating that material in my oral statement I would like to highlight four key points.

First, it is important to make a distinction between issues relating to access to care and VA's information security efforts. I believe there is no causal relationship between alleged appointment manipulation and findings in the OIG's FISMA audit. To my knowledge there have been no indications that appointments were changed or canceled other than through the normal way that the software was designed to do, though in this case inappropriately.

Second, there is no disagreement that the technology underlying the current appointment scheduling system is cumbersome and outdated. Since the scheduling software was originally deployed the focus has been to add more functionality as well as correct differences in how the software worked versus the scheduling process. In hindsight, more focus should have been given to improving the usability of the tool. In summary, VA should have driven harder and earlier to replace it.

Third, it is also important to note resourcing recommendations for IT investments are made by each of the administrations based on business priorities and using those prioritized requirements we follow a consensus based process to not only develop our IT submission to the President's budget but also in developing our IT investment budget at the start of each year.

Fourth, IT risk management is a process of assembling information upon which leadership can make judgments and decisions. The identification of hazards or weaknesses in an operating environment contribute to your risk profile and have impact on its ability to achieve business objectives, but these weaknesses are but one component of assessing risks. Fundamentally managing IT risk at

VA is not just about assessing and quantifying all the things that could go wrong, but more importantly understanding all the things that need to go right for the VA to be successful. For me, finding and keeping that balance while delivering benefits and services to veterans is a personal obligation, one that motivates me to serve veterans.

The veteran for me is my grandfather, William, who was wounded in the trenches in World War I, and went on to serve in the British channel and the Mediterranean in World War II. It is my father, Steve, my father-in-law Grengel, both deceased. My brother-in-law Ted, Navy Retired. My brother Alex, Army National Guard Separated. My nephews, Michael and Duncan, presently serving on active duty. My brother Chuck, Army National Guard, killed in action, Baghdad, 2005. His widow Carol, along with his two orphans, my nephew Jackson and my niece Maddy, a niece who will never meet her father. They as well as many of the friends I served with in the Air Force shape my decisions and actions as I endeavor to find that appropriate balance of risk between information protection and the delivery of care, services, and benefits to our nation's veterans.

This concludes my oral statement. I would be happy to take your questions.

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

The CHAIRMAN. Thank you, Mr. Warren. And now I will call on Ms. McCauley for your testimony. Please proceed.

STATEMENT OF SONDRA MCCAULEY

Ms. MCCAULEY. Mr. Chairman and Members of the Committee, thank you for the opportunity to discuss the OIG's work regarding VA's management of its IT security program. With me today is Mr. Michael Bowman, Director of the OIG's IT and Security Audits Division.

Secure IT systems and networks are critical to support VA's missions of providing medical care, benefits, and services to veterans. However, for over a dozen consecutive years our independent auditors have identified VA's IT security as a material weakness. In March, 2012 VA instituted the Continuous Readiness in Information Security Program, CRISP, to ensure year-round IT monitoring and work to resolve the IT material weakness. Our fiscal year 2014 audit identified more focused VA efforts to standardize IT security controls, such as implementing predictive scanning and an IT tool for assessing, authorizing, and monitoring VA security. However, as in prior years we continue to see systemic deficiencies in four key areas.

Configuration management, we found critical systems were not timely patched and securely configured to mitigate known vulnerabilities. Access controls, we identified default passwords, weak passwords, and vulnerable third party applications providing well-known attack points from malicious users. Security management, we noted instances of outdated security management documentation, background reinvestigations not performed timely, and plans of action and milestones updated or closed without written justification. Contingency planning, we found backup tapes that

were not encrypted prior to storage and contingency plans that did not reflect the current operating environment. We continue to find these control activities were not well designed or operating effectively.

We also disclosed significant technical weaknesses in databases, servers, and network devices for transmitting sensitive information among VA medical centers, data centers, and VA central office. Particularly disconcerting were the significant number of critical and high-severity vulnerabilities at data centers more than five years old.

Moving forward VA must fully implement an enterprise information security program and improve monitoring to ensure security controls are operating as intended at all facilities. Consistent and proactive enforcement of established policies and procedures is critical to remediate IT security deficiencies across VA's dispersed portfolio of legacy applications and newly implemented systems. Effective communication between VA management and field offices is also needed to notify the appropriate personnel of identified security deficiencies so that they can timely implement corrective actions.

Our fiscal year 2014 FISMA report discussing these IT security challenges is anticipated for release in Spring, 2015. We expect that most of the 35 outstanding recommendations will remain open. However, this year VA must also address concerns not previously highlighted. These include systemic deficiencies with temporary authorizations to operate systems based on incomplete security reviews, ineffective protections for medical devices containing sensitive patient data, foreign hackers on the VA network, sensitive VA data transmitted over unsecure internet connections, and the need for an effective patient scheduling system to minimize veteran delays and ensure accurate wait time data.

In conclusion, VA has made improvements in its IT security but more remains to be done. Until a proven process is in place to ensure control enterprise-wide, the IT material weakness will stand and VA's systems and sensitive veterans' data will remain at risk. IT weaknesses and vulnerabilities can expose millions of veterans to potential loss of privacy, identity theft, and other financial crimes. Mr. Chairman, this concludes my statement. We would be happy to answer any questions you or other members of the committee may have.

[THE PREPARED STATEMENT OF SONDRA MCCAULEY APPEARS IN THE APPENDIX]

The CHAIRMAN. Thank you, Ms. McCauley. Now we will recognize Mr. Greg Wilshusen to proceed with his testimony. Thank you. You are recognized, sir.

STATEMENT OF GREG WILSHUSEN

Mr. WILSHUSEN. Mr. Chairman, Mr. Ranking Member, and members of the committee, thank you for the opportunity to testify at today's hearing on information security at the Department of Veterans Affairs. Securing its information and computing systems is vital because VA collects and maintains a large volume of sensitive personal information in performing its mission of promoting the health, welfare, and dignity of our nation's veterans. As you know,

VA has faced longstanding challenges in its efforts to secure its information and information systems. My statement today summarizes the key findings and recommendations from the report we released yesterday on VA's efforts to address previously identified security vulnerabilities. The weaknesses we reviewed pertained to the department's incident response efforts, two key web applications, and devices connected to its network.

Before I begin, Mr. Chairman, if I may, I would like to recognize several individuals who were instrumental in performing the audit work that underpins my testimony. With me today are Jennifer Franks, Tyler Mountjoy, Hal Lewis, and Chris Warweg. I would also like to recognize Jeff Knott, Naba Barkakati, Lon Chin, and Lee McCracken, who are back at the office.

Mr. Chairman, while VA has taken actions to mitigate the vulnerabilities we reviewed they were insufficient to ensure that the weaknesses were fully addressed. Although the department acted to contain and eradicate an incident detected in 2012 involving the intrusion of its network, it could not demonstrate that these actions were effective. For example, VA officials could not locate a forensic analysis report and did not retain digital evidence after 30 days, contrary to federal guidelines which call for the agencies to maintain records associated with security incidents for three years. VA also had not implemented at the time of our review a solution intended to address an underlying vulnerability that contributed to the incident. It had taken other limited actions but these were not sufficient to prevent recurrence of a similar incident. In addition the department's Network and Security Operations Center, or NSOC, did not have sufficient visibility into computer networks across the department. As a result NSOC can not be assured that the incident was fully contained and eradicated. NSOC has initiatives underway to further improve its incident response capabilities. However, it has not yet established a time frame for completing these actions.

Regarding the two key applications we reviewed as of June, 2014, VA resolved six of nine vulnerabilities that NSOC identified, including a critical vulnerability which VA corrected within one week of discovery. However, VA had not developed plans of actions and milestones for the three remaining high risk vulnerabilities, thereby diminishing assurance that it will correct these weaknesses in a timely and effective manner.

VA also has not conducted software source code scans for one of the two applications. This type of analysis can help developers identify and reduce or eliminate potential flaws. At the time of our review VA officials stated that they had drafted a policy requiring the use of these tools but it had not yet been approved.

Regarding devices on its network, VA has not always applied critical software patches within 30 days in accordance with this policy. For example as of May, 2014 VA had not implemented ten critical patches which had been available for periods ranging from four to 31 months. The patches were intended to resolve a total of 301 vulnerabilities and each one was missing on numerous devices or instances, ranging from about 9,200 instances to about 286,000 instances. In addition, VA scans for non-Windows based systems were not comprehensive because they were not performed in an au-

thenticated mode. As a result, increased risk exists that VA will not detect vulnerabilities and take steps to mitigate them.

While the department has established an organization to improve its remediation efforts it has not yet identified the specific actions, priorities, and milestones for accomplishing these tasks thereby limiting its effectiveness. In our report we made eight recommendations to assist VA in addressing these matters. The department agreed with our recommendations and stated that it had already taken actions to address six of the eight recommendations and plans to address the other two. We have not yet verified these actions to determine whether they effectively addressed the issues raised in our report. But we intend to do so as part of our normal follow up procedures.

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

[THE PREPARED STATEMENT OF GREGORY WILSHUSEN APPEARS IN THE APPENDIX]

The CHAIRMAN. Thank you very much. We appreciate it very much. Thank you all for your testimony. And I will recognize myself now for five minutes to ask questions.

We will start with Mr. Warren. As confirmed by the OIG and the recent wait times report, fake patient appointments called the ZZ test appointments were used to secure appointment times. The fake appointments made it appear as though the provider had a full appointment schedule and it prevented veterans from obtaining timely appointments. According to the emails obtained by the committee investigators there are hundreds of appointments being taken by ZZ test patients just in one VA facility alone in Portland, Oregon. To me it seems that some VA employees were deliberately and knowingly withholding care from our veterans. Inexcusable. Can you explain how the VA network allowed for this to happen?

Mr. WARREN. Sir, I am not aware of the incident you are referring to in terms of using I think you said ZZ patient as a category. Glad to take that back to the team to understand it. If folks are using false accounts or false patients to block veterans getting appointments, I find that as abhorrent as you do, sir. So we will, I will gladly take that back.

The CHAIRMAN. You are not, you are not aware of that?

Mr. WARREN. I am not aware of that, sir.

The CHAIRMAN. You are not aware of that by another title, other than ZZ patients?

Mr. WARREN. I am not aware of that but I will definitely take that back and get back to you with what we find, sir.

The CHAIRMAN. Well please get back to us as soon as possible.

Mr. WARREN. Yes, sir.

The CHAIRMAN. Thank you. Anyone else want to comment on this particular subject in the panel? Okay. Next question for Ms. McCauley. In its Phoenix report OIG explained that the VistA system audit trail was not on. The lack of audit trails limits and in some cases blocks review efforts looking for data manipulation and destruction. Did your work identify this concern in other systems and other sites?

Ms. MCCAULEY. Yes. As part of the consolidated financial statement review as well as the FISMA work that we do every year we

found that event logs were not turned on consistently. And this does pose a problem when we as auditors try to go in and do an independent assessment of a system to see the activity on the system. We need the historic data to see whether or not there was abuse of the system or any malicious intent by any users.

The CHAIRMAN. Which locations? Would you, can you tell me which locations?

Ms. MCCAULEY. I do not have that information but I could take that for the record.

The CHAIRMAN. Can you get back to us on that? I appreciate that. All right. Ms. McCauley, how effective has the Continuous Readiness and Information Security Program, CRISP, been in improving VA's information security posture?

Ms. MCCAULEY. Every year as part of our FISMA work we have seen improvements in VA's IT security. With the inception of CRISP in 2012 we have seen the institution of continuous monitoring. We have seen predictive scanning of VA networks; role-based and security awareness training for users to ensure that they understand the policies and regulations; contingency planning testing; fewer outdated background investigations; more consistent compliance with U.S. government baseline standards; as well as use of a governance, risk, and compliance tool to monitor and assess VA's IT posture. However, we are still looking at these improvements because many of them take time to mature and demonstrate their effectiveness.

The CHAIRMAN. Thank you very much. Next question is for Mr. Wilshusen. Based on the previous identified vulnerabilities that continue to exist at VA, what impact could these vulnerabilities have on allowing data manipulation of veterans' sensitive information?

Mr. WILSHUSEN. Well sir, I think they could have. They increase unnecessarily the risk that such information could be compromised. For example, the patches that had not been installed could potentially lead to increased risk that a veteran's information, including his personal information, could be affected——

The CHAIRMAN. Okay. Give us an example of some of the information that could be manipulated.

Mr. WILSHUSEN. Well this would be information that may be stored on various different work stations throughout the organization. And it could be any type of particularly sensitive information that may be maintained relative to the veterans.

The CHAIRMAN. All right, next question for Mr. Warren. Are you aware that because audit controls are sometimes inactive VA employees are able to have unauthorized access to modify or delete patient records? Are you aware of this, Mr. Warren?

Mr. WARREN. Sir, I am not aware that folks have gone in and changed records. And in fact when the audit team raised the issue to us that auditing was not turned on for the scheduling systems we turned it on. And not only did we turn it on but it reflected our history of a decentralized program where every site controlled what was turned on or off. We pulled the ability to turn it off at the local sites away from them.

The CHAIRMAN. I understand this is only for the scheduling system and not the other part of the network?

Mr. WARREN. This is for, for the scheduling system. And based upon which system you are speaking with, different systems have different levels of monitoring on them in terms of records changed or not, and different levels of logging of events that are taking place. Based upon what the GAO identified for us, we have gone back and we have raised, or if you will extended the time of how long we keep logs. Because they flagged for me a concern that we did not have material that you could see if you needed to come back and check. So we have used that input for us to improve what we are doing.

The CHAIRMAN. Okay. Does OIG want to testify on that particular subject? I would appreciate it if somebody would speak up on this.

Ms. MCCAULEY. No, I do not have much to add on that. Yet as we conducted the Phoenix wait times review we did alert OI&T that the logs were not on and they did turn them on. We also asked OI&T to discontinue removing the names of former employees from the, system and putting them rather in a disabled state so that we can do our work, our investigative work.

The CHAIRMAN. Okay, thank you. I now yield to Ranking Member Michaud. You are recognized for five minutes or so.

Mr. MICHAUD. Thank you very much, Mr. Chairman. The IG, you testified that you expect that most of the 35 recommendations to remain open in the next year's report. In this year's report the VA recommended that most of the recommendations be closed. I guess the question for the IG is can you speak to this apparent disconnect between what you are recommending and what the VA is saying?

Ms. MCCAULEY. Yes. As I stated previously, for more than a dozen years we have identified IT as a security weakness. And in our reports we have continued to find pervasive problems with information security control deficiencies across the agency. We have issued recommendations with our reports year after year and most of those recommendations have carried forth. Some of the recommendations are over five years old. In terms of the vulnerabilities we are finding that, and will be reporting for this year's FISMA report, that for the last three years the number of vulnerabilities at the critical and high severity level, they have remained pretty much constant. And so because of these as well as other control deficiencies, including access controls, configuration management controls, security management issues, and contingency planning issues, our independent auditors have determined that the IT material weakness will continue to stand until they are addressed. The OI&T has provided some information for us to close the recommendations. But based on the results of our testing and our FISMA look, we have determined that the actions are not adequate to close the material weakness.

Mr. MICHAUD. Thank you. Mr. Warren, would you address that as well? Why is there, appears to be a disconnect between what the VA is recommending and what the Inspector General has stated?

Mr. WARREN. Thank you, Ranking Member Michaud. We delivered evidentiary material to the audit team for 18 of 35 of the FISMA findings and seven of the 21 FISCAM findings. The feedback we received from the audit team was that there was not

enough evidentiary material to support that so we are going back to understand what additional documentation is necessary to support those specific findings.

We recognize, I recognize, and it is one of the reasons I applied more resources and I push on the team very, very hard, this is just the down payment, if you will, of the things that we need to do and the things that we have been doing. We are still overcoming our legacy of a large decentralized organization in terms of making sure at those 1,300 facilities everybody is complying with the standards and that we are implementing the changes that are necessary and appropriate at that time.

Mr. MICHAUD. Thank you. Can you also, Mr. Warren, tell me a little bit about the RFP process for the new scheduling software? What are the key requirements? Is there a provision for self-scheduling capabilities within that?

Mr. WARREN. Yes, sir. The RFP to replace the existing scheduling software, and again it is one of three parallel paths but let me just talk about the replacement. That RFP is supposed to be on the street this Friday. I got a note from the acquisition community guaranteeing that, or promising that this morning everything is on track that we will be on the street with that this coming Friday. Key aspects of this acquisition is we are buying a commercial product, recognition that capability to do scheduling exists today. So key point, commercial product. Second key point is we did full and open. So instead of just doing, having vendors who have a relationship with the federal government being able to compete, we opened it up for all vendors. Anybody who has provided that type of capability, we wanted them to come to the table. Also key is we are running a two-step process. We are asking for folks to bid, a written response to the things being asked in terms of capabilities. We will down select and then we will go to a demo period in terms of having the vendor show the capability. And the evaluators will include schedulers from the sites because we want to make sure the tool will meet their need. So once that comes in, we expect to award that contract end of March, no later than end of March. And then we are going to be on six-month cycles dropping capability out to the sites as we bring on what is needed.

With respect to veteran self-scheduling, we have a parallel path for that to bring online an app that will allow veterans first to request an appointment and then build on it such that they actually can schedule an appointment. And we are making sure we synchronize that mobile app with whatever that final commercial product is.

Mr. MICHAUD. And does that address security issues and would deter improper data manipulation as well?

Mr. WARREN. Sir, we have built into the requirement that logging needs to be there. But by definition a scheduling piece of software allows the changing and cancelling of appointments. So making sure the logging is on, the audit trail is on, will allow teams to look for unusual patterns of cancellations or changes. So that is built into the requirement, to have that type of auditing and logging on it so if that type of behavior happens folks can see it and take the appropriate action.

Mr. MICHAUD. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you. Now I will recognize Mr. Lamborn for five minutes.

Mr. LAMBORN. Thank you, Mr. Chairman. Mr. Warren, one of the concerns I have with the VA's ability to safeguard our veterans' personal information is the fact that there are no user based restrictions in place in VistA that would ensure that employees only have access to the information that their job positions call for. Now given reports of unauthorized access and zeroing out of appointments, do current systems create an auditable log that shows who accessed specific data or made a scheduling change? I know we already touched on that some but I want a full answer on that.

Mr. WARREN. Sir, there is, there are two categories of applications that are in use within the VistA constellation or universe today. The majority of them actually log if, when a person accesses a particular thing or makes a change. There is a second class of tools that started to be introduced in 2006 that we are slowly transferring out that actually do not carry the appropriate log on it. So the majority of cases it is flagged and it is logged. But there are certain pieces of software where those logging and control does not take place.

Mr. LAMBORN. How soon will you be at the point where only the system administrator can turn off the logging aspect?

Mr. WARREN. So for logging, which is running on a parallel track, we have actually pulled back the ability for folks locally to change logging. So now you cannot do it locally. It has to be done nationally based upon the observations that the audit team gave us that was specific to scheduling. I will go back and confirm for the other modules if we have done the same thing in terms of pulling that authority back. But I will bring that back for the record, sir.

Mr. LAMBORN. Yes, and if you could bring that back for the record, thank you.

Mr. WARREN. Yes, sir.

Mr. LAMBORN. Mr. Wilshusen, you state in your report that the VA said that they were doing six of the eight recommendations but there were two that were not satisfactorily addressed. Which two were those?

Mr. WILSHUSEN. Well those were actually two recommendations that they still plan to address. It is not that they disagreed with our recommendations——

Mr. LAMBORN. Okay.

Mr. WILSHUSEN [continuing]. But they still plan to do those.

Mr. LAMBORN. And which two are those?

Mr. WILSHUSEN. Those particular recommendations, let me just check first.

Mr. LAMBORN. And I am looking at page five and six of the latest GAO report.

Mr. WILSHUSEN. Right. The——

Mr. LAMBORN. Or Mr. Warren, could you——

Mr. WILSHUSEN. Yes, I will have to get back——

Mr. LAMBORN [continuing]. Can you jump in on this, Mr. Warren?

Mr. WARREN. Yes, sir. The two areas where we did not ask for closure because more work needed to be done is on the time frames for completing initiatives to improve an incident response capa-

bility. It actually is a follow up from another GAO report, where we are putting in the notifications as well as the follow up actions that are required not only for the incident teams at the NSOC but as we cascaded down into the sites. The second area, which is a harder challenge for us from a technical standpoint, was referred to in the opening remarks and it deals with scanning non-Windows based systems. Because of the way those systems are designed it is not easily able to scan them from a central location. So we have reached out to our vendors who provide those systems and asked them how can we roll the accounts up into a centralized area such that we can do the types of scans being asked for us. So those two are open because we still have work to do on those.

Mr. WILSHUSEN. And that is correct.

Mr. LAMBORN. And Mr. Wilshusen, what is your response to their stated intention on those two unresolved areas?

Mr. WILSHUSEN. Well if they address the areas and implement those actions effectively then that could address the intent of our recommendation and hopefully will mitigate part of the weakness. It is something we will follow up on as part of our audit follow up process, to determine the effectiveness of their actions once taken.

Mr. LAMBORN. Okay, thank you all for your answers and for being here. Mr. Chairman, I yield back.

The CHAIRMAN. Thank you. I appreciate it. Now we will recognize Mr. Takano for five minutes.

Mr. TAKANO. Thank you, Mr. Chairman. Mr. Warren, the Inspector General found that the, "VA specific guidance for integrating security into the budgeting process does not exist." In light of this, does the VA have a clear picture of what the ultimate costs are for the scheduling software and VistA modernization efforts? And whether or not security is being properly integrated into the budgeting process for these efforts?

Mr. WARREN. Thank you for that question, Congressman Takano. There is actually three pieces, if I can hit those.

Mr. TAKANO. Okay.

Mr. WARREN. The first one deals with how do we lay out the guidance and instructions to the organization to plan for security as part of any investments or operating costs? That change was implemented as part of the fiscal year 2015 execution budget and the 2016 planning budget, the budget that Mr. Chairman referred to showing up in February. So put it in place, build it into how we do that. With respect to VistA evolution, one of the key aspects of VistA evolution, part of the architectural change in referring to Mr. Lamborn's question earlier, that architectural change to make sure all components within the VistA constellation actually audit appropriately are part of VistA evolution. So we have built in security into the architecture. We have also just moved out and we have reached to a third party to come in and do an architectural review of VistA evolution and we are also reaching out to the open source community to have them look at what our designs are going forward to make sure we have not missed anything. The third one I believe was on VBMS, unless I missed that piece, sir. That is actually built into the original design and there are very, very stringent access controls within VBMS because it is a new software and we were able to build it in from the start. Security was key in today's

era, security was key in the last five years. More than five years ago, security was not necessarily a key design criteria when we were delivering a new product. And the whole industry is actually dealing with that change, sir.

Mr. TAKANO. So I just want to repeat, do we have a clear understanding of what the ultimate costs are going to be?

Mr. WARREN. For information protection, I have a budget that is laid out for 2015. Intent had been to clear the material weakness, 2014. We fell short. Again, why I applied more resources on top of what was already budgeted for 2015. We identified areas where we needed to do more, we needed to do different. So brought in more resources to take that on. We have that as a base program going through into 2017 and 2018. So we expect to continue that same level of resourcing. It is sitting at about $160 million to $180 million. But that does not include the staffing. So again, if you look at my workforce I have approximately 5,500 employees who are out in the field. Security is half of their job, day to day. So that is an additional $300 million a year in salary costs on top of that. So I have a pretty good sense of what the costs are to deal with the issues identified. But recognizing that the threat keeps evolving and we are going to keep adjusting what we need to bring in in case there are surprises that come out or, again, as the, our partners the auditors identify, you missed it here and you may think something at headquarters is happening right. But out in the field it is not, you need to go in and redouble your efforts in those areas.

Mr. TAKANO. Can you, can you elaborate a little bit more on this open source community? And how that may, is or is not an advantage of the VistA system, which I understand is owned by the VA?

Mr. WARREN. The VistA system is a government owned product. It was developed with tax dollars. What we recognized about three years ago is there was actually a community of medical centers and organizations that were using VistA as part of care delivery outside of the VA. In fact, Indian Health Service is based upon a VistA variant.

Mr. TAKANO. So these are entities outside the VA?

Mr. WARREN. Outside of the VA and——

Mr. TAKANO. How extensive is this, are these entities? I mean, just I want to get a sense of the size of these communities.

Mr. WARREN. It is worldwide. I believe the country of Norway uses VistA as their healthcare delivery system.

Mr. TAKANO. Oh, really?

Mr. WARREN. We have engagement with Jordan, where they are actually converting to VistA as their primary system. We will gladly get you back for the record a map and a list of all of the local communities——

Mr. TAKANO. I would like to get a clear picture. Because I, it is one of the things that we are——

Mr. WARREN. Glad to.

Mr. TAKANO [continuing]. Of course this integration with DoD and even future integration with non-VA providers, understanding VistA and its, and its advantages and shortcomings is really going to be important to me as far as, since it is a wholly owned piece of property by the federal government.

Mr. WARREN. And we have actually placed it out there. Because the challenge we had in the past was for individuals to use VistA code they had to do a Freedom of Information Act Request.

Mr. TAKANO. Yes.

Mr. WARREN. So all kinds of process you had to go through. So the reason we established and supported that open source community was to remove that burden from people taking VistA and using it. So it is out there and folks are using the code and maturing the code as they go forward.

Mr. TAKANO. My time has run out but I would like to explore more about this open source nature of this, of this software.

Mr. WARREN. Glad to, sir.

Mr. TAKANO. Mr. Chairman, I yield back.

The CHAIRMAN. Thank you, Mr. Takano. And what we will do is maybe after this first round if anyone else has any additional questions——

Mr. TAKANO. Sure. Thank you.

The CHAIRMAN [continuing]. I will give you the opportunity.

Mr. TAKANO. I appreciate that.

The CHAIRMAN. Thank you. Dr. Roe, you are recognized for five minutes.

Dr. ROE. I thank the chairman. And if you would indulge me for just a minute, I do not know whether this will be the last time I have an opportunity to serve with the Ranking Member Mike Michaud. But Mike and I have served on this committee together for six years, and my entire time in Congress. I have gone to Afghanistan with Mike. I think he truly has the veterans' best interest at heart. He has worked in a very bipartisan way. And I would just like to take this opportunity personally, Mike, to thank you for your service.

[Applause.]

Dr. ROE. I sincerely mean that. And it will be a real loss to our committee and I look forward to continuing our friendship once you leave the U.S. Congress. And again, thank you for your service. And Mr. Warren, thank you and your family for your service to the country. And my heart goes out to you for your loss. I share that as a fellow veteran and I want to thank you for your, your family is a true patriotic family so thank you for your service to our country.

You know, I have a hard enough time turning on a PDA, okay? So some of this is going over my head, past my head, or whatever. Just for a simple technologically challenged fellow like myself, could you tell me what a material weakness is? And the reason I bring that up is because if you look in a hospital, where I practiced, and a nurse gives somebody one Tylenol instead of two, that is a drug, a medication error. It goes down as a medication error but it really does not hurt anything. Are these things significant that you talk about in material weakness? And would it cause a significant problem or glitch if this were to not be addressed? And anybody can touch base on that.

Mr. WARREN. Sir, if I could it is—why don't you go ahead since it comes out of the audit community, and if I could follow up.

Ms. MCCAULEY. Yes. The IG declared information security a material weakness as part of its consolidated financial statement au-

dits. Annually we are required to review the consolidated financial statements for their accuracy as well as to examine the financial systems that support them to make sure that there is no material misstatement in the statements. And as part of that we found out that there were the weaknesses in the systems that support the financial transactions of the department. There are several levels or categories of weakness, or we say risk, and the material weakness is the highest of them. There are also significant deficiencies. And there is a dollar threshold associated with that material weakness as well. And so based on the pervasive problems across the department we have ascribed material weakness to information security because there are so many risks involved.

Dr. ROE. So if it is not addressed a significant occurrence could happen? A breach could occur?

Ms. MCCAULEY. Exactly. We are looking at it from a risk standpoint.

Dr. ROE. Risk standpoint. I think the question, Mr. Warren, for you, and when you begin to get the scheduling system. And I can assure you, I hope the scheduling system works better than the one they have now because it is terrible now. I get complaints about it all the time and I hope that it is not punch one, two, three, four, and then you start all over again. The airlines do it very well right now. Quite frankly you can book an airline flight and your seat on the airplane and so forth. Once this gets started, how long will it take to ramp it up where it is actually functional?

Mr. WARREN. So two items, if I may. The first one to deal with the difficulty in accessing the screen. So instead of just waiting for the replacement of the software we actually put on contract in August, we get the first delivery coming in in December, January, which is to take in the existing system all of those separate screens and pull them into a single screen so it is easy for them to use. So we wanted to make sure we did the replacement right but we also wanted to get relief to the scheduler. So there would be reason not to get that scheduler done right and no reason not to make sure those right items are there. So relief on the way for the schedulers to make sure they have that usability to deal with the difficulty of it.

With respect to the replacement for the existing system, right now the, again we are laying a timeline with some assumptions about the number of bidders. We are expecting to go through the two-step process and award by March. So end of March, no later than. So we are pushing very, very aggressive on this for something that is an open competition. So a lot folks are, not cutting corners, but streamlining every darn thing we can.

We are, we have laid out notionally, we are saying we want six-month deliveries. So four deliveries so we can make sure as soon as we can we are using that commercial product. So we are not asking for somebody to build us a new scheduling——

Dr. ROE. So by the end of 2015 maybe it is ramped up?

Mr. WARREN. We are expecting to get capability online in 2015, starting it, and then basically rolling it out in phases across the complex as well as adding capability to it over that two-year period.

Dr. ROE. Okay. So a couple of years. Okay. That makes sense. And one other thing. We go to many classified briefings and some

of those I think concern veterans' records and the amount of foreign entities that may be hacking those records. Are you able to identify that when that is happening? Is the system secure enough to keep a foreign entity from putting malware on something that is then backdooring into another system?

Mr. WARREN. Sir, we actually do not care where it comes from. If somebody is trying to come after veterans' records, that is what we are interested in. And the way the system is set up, and we start from the outside with Homeland Security. They have Einstein 3 which basically covers our back and maintains the perimeter. So scanning on their end. We also work our way inward in terms of at our boundaries and multiple locations. One of the things that the IG identified for us as part of the audit, there were a couple of areas where we had blind spots. And so we are moving out and filling those blind spots. But we track all traffic coming in and all traffic going out through four key points. So all traffic is gated and then monitored as it is coming in and leaving the perimeter. So we believe we have pretty good visibility. Because we know malware will end up on desktops. Right? Folks click on the stupidest emails, that human condition, whatever it is, that causes you to want to see some picture or some thing—sir, please do not, it is not good. But we know that is going to happen. So the protections that are in place and the multilayers that are in place is to deal with folks doing bad things. Because I cannot stop them from going to the internet because it is pervasive in how we do our business.

Dr. ROE. I thank you and I yield back.

The CHAIRMAN. Thank you. Now Ms. Brownley, you are recognized for five minutes.

Ms. BROWNLEY. Thank you, Mr. Chairman. Mr. Warren, I just wanted to follow up again on, I am glad to hear that your, the RFP is going out for this new system, and you seem to be on track with that. You mentioned the self-scheduling solution. And is that going to be part of this RFP that you are speaking of that is going to happen this Friday, I think I heard you say?

Mr. WARREN. Ma'am, we actually are running parallel—I am going to lean over so I can——

Ms. BROWNLEY. I know, we have to look across.

Mr. WARREN. We are actually running on parallel tracks. So it is one of the options that is on the commercial product we are asking for. The second piece is we actually doing development for an app in terms of figuring out can we provide that and we would do it in as a two-step. The first step would be for veterans to ask for an appointment, so it does not have that deep connection in and make the changes. I do not know if we have briefed the complexity of it. We actually pull information from 71 systems when you actually try to schedule and then you have to send information back out to another 41. So basically two-phased. First phase to allow it to ask for an appointment. So it would get to a scheduler and they would work it. And then phase two is to make the connections so they actually could see what the availability was and start doing that negotiation online. And that is, that is probably a year and a bit out to get that full functionality. Because it is not a trivial thing to do and we want to make sure we do it right.

Ms. BROWNLEY. Okay. It seems to me that it is, and again like Dr. Roe I am not a master of IT issues at all. But it seems to me that, I mean there are apps out there in the private industry now for self-scheduling. It seems to me like it would be rather simple, particularly when we have the issues of canceled appointments, etcetera, and being able to, you know, use every single day efficiently and making sure that each one of those appointments are full, that it seems like it is a pretty easy process as opposed to a complex one.

Mr. WARREN. So the fact that the marketplace has matured to the point where folks can do schedulings online and those tools are out there is what drove us to buying a commercial product. So many years ago when this was tried before it was there was nothing out there, the market was not mature, we had to build it ourselves. The recognition and the America COMPETES Act that we did two years ago, the competition, again validated yes there were commercial products that were ready to be done. And we were also able to validate how you test it and prove it. Because the challenge for us is not that commercial product but how do we make sure when it connects into all of the existing capabilities that it does it right? Because when we schedule it is more than just the patient available, the veteran, it is the clinician, it is the room, it is the equipment, it is the assistance, it is the consumable products that need to be used. So we want to make sure we do that right. But we are building, if you will, we are counting on the fact that yes, that capability exists out there today and you are able to do those. Now we have to do the hard part as the vendor bring it in and the connections and making sure those connections work correctly.

Ms. BROWNLEY. And so when is the timeframe for completion of all of that?

Mr. WARREN. So the RFP for the replacement of the system goes out by this Friday.

Ms. BROWNLEY. Yes.

Mr. WARREN. We were trying to pull it in a little bit earlier but this Friday is a guaranteed it will be out.

Ms. BROWNLEY. Yes.

Mr. WARREN. We expect it, because it is a two-step, making sure that we have schedulers as part of the evaluation process, award of the contract by the end of March. And then what we are asking for is four six-month deliveries of capability. So in other words, all the things you need to do to schedule are many. It is more than just an appointment. We also want to figure out how we bring in televideo scheduling into it.

Ms. BROWNLEY. Yes, I am just talking about the, you know, the potential of having an app, a veteran on their phone, have an app, and be able to make their own appointment.

Mr. WARREN. So the app for a veteran to ask for an appointment is supposed to come out in 2015.

Ms. BROWNLEY. In 2015?

Mr. WARREN. So that is what is laid out. And that is separate from the replacement of the existing scheduling system. But glad to, for the record, lay out the schedule of those critical components. We have come up and briefed the staff with the detail but glad to bring another copy up with an update, ma'am.

Ms. BROWNLEY. Thank you very much. And I might not have time but I will at least get the question out. It seems to me in reviewing the total number of security incidents as reported across all federal agencies, the total number of security incidents reported at the VA is less. It is clear that the VA has a greater problem with non-cyber incidences. And so I guess my question really is, you know, what is the VA doing around non-cyber? You know, paper flow, paper information, hard copies, and so forth with regards to security training programs and, and other mitigations to address that?

Mr. WARREN. Mr. Chairman, can I answer?

The CHAIRMAN. Yes.

Mr. WARREN. So if I could I would like to use this as an opportunity, something that we have been doing is we have been doing a monthly report. It has been in tabular form so this is everything that happens in a month. But what we did this past month is it is so hard to read this table we actually turned it into a chart. And to your point, ma'am, our incidents where we have fallen short have been in people and process steps, where folks did the wrong thing. They sent the wrong paper to the wrong person, or they downloaded the information and lost control of it. What we do with those incidences, it is part of our data breach core team. Anytime where there is the potential that a veteran's information was put at risk, and in the past month it was 536 times in October, we fell short of our responsibilities. Each of those veterans received credit monitoring. We also went back into the leadership chain to the organization where the failure took place and we identify was it a process failure? Was it a people failure? Was it an organizational failure? And we leave it to their chain to make the appropriate corrective actions. We build it into our annual training, so we look at what happened in the prior year. And every employee and contractor working with the VA is required to take security training before they can use systems. And we refresh that to point out do not do this, do not do that, look out for this, be aware of that.

Ms. BROWNLEY. Thank you. And thank you, Mr. Chairman, for your indulgence.

The CHAIRMAN. How long has this been in place?

Mr. WARREN. Sir, the actual tabular reporting has been out there for at least three years, if not four. But the, it has been hard to understand. And so as part of our transparency is how do we put it into an info graphic so it really lays out what is the threat and where have we fallen short? Because we think it is important for that to be visible and folks to be aware.

The CHAIRMAN. Thank you. Dr. Benishek, you are recognized for five minutes.

Dr. BENISHEK. All right, thank you, Mr. Chairman. I have a question concerning the VistA program and your answer to Mr. Lamborn. As I understand it there is audits. You are not sure if the audits are taking place in all areas of VistA?

Mr. WARREN. So what I asked was to be able to go back and confirm for which systems what auditing is turned on at what level. For scheduling I know it is turned on.

Dr. BENISHEK. Well why, do you not know, do you not know that answer?

Mr. WARREN. Sir, I did not come prepared with that answer at my fingertips but I will be glad——

Dr. BENISHEK. Well how many different parts of VistA are there?

Mr. WARREN. I believe the reports vary between 86 to 128 different modules or applications.

Dr. BENISHEK. So like the patient, but it is all patient data, right?

Mr. WARREN. Patient data and where the data is held is actually a very small component of VistA.

Dr. BENISHEK. Well I guess I do not understand why these audits are not in place. Why can somebody get access to a record without a record of them accessing it? Any case?

Mr. WARREN. So for the majority of applications that individuals use to access veterans' data or to do actions that result in veterans' data, the majority of those there is logging of who accessed the data and what they did and what data was changed. For a couple of applications starting in 2006 a particular tool was used to deploy that software. It does not have the appropriate auditing in place. We are working through to actually replace all of that software.

Dr. BENISHEK. All right. As I understand it there was like eight major areas that were addressed by the GAO and the IG and you have addressed six of the eight but the other two areas were not addressed. Is that right, Mr. Wilshusen? Is that the testimony?

Mr. WILSHUSEN. No, it is not that they were not addressed. VA responded that it concurred with all eight of our recommendations and that it had already taken actions to implement six of those recommendations and that it plans to perform actions to complete the other two recommendations.

Dr. BENISHEK. And how long has it been now since that came out?

Mr. WILSHUSEN. Well the report just came out, was issued on November 13th and we released it yesterday. But we had briefed VA on our recommended actions and activities before then.

Dr. BENISHEK. So there is a plan, then, Mr. Warren to respond?

Mr. WARREN. Yes, sir. For the eight items identified, six of those actions either underway or actions we needed to change. Two of them it took more work, so we are not able to come in and say we believe we have things underway to ask for closure. Two of them took more work and will take more work, one of which needs time, the other one trying to deal with the technical challenge in terms of how do we do what the audit, what GAO asked us to do.

Dr. BENISHEK. All right. I still am somewhat concerned about this, this access to data issue. You know, I worked at the VA and I have seen data change in the system without adequate explanation why it occurred. And you know, that is a very concern to me especially in view of the fact that there is risk of foreign entities accessing the data. Is that not occurring today? Has that patch been done?

Mr. WARREN. Sir, if you have a specific instance where data changed, and it was somebody you were seeing, and you have a question about why it changed, definitely ask. Because we can——

Dr. BENISHEK. Well no, I did that at the time but I did not get an answer.

Mr. WARREN. And when was that, sir?

Dr. BENISHEK. That was before I came here. It would have been prior to 2011. But you know, a chart changed. And there was no, there was no, I mean it was a pathology report that initially was benign and then came back malignant with no evidence of anybody changing it except for the fact that I had told the patient that the path report was benign, and then when it came back the next time I had to tell him that the path report was malignant because it, and I did not have a piece of paper to document the fact that it was benign before. So it made me look bad.

Mr. WARREN. Sir, I would——

Dr. BENISHEK. Do you understand what I am saying?

Mr. WARREN. Yes, sir. I would——

Dr. BENISHEK. And that is the kind of stuff that I am concerned about, especially if there is foreign access. Now the IG and the GAO, is there a possibility for foreign access to the VA system at this time?

Mr. WILSHUSEN. Well with respect to foreign access let me just say in terms of external access——

Dr. BENISHEK. Okay.

Mr. WILSHUSEN [continuing]. Regardless of the source, the findings that we identified are vulnerabilities in VA systems that have not yet been——

Dr. BENISHEK. At this time.

Mr. WILSHUSEN [continuing]. Corrected including ten critical patches that address up to 301 vulnerabilities. So the risk, is unnecessarily increased that unauthorized access could occur.

Dr. BENISHEK. Is it still present today?

Mr. WILSHUSEN. Yes. As far as when we did our review in, as of June, 2014, those vulnerabilities had not been addressed.

Dr. BENISHEK. All right. Mr. Warren, do you have any answer to that? What are we going to do about that with the 5,500 employees that you have?

Mr. WARREN. So managing vulnerabilities and particular patching of software. So that is one of the most dynamic parts of the job. If I can set aside the group that the IG identified for us that our financial system is out of date and the software actually cannot be patched. So that software cannot be patched, will not be patched, without breaking the finance systems at the VA. So we have compensating controls around that to put increased protections in place while we do it. For systems that exist outside of that pool, if I can. We have a very active if you will prioritization in terms of what we patch when and why. We count a lot on the fact that we have multiple layers of defenses on top of it. There is a balance between patching something, testing something before you patch it, because we have had instances in the past where the manufacturer sends us the patch, we push it out to the site, and we bring the site down. Because the software that runs on top of those work stations or servers run differently than how the vendor expected them to act. So we are always working a list of criticals, to highs, to mediums.

Dr. BENISHEK. But—all right.

Mr. WARREN. And again, we run a punch list. We deal with the highs, I am sorry, we deal with the criticals and then we work—I am sorry, sir.

Dr. BENISHEK. Sorry, my time is up.

The CHAIRMAN. No, that is okay. Thank you, doctor. Yes, I want to ask OIG, Ms. McCauley, do foreign entities have the ability to enter the network?

Ms. MCCAULEY. We certainly continue to have concerns in that regard. I would like to ask Mr. Bowman to address that question, if I may?

The CHAIRMAN. You are recognized, sir.

Mr. BOWMAN. Every year we identify access control issues, configuration management issues, well known vulnerabilities. And these are all attack points by foreign nation states. So that possibility, that threat still exists. And once inside the VA network, such as the case where domain control was infiltrated, they can use that as a pivot point to laterally move throughout the VA network. So that threat still exists and we continue to identify vulnerabilities that need to be addressed.

The CHAIRMAN. Thank you. I would like to recognize Ms. Kirkpatrick for five minutes.

Ms. KIRKPATRICK. Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Ms. KIRKPATRICK. Let me first add to Dr. Roe's comments and thank our Ranking Member Mr. Michaud for your leadership. You have been a dedicated public servant, committed to our veterans, and it has just been an absolute pleasure serving under your leadership. And I really appreciate the bipartisan way that you have worked with the chairman and with the committee, making this one of the most productive committees in Congress. So thank you for that, and I wish you the very best in your future endeavors. And I hope you will stay in touch, so thank you.

The CHAIRMAN. I will second that.

Ms. KIRKPATRICK. Thank you.

The CHAIRMAN. We will not count that time against you, either.

Ms. KIRKPATRICK. Oh, okay. Well I will be brief, Mr. Chairman. I am glad to hear that you are looking at a commercial off the shelf version of the scheduling software. But did you do a cost benefit analysis between the cost and benefit of doing that versus continuing to invest in the VistA program and patch that and reform that VistA program?

Mr. WARREN. Looking at what the projected costs were for building inside versus outside was something that was evaluated. And when we looked at it there was a recognition that we could get to a solution faster, which was one of our driving goals, instead of us having to try and build it in house. And just to revisit history, and again it is an ugly history for us, from 1999 to 2009 the department tried for ten years to build a scheduling software package. In 2009 we killed that program. I was part of the team that said stop wasting the dollars, kill this program. That was a serious contribution to when we sat down and asked do we want to try this again and try and build something? Or do we use what already exists in the marketplace? And what drove us to it was it is there, it works, it is viable. Let us build on that instead of trying to do something that we have proven we could not do, specifically with scheduling.

Ms. KIRKPATRICK. How close are we to having VistA be interoperable with the Department of Defense system and with this new off the shelf scheduling system? Will they be interoperable?

Mr. WARREN. So if I could I would like to offer in for the record, I brought in a four-slide deck and a copy for the ranking member and the chairman and yourself, if you would like. Glad to hand it up. I do not know how to do that. It actually walks through how interoperability is happening. So I believe we have—we do not have copies. I will give you my copy, glad to give you my copy. And what it does is it lays out how data is flowing today. And too often we talk about interoperability as something that requires VA and DoD to use the same system. I do not know how we do this. Glad to give you that, ma'am, and we will get other copies up for the record.

Ms. KIRKPATRICK. Thank you.

Mr. WARREN. And what it does it lays out how data is flowing in four areas. The first one is between VA and DoD. And we actually move it first bidirectional. So if we have veterans or servicemembers that are seeing care between the two locations, we are moving that data back and forth today, irrespective of what system we use. For servicemembers who separate their medical record transfers over within 30 days and it comes into the VA system and it is available if a veteran ex-servicemember presents himself for care. Otherwise, we do not see it. It is there. The third area is polytrauma. As soon as a servicemember transfers to us the whole record comes over. That is how we move data back and forth in the existing system. Hard to see, it is in a panel somewhere else. JANUS, we have talked about this integrated viewer. We now see this data in a single view. Not just VA and DoD data, but all of the VA data. In the past when a veteran went to three medical centers you had to look at three places. Today you see it together in one place. The third area covered in that deck lays out the interoperability with third party providers. A lot of DoD care is done out in the private sector. With the Veterans Access to Care and Accountability Act, $10 billion of care is going to happen over the next couple of years. What record we use or DoD use has no effect on that data coming in. So laying out where, exchanges where we have got relationships, I believe it is 28 organizations where we move data back and forth between the two. And then also where they do not have the ability to view back and forth, the secure transfer of data. We have nine relationships with those and again that is in that four-page deck. And the last one, it was a key commitment we made which was break the medical record free from the institution, the personal health record that a veteran can download and use. And it lays out all of the downloads and all of the capabilities that we put out there for veterans to take their record and go with it if they want to do it physically, or how through My HealtheVet they can see their information, how they can ask for renewals of medications, and how they can do secure messaging with their clinician, with their care provider if they have any questions.

Ms. KIRKPATRICK. And are you saying that capability is available now?

Mr. WARREN. That capability is there. And hopefully, I am not sure where those four slides went, it lays out, we have been work-

ing very hard on how do we clearly lay that out? We have had a difficulty in saying this is how we do it. And hopefully that information of use and glad to sit down with any member and go through it, whether yourselves, with the staff, to talk about the great progress I think we have made in moving that data between not only us and DoD but also with those third party providers. That is where the key risk for us in the future is.

Ms. KIRKPATRICK. Yes.

Mr. WARREN. Because we are moving that care out. So how do we get the data back and make sure it is used as part of the care?

Ms. KIRKPATRICK. Right. Well I look forward to the slides. And let me just conclude saying I would like to get the, a copy of the map that you were talking with Mr. Takano about——

Mr. WARREN. Yes, ma'am.

Ms. KIRKPATRICK [continuing]. That shows the different places that VistA is used.

Mr. WARREN. I will be glad to submit it for the record with not just in the U.S. but worldwide where VistA is used.

Ms. KIRKPATRICK. Thank you.

Mr. WARREN. Yes, ma'am.

Ms. KIRKPATRICK. Thank you. I yield back.

The CHAIRMAN. Thank you. Mr. Huelskamp, you are recognized for five minutes.

Dr. HUELSKAMP. Thank you, Mr. Chairman. I just want to follow up and clarify something with Mr. Warren. If I understand it correctly publicly you just said that no data has been exfiltrated as a result of attacks from the VA network?

Mr. WARREN. Let me go back and be very clear to your question, sir. We have two instances that the team has identified going back to 2010, 2010 and 2012. It was the point of the hearing that we had 18 months ago. In those instances what the forensics team has identified for us is user name and password files were pulled from the enterprise. So that data came out, not veteran data. As soon as that was identified we went in, we cleaned the systems, and we reset the passwords. On Friday, and because this question comes up and it is a concern not just external but internal, we actually asked an organization called Mandiant, I think you have probably heard of them. We asked them to come in and look at those domain controllers. Because if there is a question we want to make sure it is more than just my team saying they are clean. Friday they briefed us and said they are not seeing anything on those domain controllers. Preliminary report, they will have a final report by December. We will bring that report up and brief yourself, the staff, the members, and have Mandiant there to do it, which basically says "they are clean".

Dr. HUELSKAMP. So within the timeframe since 2010 you have no knowledge that data has been exfiltrated out of the VA network?

Mr. WARREN. Sir, I have been briefed by my team of two instances where specific data was removed, usernames and passwords.

Dr. HUELSKAMP. And that happened when?

Mr. WARREN. 2010 and 2012. We briefed the staff, glad to come up and do that again, sir.

Dr. HUELSKAMP. And according to, I mean you make reference to the committee hearing, a subcommittee hearing, numerous I thought very reliable whistleblowers, they said the information removed from the network was encrypted. So and I thought the VA agreed they did not know what data was taken outside the network. But now you do know what data was exfiltrated out of the network?

Mr. WARREN. What the team did is, and because there are always unknowns, they looked at patterns and signatures in terms of what did it look like. And what the team gave back and briefed me, and we asked again and again, was they had reasonable confidence that the information that was removed from the VA was a file, the type of file that looks like what you——

Dr. HUELSKAMP. So let me interrupt because I want to go inside the network. So it was not encrypted? Or it was?

Mr. WARREN. No sir, it was encrypted.

Dr. HUELSKAMP. It was encrypted, and you broke the encryption so you know what the data was? You did not?

Mr. WARREN. No, the team identified how the file looked and what it looked like and where it came from, and said "it has the shape and characteristics of that particular type of material."

Dr. HUELSKAMP. Which allowed access throughout the network then, as I understand from the OIG?

Mr. WARREN. Again, it is an area where there is a serious disagreement with the IG, which is why we asked Mandiant to come in and have a look at it.

Dr. HUELSKAMP. Okay.

Mr. WARREN. When we became aware of it we basically changed those passwords. We also reimaged——

Dr. HUELSKAMP. I understand what you did afterwards. I am still trying to figure out what you knew that you really knew, and when it was encrypted you did not break the encryption. I want, now I want to go into within the network. Mr. Warren, how would you know if someone manipulated data within the network?

Mr. WARREN. Depending on which system you are referring to, and what type of data, the triggers or the characteristics would be different. So it is part of the monitoring that either is built into systems where we are dealing with personnel information, or it deals with monitoring that our NSOC does in terms of——

Dr. HUELSKAMP. Well I understand the variance. But would you not have to have audit controls in place and turned on in order to know whether someone actually manipulated data?

Mr. WARREN. Sir, we have audit controls turned on in many places. And again——

Dr. HUELSKAMP. Are they always turned on? Are they always on, the audit controls?

Mr. WARREN. The audit team has identified for us where they were not turned on in the past. And so we have gone in and turned those on. Also again for the record we will bring back are there any other places where those controls are not turned on.

Dr. HUELSKAMP. Why would they have been turned off?

Mr. WARREN. Again, dealing with our history where we ran in a decentralized world, where every single location made their own decisions, just basically overcoming that past where they did not

feel either auditing was important, or they did not have the size or scope for it, or somebody turned it off by mistake.

Dr. HUELSKAMP. But as of today you are confident that all audit controls are turned on within the network? Because if they are turned off, I mean, we agree you are vulnerable. And you would not even know if you are vulnerable, and you would not even know if anybody is manipulating data. And the OIG has talked about this for years. I mean, this is just not an occurrence, a few times. It is over the past plus decade, audit controls are not always on for whatever reason. So but as of today, what would happen if someone turned off an audit control?

Mr. WARREN. It would depend on which system we are speaking to. I mean, one of the things that we have deployed in our data centers is a way of measuring the configuration of a server so that before a change takes place you can actually go back and ask "did that server get changed?" So all of our servers and data systems, we actually take a measurement of them. It is a particular unique number that you use. And if somebody changes something in the system, the number changes and it tells us, "hey, something changed there." And it is a control that we use in terms of managing configuration, but also as part of our strengthening reliability of systems.

Dr. HUELSKAMP. So you are confident that they are all turned on today?

Mr. WARREN. For the record, I was going to come back where we did not have them turned on, sir.

Dr. HUELSKAMP. Okay. I am looking forward. I just want to make sure that every employee understands, you cannot turn those off. Or else the system is vulnerable, so——

Mr. WARREN. Sir, I believe we have been clear. And this hearing, I actually sent a message out to all of my employees that this was an important hearing to watch. So let me speak to them. If you are an OI&T employee, or a contractor supporting the VA, it is not your responsibility or obligation or right to mess with audit controls.

Dr. HUELSKAMP. Period. And they will lose their job, why do you not say that, too? Well, no. We cannot say that. I am sorry.

Mr. WARREN. Appropriate disciplinary action——

Dr. HUELSKAMP. It is not permitted. I yield back, Mr. Chairman.

The CHAIRMAN. Thank you. Ms. Kuster, you are recognized for five minutes.

Ms. KUSTER. Thank you very much, Mr. Chairman.

And thank you, Mr. Warren. And I too want to add to the accolades for my colleague and good friend from the neighboring state, Mr. Michaud. Thank you for being a mentor to me in my first term, I truly appreciate it. And I also want to thank you and your family for your service to our country, and I am sorry for your loss.

I would like to focus in on the scheduling. I want to not ignore what has happened here, but get past that to what we can look forward to. I was very interested when I tried to learn more about this to have conversations with private vendors about what is possible, what is available. And in particular, I am looking at the highest and best and most frugal use of our tax dollars for making sure that we are scheduling our resources, our people, our physi-

cians and caregivers, as well as our physical plant most effectively, expeditiously.

And one of the things I learned about was the algorithms now that are available. All across private sector, all healthcare providers have a drop-off rate. Obviously, there are people who miss appointments. But it turns out that they have been able to do profiling to find out what type of patients are more likely to miss appointments and what type of patients are less likely. And then they are able to use these algorithms to schedule in the morning the most reliable patients and then double-book in the afternoon, later in the day, knowing that the less reliable patients would miss out. And I just wanted to get your thoughts.

I understand the complexity and having this work with VistA, but can we look down the road to a place where we are using tax dollars and federal resources more efficiently in providing high-quality care, which is ultimately all of our goal? A bipartisan goal, by the way.

Mr. WARREN. Yes, ma'am. Thank you for that question. I will actually take that back. I don't know if those particular algorithms are built into the acquisition, but it is a great idea.

Ms. KUSTER. Yes.

Mr. WARREN. And I am sure Dr. Tushman, who I think has come up here before, who focuses on these types of things, would also have an interest in terms of how do we effectively manage and schedule those appointments and the critical resources. But I will go back and I will ask that question.

Ms. KUSTER. It was very impressive. And luckily I am not trying to influence your decision, because I don't remember the name of which of the vendors I spoke to. But it was just a very interesting notion, something as simple as figuring out who is likely to show up, using the time wisely, and then of course getting to the place where you can have self-scheduling I think is ultimately an important goal.

On the second issue, I just wanted to explore a little bit more about the issue of the security based upon authorizations. And I believe Ms. McCauley mentioned even people who had left the VA continuing to have authorization. I know just in a small law firm this was complex, people come and go and they still have their passwords. But what steps have you taken both with regard to access authorization, and secondly, the issue around the missing laptop, have you taken steps to—about property and how have you communicated those throughout the VA?

Mr. WARREN. Yes, ma'am, great question. And it actually allows me to talk about information protection as more than an IT thing, because the question you are asking about is how do we make sure when an employee leaves or a contractor leaves that their access is removed. And we count on our HR systems, our HR processes, to do that. And it is an area that has been identified as a place where the systems are not connected. So one of the things that we implemented this year was we actually asked the HR community, "hey, why don't you send us the list of people at each site who left the place. While we figure out the system stuff, how do we get the HR employees to actually tell us who left, so we can go back in and remove their access."

So it is a combination of how do we get the process to work, because too often folks leave and you don't know, with a lot of the residents and a lot of the term appointments coming in and out. And with the new HR system that the VA is rolling across the complex, it is peaking up that management of people, but until that comes into place we put in a manual safeguard, which is tell us when they leave. Give us that report you generate every two weeks and we will use that as part of us removing from.

With respect to laptops, all of our laptops are now encrypted, as well as our desktops. So we went to a Windows 7 conversion, the upgrade, it actually built in encryption to all of the hard drives. So the issue we have had in the past where a laptop or a desktop went awry, there was concerns about data on it. In most cases, veteran information is actually not stored on a desktop, it is actually stored back in servers and main systems, which allows us some of those controls.

We are still wrestling with medical devices in terms of they are not encrypted, because most medical devices there are concerns about how the care delivery as part of the tool does or does not work. And what we go through, it is a very arduous and labor-intensive process, medical device or medical application by each one actually go and encrypt. BCMA, which was a bar code medication, it was not encrypted, it was one of our biggest risks. But we spent many years working with the medical community to show them and prove to them encrypting the devices would not impact care, and now we are rolling out that out across the complex. But many, many more years of work on the medical device side to get them up to the same standard of the devices I am responsible for.

Ms. KUSTER. Great. Well, thank you, Mr. Warren. My time is up. But I also appreciate—I understand from the materials that you took a courageous stand in your just recent background and I appreciate that. So thank you very much.

I yield back, Mr. Chairman.

The CHAIRMAN. Thank you.

Dr. Wenstrup, you are recognized for five minutes.

Dr. WENSTRUP. Thank you, Mr. Chairman.

Ms. Burnette, I do not want you to feel left out today and I notice no one has asked you any questions. But I would—I am curious to know the actual role of the Enterprise Risk Management Program. If you could tell me what role you play in protecting the confidentiality and integrity of our veterans' records.

Ms. BURNETTE. The Office of Enterprise Risk Management is relatively new to OI&T and recently, about a year after we set up at OI&T, we now have an office VA-wide that has a risk registry that supports the secretary.

The idea is, it is our number-one goal is to figure out how can we forecast and get in front of those things that could potentially preclude us from being successful in helping a veteran have the experience that he should have trusting reliability.

Dr. WENSTRUP. So what type of background does somebody have for say your job. What puts you in that position and what are some of the things that you are forecasting or are trying to look for in trying to be risk averse?

Ms. BURNETTE. We have about 55 risks currently on the risk registry, 27 of them we are mitigating. And they range anywhere from human capital competencies, do we have the right people doing the right job, to our ability to move to the cloud in a very efficient manner, to operational stability, does our infrastructure have the stability. Again, all of these things are based on forecasts, so that we can get in front of those problems that we might encounter.

Dr. WENSTRUP. So are there any things that you have uncovered? Are there any thing that you identified as a potential risk, and found it and eliminated it?

Ms. BURNETTE. Yes. As a matter of fact, IT-sensitive equipment was a risk. It was written up in the GAO and the OIG report about three years ago and we have come up with about 27 mitigating strategies. It used to be—or the GAO reported that we were at 55-percent accuracy of knowing where that sensitive equipment is and we are now at 90 percent as a result of those mitigating strategies. Our goal is 95 percent. So we are still working on those, but we are making great progress.

Dr. WENSTRUP. I mean, do you look at everything from staffing weaknesses——

Ms. BURNETTE. Yes.

Dr. WENSTRUP [continuing]. You know, people within the system that could be doing harm? How do you find those types of things, how do you look at that?

Ms. BURNETTE. I don't know about looking in the system for people that are doing harm, but we definitely look at what kinds of technologies are on the horizon and do we have the right competencies in our workforce, and what kind of training modules do we need to develop to support those.

Dr. WENSTRUP. How many people in your department, if you will, in your section?

Ms. BURNETTE. I have about 20 people that do risk management planning. So they go out and they look at the OIG and the GAO reports, they work with risk champions, they look at what's happening in the IT arena. And then we have about—we have a total of 100, so the remaining 80 actually support mitigating strategies. So they go out and do security-control assessments. Many of the NIST controls that the OIG had mentioned, we also support those.

It is the actual assessment process. So you need to go out and we need to validate that, yeah, this is a forecasted risk and start developing mitigating strategies, and we do that in conjunction with the subject matter experts from the different parts of the organization.

Dr. WENSTRUP. I am just curious what type of background someone has in this role. I mean, is there a degree in this? Where does it come from?

Ms. BURNETTE. It is actually very new to the Federal Government, Enterprise Risk Management. Like I said, my organization, who does a phenomenal job, is only about two years old. And OMB has recently issued——

Dr. WENSTRUP. So there is no like—there is no specific background to this?

Ms. BURNETTE. Well, I think we deal with risk every single day. I mean, I have spent 20 years in the federal sector and I have

worked managing large-scale program management offices that do weather site modernization and all the risks that are associated with that, to managing large-scale acquisitions for——

Dr. WENSTRUP. Well, we are all in favor, I would say, of preemptive action on things——

Ms. BURNETTE. Exactly.

Dr. WENSTRUP [continuing]. Of course, and that sounds like that is the role. How do we measure if we are getting the bang for our buck?

Ms. BURNETTE. Well, I mean, I think one of the ways we measure it is through the ITS, and inventory would be a good example. I mean, certainly understanding where our equipment is and ensuring that there is accuracy associated with that and making sure that it is disposed of properly. All of those things——

Dr. WENSTRUP. Shouldn't those things be within their own departments, though? Quality assurance, if you will? There is accountability within each department? I am just trying to figure out this role. I mean, I don't know if you are going around patting people on the back, saying you are doing a great job, keep it up, or what are we really—what are we really getting from this entity? I am just curious, because I am not familiar with it.

Mr. WARREN. Congressman Wenstrup——

Dr. WENSTRUP. Yes.

Mr. WARREN [continuing]. Mr. Chairman, if I could?

Dr. WENSTRUP. Sure.

Mr. WARREN. Ms. Burnette's organization and her team I look to, and we look to, to look over our horizon. Too often my day and my leaders are all about operational delivery of capabilities. We do fixate and focus to the now and the near. We probably have a six-month to a nine-month time horizon where this thing is due, where are you on that. Too often, because you are looking down, you can't see something that is coming at you. So we look at her team to actually broaden the view and ask, okay, what is it that we are not seeing? What is it that we are not dealing with right now? But if we don't do something, we need to.

And so we count on the team and it is a two-part team. One part is look over the horizon and use the reports from the auditors, from outside folks, from other organizations what they have seen. The other pieces we use for internal controls, we actually send them out and do the checks. Because the IT organization is so large, I actually make sure there are things that we look at. As an example, we look at the top ten travelers every year. Why did those people travel? Should they be traveling that much? We also go out and look at, as Ms. Burnette talked about, inventory. It was a big issue for us, folks not tracking and managing their inventory.

And so we moved away based upon her team's counsel from a once-a-year audit or inventory to right now every month ten percent of the inventory is assessed. So you are not all of a sudden at the end of the year going, oh, my gosh, we have lost it all, but how do I look at ten percent at a time. And that we embrace as a result of her team saying, you know, if you don't get your arms around this, you have got a serious problem. You have got a serious problem from an asset value, but also the information protection side, things will be leaving.

So, again, over the horizon, but also a part of it is looking to make sure are we doing the day-to-day things and from an internal accountability standpoint, internal controls.

Dr. WENSTRUP. Thank you.

Mr. WARREN. Hopefully that helps, sir.

Dr. WENSTRUP. It was very helpful. Thank you, I appreciate it.

The CHAIRMAN. Okay. Why don't we go with now Mr. O'Rourke. You are recognized for five minutes. Thank you.

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

A question for the GAO, Mr. Wilshusen, and then also for Ms. McCauley. Some of the deficiencies that we have talked about today, how bad are they relative to other federal agencies or departments, you know, the 12 years of material weakness in IT security? Do you see that in those who manage Medicaid, Medicare, Social Security records, for example? Is there a comparable we can look at, and if so, how does the VA do against that comparable?

Mr. WILSHUSEN. Let me start off before Ms. McCauley may speak.

One is, as Ms. McCauley mentioned, VA has a material weakness in its information security controls. Within the 24 CFO Act agencies, those agencies covered by the Chief Financial Officers Act, and include the major departments and agencies within the Federal Government, and there are 24 of them, seven of the 24 also reported a material weakness in fiscal year 2013. We don't have the information yet for 2014, but for 2013, seven. So VA was one of seven agencies out of 24 that had a material weakness in its information security program.

At the same time, there were 11 other agencies that had significant deficiencies in their information security controls. GAO has been identifying information security as a government-wide high-risk area since 1997. So it is a problem that extends beyond VA and touches upon many of the federal agencies within the Federal Government.

Mr. O'ROURKE. How about—so you have the data for those two years, do you have—and the government has been tracking it since '97—do you have any that since 2002 have had this problem sustained over that period of time?

Mr. WILSHUSEN. Right. That would be relatively few of the agencies, the exact number I can get to you, I don't have that right now. But I do know as an example, the Internal Revenue Service was one agency for which we have conducted the audit on an annual basis and identified it having a material weakness for a number of years. But over the last couple years, it made strides in improving security to where we were able to upgrade it to a significant deficiency.

Mr. O'ROURKE. Great. And, Ms. McCauley, I don't know if you have anything to add. I guess I am trying to find some context to understand how VA is doing relative to other large agencies or departments that may have had similar problems. Are they reacting as quickly, more quickly, more slowly? How are they doing?

Ms. MCCAULEY. I really can't comment on that. In the OIG we have purview of just the Department of Veterans' Affairs, their information security program, and we haven't taken the comparative

look and really—the GAO is in a better position to do that because they do the work government-wide.

Mr. O'ROURKE. Right. So maybe from the GAO it would be great to get——

Mr. WILSHUSEN. Sure. And just as another metric, if you will. For fiscal year 2013, 21 out of the 24 agencies had their Office of Inspectors General designate that agency as having a major management challenge in information security. So it is an issue that extends to most of the federal agencies within the Federal Government.

Mr. O'ROURKE. And for the two of you, the title of today's hearing is VA's Longstanding Information Security Weaknesses are Increasing Patient Wait Times and Allowing Extensive Data Manipulation; is that a fact?

Mr. WILSHUSEN. We did not look at the patient wait issue. As far as that is concerned, it relates primarily to VistA and we didn't look at that as part of our review.

Mr. O'ROURKE. Okay. Did the IG look at that?

Ms. MCCAULEY. We looked at the VistA system just as part of the wait times review. And the issues that we found were mainly related to the data integrity because of the use of unofficial wait lists, and also the issue of the audit logs turned off. But apart from that, we have not taken the look that would be needed to identify any kind of other information security deficiencies.

Mr. O'ROURKE. And based on Mr. Warren's responses today to your findings and to questions from the committee, do you have any ongoing concerns about the level of urgency and attention that VA is giving to the concerns that you have raised, the deficiencies that you have outlined?

Ms. MCCAULEY. The deficiencies with regard to the material weakness?

Mr. O'ROURKE. Correct. From his answers today and responses taken so far, do you have any ongoing concerns?

Ms. MCCAULEY. Well, the ongoing concern is that from year to year we continue to issue recommendations for improvement and many of these recommendations just continue to carry forward. Of the 35 recommendations from last year, most again will carry forward into the report for fiscal year 2014, and we continue to see the deficiencies across all of the control area. So, yes, we have a concern in not seeing the numbers go down as a result of our scanning.

Mr. WILSHUSEN. And if I may just add with respect to our report? As I mentioned earlier, we had eight recommendations, to which VA agreed with all eight. But in their responses to two of our recommendations they did not seem to directly address the actions that we had recommended. One was to apply missing security patches. In its response to that recommendation, VA talked about its monthly scans, which are of course a critical control. But the bottom line is once they identify those patches, they need to apply them.

And then our other recommendation with respect to identifying the actions, priorities and milestones for tasks related to improving their vulnerability remediation process, they really didn't address the priorities that they were to establish.

Mr. O'ROURKE. So unfortunately, and returning the time back to the Chair, it sounds like we may be here next year talking about these same issues.

I yield back.

The CHAIRMAN. Well, why aren't we implementing these recommendations, sir? And quickly, just very brief, because I want to get to Ms. Walorski.

Mr. WARREN. We are—and, again, we are implementing the recommendations. It is a question of whether the auditor believes that we have made enough progress over enough time for us to receive, if you will, credit for the work done. One of the challenges—and we have a very good relationship and the very good relationship is we have honest dialogue, what the auditor has seen and what we are doing, what fits, what doesn't fit.

The CHAIRMAN. Okay, very good.

You are recognized, Ms. Walorski, for five minutes.

Ms. WALORSKI. Thank you, Mr. Chairman.

I just think it is clear after almost two hours of testimony that the findings presented here just continue to reinforce the fact, and I guess Mr. O'Rourke's fact as well, that the personal information of millions of veterans still remains at risk. And to associate myself with your comment as well, I would like to encourage my colleagues to support my bill, H.R. 4370, that we have talked about in here before. The bill is based on a federal industry best practices that establishes an explicit plan of action to resolve VA's numerous IT security weaknesses.

With that, Mr. Warren, phishing represented almost 70 percent of the total incidents reported to the U.S. Computer Emergency Readiness Team in fiscal year 2013, but the VA reported only one phishing incident throughout the entire year and yet there were almost 1600 malicious code incidents reported. That appears to be a striking imbalance. Given that the goal of phishing is to deliver malware to the recipient, is this where the high number of—high volume of malicious codes are coming from?

Mr. WARREN. I can't speak to other organizations. I will go back and confirm that number just to make sure that what is reported is correct. So I will come back with the actual number for 2013.

But there are two things that the VA is different with respect to the other organizations reported. We are the first department that turned on Einstein 3, and Einstein 3 is the latest that Homeland Security has brought to the table, and it blocks most of those phishing and other malicious attempts out of the email stream before it even gets to us. So there is a lot of work that takes place outside.

We also have very complex systems at our boundary as well, where we are picking those out and we are stopping them. We stop more than 80 percent of the emails that come to our boundary before they even get to a desktop.

So there is a lot of things that we have put in place as part of our continuous monitoring, as part of our defense in depth, that tries to stop those things from getting to us, so the individual doesn't make that mistake of clicking on a link.

Ms. WALORSKI. Can you elaborate on a question that was asked earlier about moving forward on this issue of encryption on medical devices?

Mr. WARREN. The encryption on medical devices, it is a hard challenge for us and it starts with how the FDA certifies medical devices. And a lot of, I believe, new rule making took place in the last year, where prior to that rule making most vendors believed that when their medical device was certified or licensed no changes could be made to it, no encryption, no patching, nothing. And so we have had to actually move those devices into an isolation architecture. One of the things that the audit team has pointed out for us, we need to do better there, and there is a major effort this coming year to tighten it up.

So we actually now work with manufacturers. There is actually a command center in Atlanta that HHS runs where we have our employees embedded with HHS and the Defense Health service dealing with medical devices. How can you secure them? Because it is an area of concern for the medical industry.

Ms. WALORSKI. And it has been pretty well—I think it has been pretty well documented today by both the OIG and the GAO representatives being here to a question that was asked earlier about this issue of foreign entities potentially having access to our domain controller. How long would you estimate, Mr. Warren, it will take to put the patches and the different types of security links into the system that will prohibit a foreign entity from being able to access the system, how long will it take?

Mr. WARREN. So every day I get a new list of things to patch. So——

Ms. WALORSKI. But how long will it be based upon——

Mr. WARREN. We will never be patched, we will never be patched. As an example, on Tuesday Microsoft released a patch for something that has been in existence for 20 years. So every day industry is finding new ways that things can be exploited.

Ms. WALORSKI. If we will never be patched, how will we ever secure and have a vulnerable system to protect our veterans' personal information, and how will we ever connect to a DoD computer system if ours on the VA side is so vulnerable that we would suddenly have a tunnel of potential foreign entities right into the DoD system?

Mr. WARREN. So patching, ma'am, is one part of a complex set of tools.

Ms. WALORSKI. But you just said we will never be secure.

Mr. WARREN. So patching is one piece, so patching is one piece of defending systems.

Ms. WALORSKI. I understand, but you are the expert. You patch, you siphon, you do all these things, how long is it going to take to have the security of knowing that these domain controllers cannot be attacked and infiltrated by a foreign entity?

Mr. WARREN. I believe——

Ms. WALORSKI. Because that opens the door to will we ever connect with DoD.

Mr. WARREN. Yes, ma'am. I believe, based upon what the team has briefed me on and the third-party Mandiant that has come in and looked at our domain controllers, that has happened today and

prior to today. Those domain controllers are secured, and we continue to secure them and we continue to monitor them.

Ms. WALORSKI. So back to your comment that we will never be secure. What will we never be secure on, our veterans' information?

Mr. WARREN. If I could clarify, ma'am?

Ms. WALORSKI. Sure.

Mr. WARREN. I said things would not always be patched, because patching of vulnerabilities is one part of a spectrum of things that we need to do.

Ms. WALORSKI. So in your opinion today, you are really disagreeing with these two here. You are basically saying, you just said, that the domain controllers are safe and they cannot be encrypted, they cannot be corrupted by a foreign entity?

Mr. WARREN. The report we have received, and we brought in a third party to look at it and we will bring that report up to the committee and the staff, is they are seeing nothing on the domain controllers that causes them to believe that they are compromised. So I believe we have got that locked down.

With respect to patching, with respect to information protection, there is a whole host of things that you do to try and protect the enterprise; not just technical stuff, but also——

Ms. WALORSKI. Are the veterans' personal information in my district safe and secure today? 57,000 in the State of Indiana, are they secure?

Mr. WARREN. Ma'am, my data is in there. I will take the——

Ms. WALORSKI. You are not in my district. Are the 57,000 veterans in my district secure today?

Mr. WARREN. I believe it is, ma'am, I believe it is. I believe——

Ms. WALORSKI. Thank you.

I am sorry, Mr. Chairman, I yield back.

The CHAIRMAN. Mr. Walz, you are recognized for five minutes.

Mr. WALZ. Thank you, Mr. Chairman.

I too would like to thank the ranking member for his service, not just as a member of this committee and as a leader and a mentor, but as a veteran. I feel I was well served by his leadership. So thank you, Mr. Michaud.

I am really interested, I am going to go with Ms. Burnette in this over the horizon. I want to thank all of you for your service, but the one thing I would say—and I was one of those, as I said here, I was one of those 20 million veterans back in May, 2006 in the data breach when the laptop was lost, you came here. And then I still remember the day, it was a beautiful fall day, it was September 26th, 2007. Mr. Wilshusen, you were sitting right in that seat and I was sitting right in this seat, so this is deja vu.

And I made the comment to Ms. Melvin, your associate, and I said, "I feel that the issue here is more about culture of the VA and I am convinced that it is central before we can move forward to really understand the IT implications."

Ms. Melvin said, "I would agree with you, definitely key to this is cultural transformation that's necessary, along with the actual implementation of new processes."

I'm reading from the transcript of that day in this hearing, in this room.

Mr. Wilshusen, you came forward then and said, "And I would just add that from an information security perspective that the tone at the top has increased significantly with regard to taking corrective actions to implement effective security controls since that May 2006 data breach. I think it was a watershed event, which really caused and highlighted the need for strong information security that is coming."

And at the end of mine I said, "Great, I look forward to that. And I yield back."

Seven years and here we are. Was it still a watershed event?

Mr. WILSHUSEN. In terms of recognition and awareness of the need to detect and report on security incidents that have been detected, I would say yes.

At that time, just to give you an example, the number of incidents that were reported to U.S. CERT in fiscal year 2005–2006 was about I think 5,500 or so. This past year, it was over 70,000. And so the number of incidents that have been reported by agencies has increased significantly. Now, that can be for a number of reasons. One, better reporting, better detection on the part of agencies, the understanding of the need to report——

Mr. WALZ. When I go through this whole transcript, some of those fundamental issues have still not been corrected even though they were pointed out on that day.

Mr. WILSHUSEN. Right, I would agree with that. But in terms of being——

Mr. WALZ. How do you explain that, Mr. Warren? That suggestions were made, the OIG was here, Ms. Melvin was here, Mr. Wilshusen was here, they suggested some of these, they still have not been implemented.

Mr. WARREN. So the cultural changes or the technical changes?

Mr. WALZ. Some of the technical, and I would argue the cultural is certainly somewhat more subjective, but it gets back to my central goal. You brought up a great point and I think you are right, Mr. Warren, we can't limp from incident to incident to incident, it has got to be the over-the-horizon vision on this. I am still looking how this is all going to fit in a longitudinal transformational plan, because at that time what you were here for too was asking for more money, which you yourself said on that day in 2007, "We cancelled that program that we were asking money for in 2009."

Mr. WARREN. So to the cultural question, the change started as a watershed event. The fact that at that point when it happened, IT was something that was buried in all the programs. And with the help of this committee, we moved away from something in the shadows to a single organization. It took until 2009 where we actually moved out on the centralization. We are recognizing that you have got to manage this as a business enabler, which includes protecting the veterans' information.

From there, we have moved to the point when we talked about CRISP, this Continuous Readiness and Information Protection, was that next level, which is it is not an IT thing. Too often we say, yeah, the IT folks have got it. It is about how people think about the data, how they manage the data and how they protect the data. Over 90 percent of our incidents deal with people, they deal with

folks doing bad things. Taking stuff out of systems, leaving it on paper——

Mr. WALZ. That is cultural.

Mr. WARREN [continuing]. Or throwing it away. That is cultural and we focus on that. And what has really been key with CRISP, that is another major step for us, leadership. Not IT leadership, but the deputy secretary, the secretary, the under secretaries all heard, and it was said from the leadership down, this is key to us. And so this communication about what it is and why it is.

This report that I talked about that comes out monthly, that is a daily report that goes out to all of the VA leadership of every incident where veterans' data was put at risk. They have membership on this data breach team. So this it happens out there and we don't worry about it has gone away. Folks are aware of it and they understand what we need to do about it.

Mr. WALZ. How different will this hearing be in 2021 on this issue?

Mr. WARREN. I will tell you, sir——

Mr. WALZ. Competent.

Mr. WARREN [continuing]. I drive hard and one of the things, I drag my folks through a knothole starting in April, four nights a week. Where are we on? And when I say night, 6 o'clock every night. And we shut it down in the end August, as we are waiting for the audit results, we are starting that back up again as we get prepared for the audit team. And it is constant attention, constant reinforcement, as well as you all support from a resourcing standpoint and the mouthpiece of this is important, because it is your data, it is my data, it is our family's data, and it is key to getting quality——

Mr. WALZ. I couldn't agree more. I just think it becomes harder and harder and harder, especially on the resourcing, to make the case. I think you understand that——

Mr. WARREN. Yes, sir.

Mr. WALZ [continuing]. And that is going to be the challenge.

I yield back.

The CHAIRMAN. Thank you.

Ms. Brown, you are recognized for five minutes.

Ms. BROWN. Thank you. Thank you, Mr. Chairman, and also ranking member. I want to thank you for your leadership and keeping this committee bipartisan, what has been the 22 years I have been here.

And I also want to say that when I came to this committee the main worry veterans was having was how to reconstruct their files for benefits, because much of it was lost in St. Louis fire. When we had Katrina, many of the veterans had real problems trying to get their records, because it was in a region and they could not access to other regions.

So my question, as we move forward we need to make sure that, whether it is manmade or whether it is outside sources, that we are able to get that information for the veterans as we balance security and information.

Mr. Warren, thank you for your service, and can you tell me how we are integrating that into the system?

Mr. WARREN. Yes, ma'am. And to make a connection, my father's records were lost in that St. Louis fire. So before I even came to the VA, I was aware of how dramatic and traumatic that event was for many, many veterans.

But with respect to bringing the information over so we can make those benefits determinations, we look at that as two major components. The first one, we have talked about this before in terms of VBMS, moving away from a paper manual process to an automated tool that is delivering and the organization is using to meet the commitment we have made for 2015. We have moved from piles of paper to 95 percent, over 95 percent of those records are in electrons.

Ms. BROWN. Just one quick question. But with Katrina, we could not get those records.

Mr. WARREN. So with Katrina, on the benefits side, you are correct. But what was interesting on the health side, within 24 hours those medical records in VistA were available for the folks who left the area when they came to other medical locations. VistA was up, their data was there, and they were able to get care based upon that.

So we have been applying that knowledge into how do we do it on the benefits side. The first part is, get the tool in place that allows us to move away from paper. The second piece is the partnership with DoD in terms of moving that single treatment record over. Traumatic, dramatic, the fact that as of 1 January, any service member who left service as of 1 January, the DoD is sending over that single treatment record with the certification on top of it. It allows us to move forward and rate those claims. We are working with them to move back to get the folks who left prior to 1 January. That is going to be a heavy lift, the challenge is in the reserve component and the guard component where the data is not in one place.

So it is an area we focused on. I know Under Secretary Hickey spends a lot of time there. I know the deputy and the secretary also are very interested in making sure we get what is due to our veterans and part of that benefits piece is a key one.

Ms. BROWN. We had several meetings, not just with VA, but with the banking community, because the question keeps coming up about the foreign attacking the system, they have attacked the banking system. I got a call from my bank saying someone was charging my card in China. So it is clearly a problem. What are we doing as we coordinate these efforts? It is not just the VA, it is the entire system.

Mr. WARREN. Great question, ma'am. And one of the things—and I would limit, because I am focused on how do I protect the veterans' data, and that is my fisc (?) in terms of—and my team's—is how do we protect inward. But we also, with our partnership with Homeland Security, we share with them all our data feeds. All right? So what we see, what gets through their defenses, how we respond to them, that gets to them. They also send the same to us. But teaming in terms of how do we protect the homeland, I would say that is probably the next area, beyond my scope and charge, but my hope is somebody is going to take that on.

Ms. BROWN. I think that is pretty much all of my questions, most of them was answered prior to. But I want to again thank you for your service. And I think you have been in this position since 2007?

Mr. WARREN. Yes, ma'am.

Ms. BROWN. It is refreshing.

Mr. WARREN. I am here to stay the course, I have got a commitment.

Ms. BROWN. Last thing. People keep talking, my colleagues, about the recommendations. And recommendations are very important and I guess you have to prioritize those recommendations. My question pertains to you all have made a lot of progress and I don't know whether or not you all have emphasized—some of those issues are going to be reoccurring, but emphasized the improvement that has been made in the VA system, and I would like for you all to give them a shout out for what they are doing for the people back home just listening.

Mr. WARREN. Ma'am, I really appreciate the opportunity to talk about the great work that my employees, that our employees are doing. We are the first department that has continuous monitoring in place and it is as a result of what they have done. We are the first department that brought Einstein on board in terms of those perimeters. The audit team has recognized where we have done improvements. But with that and with their dedication, and not just on the security side but making sure we are enabling that delivery of benefits and services, we know we have more to do. And we are committed to doing that, because 56 percent of my employees are in the same place I am, they are veterans. It is their data that they are protecting, it is their benefits and services that they are delivering to the buddies, their colleagues.

And so I appreciate their commitment and dedication every day, and I am honored to serve as their leader. Thank you.

Ms. BROWN. Thank you.

Can the IG answer that question also?

The CHAIRMAN. Yeah, absolutely.

Ms. BROWN. All right. Would you, please?

Ms. MCCAULEY. Could you repeat the question again?

Ms. BROWN. Would you discuss the improvements that the VA has made? And, you know, you have talked about some of the issues will be back next year. Well, we have the same issues every year on every committee, whether it is—so can you give a shout out for the people that is listening to show the improvements that the VA have made over this period?

Ms. MCCAULEY. Certainly. Yes, as we conduct our FISMA assessments every year, we do see incremental improvement, and especially with the inception of CRISP in 2012. And as I mentioned earlier, we are seeing the continuous monitoring and the predictive scanning, and the improved training and testing of contingency plans and what have you. We know that the teams are working hard and we are continuing the dialogue with the OI&T and the IT professionals to ensure that they understand what requirements, the criteria that we are using to measure their progress by. And we had that discussion just the other day to ensure that we continue to talk about that and make sure we are all clear in terms

of the demonstrated progress, but also the substantiating documentation that is needed.

Ms. BROWN. It seems to me that a lot of the problems pertain to training and I hope in your request you are asking for the money for training, Mr. Warren, because a lot of the problems, people taking things home, leaving information out, is just—like you say, you constantly have to remind them——

Mr. WARREN. Yes, ma'am.

Ms. BROWN [continuing]. Of their responsibilities.

Mr. WARREN. It is a key component of making sure that veterans' data is protected and we meet our stewardship obligations.

Ms. BROWN. Thank you, Mr. Chairman. I yield back the balance of my time.

The CHAIRMAN. Thank you very much.

With the consent of the ranking member and myself, counsel is permitted to ask questions. So, without objection, so ordered.

We are going to start with the majority counsel. You are recognized, sir.

Mr. HANNEL. Thank you, Chairman.

Mr. Warren, as you have been testifying in the last 20 minutes, one of those outstanding IT employees of yours has emailed me as a whistleblower, and he has provided a number of emails. And in his emails it shows where he has been trying to get a problem addressed and his supervisors have basically shut him down. This is not speculation, I have looked at the emails.

My question to you is this. Based on what he is sharing with us, with me, he has said that he recently mitigated 72,000 accounts that were not picked up by VA's audit tool. Of course, these 72,000 accounts were for employees who have left the VA. These accounts were never closed, locked out, secured, nothing, they remained open. So these 72,000 former VA employees could access VA's network for an extensive period of time. So my question is how do you address this? How do you stop this? And because he has been trying to deal with this issue and he has been shut down by his supervisors, how do you deal with that?

Mr. WARREN. So the first thing. For the employee, thank you for coming forward. And if they are willing—all employees who come forward with issues like that, so I take it outside of the leadership chain, so they feel that they are getting the support they need, I send them to my chief of staff, because she is not in the chain for any of them. And we normally do fact finding or AIBs, if it raises to that level. So if he is willing to bring that information forward. I find it problematic that he has been trying to solve something and his chain did not support him. So if he is willing to do that or if you are willing to share—again, if the employee is uncomfortable—want to take that, want to take the appropriate action. It is inappropriate for anybody in the chain not to support individuals doing the right thing. And so if the employee is willing to come forward, send me an email, *stephen.warren@va.gov*, and I will personally take that on.

Mr. HANNEL. I will work with him and I will also—Mr. Wilshusen, I saw you were curious of those emails, I will share those with you as well.

Mr. WILSHUSEN. Thank you.

The CHAIRMAN. Thank you.

Now I would like to recognize the minority counsel to ask questions.

Mr. TUCKER. Thank you, Mr. Chairman. I have no further questions.

The CHAIRMAN. All right, very good.

I have one question and Ms. Brown, do you have any other questions?

Ms. BROWN. No.

The CHAIRMAN. Mr. Walz, do you have questions?

Mr. WALZ. No, thank you.

The CHAIRMAN. Okay.

Ms. BROWN. I would like to see the email also——

The CHAIRMAN. Absolutely.

Ms. BROWN [continuing]. Because——

Mr. WILSHUSEN. Since it has been referenced.

Ms. BROWN. Yeah, since it has been referenced, I would like to see it.

The CHAIRMAN. Absolutely, absolutely.

One question. And it appears that almost—and, Mr. Walz, if you want to follow up with this, please don't hesitate. It appears that almost half of the cyber incidents reported came from just two government agencies, the VA and HHS. VA had the highest number of incidents reported overall and the highest number of malware incidents reported. It is apparent that the healthcare data has become and it has become a significant target of attackers. Healthcare data is 10 to 20 times more valuable now on the black market than credit card data. Unbelievable.

So again I want to ask the question, but again we don't want to be here next year discussing the same topics, and I know Mr. Walz might want to add something. The question is what is VA doing to lower these numbers systematically? And I will ask Mr. Warren first.

Mr. WARREN. Thank you for that question, because it actually allows me to do a shout out to the VA employees, because they do report. And we have seen when we look comparatively for the rest of the Federal Government, given that we are under the same threats, that if you do the calculation of per head we report within the one hour. In fact, U.S. CERT has said, stop telling us, you are reporting too much, because we make sure we follow the letter of the law with reporting.

The other big change that we are seeing is when we converted to PIV cards, our increase in reporting as a result of PIV cards, that is actually a security incident. And so our year-to-year increase has been a result of since everybody has gone to a PIV card, 360,000 of them, and we lose about a hundred of them a month, and when you start adding those up, that is a lot of incidents that are being reported.

So lots of good reporting. But with those numbers, one of the things that I have high confidence in because of the things that the team has put in place is that we are able to report them, and we are able to report them because we are seeing them, because we are containing them, and because we are eradicating them.

The CHAIRMAN. What are we going to do about the numbers, the incidents?

Mr. WARREN. Sir, the numbers will continue to go up. The threat environment, not just to the VA, but other departments, keeps increasing. No department can stop the threat coming from the outside. So what we have to do is make sure we have defense in depth, to make sure we have teamed with Homeland Security and they are using the signatures from the classified world to help protect us.

The CHAIRMAN. If there are no further questions—do you have anything to add, Ms. Brown?

Ms. BROWN. No, I just want him——

The CHAIRMAN. Please, thank you.

Ms. BROWN. He mentioned the Homeland Security program that you have in place, can you go through that again quickly?

Mr. WARREN. Yes, ma'am. There is a program called Einstein 3, it is actually—it has been over multiple years as they have brought new protections on. And what it does, it is a two-part process. The first piece is departments move all of your traffic into control points. We have four control points. And at the control points, they use very technical and specialized equipment to look at all the traffic coming over the boundary. So we count on them, if you will, to have our back, because they have got our outer perimeter, and they are able to use stuff out of the defense world and the classified world that we would never see to help protect us. It is an area where they are able to add all of their knowledge in to make sure that we don't have to deal with that. That is where the strength in numbers is really working for us and we really appreciate their support.

Ms. BROWN. And so you stop over 80 percent of the—before it gets to the VA?

Mr. WARREN. Yes, ma'am. Over 80 percent of our emails never make it to an employee's desktop. And if I just do the numbers, is we stopped last month 82 million emails, we stopped them at the perimeter, because there was something suspicious about them. We stopped 206 million pieces of malware, 206 million pieces of malware in the month of October, before it even got to our employees' desktop.

The CHAIRMAN. Okay. I would like to recognize the ranking—actually, the majority counsel for a question.

Mr. HANNEL. One last question, Ms. McCauley. Einstein only identifies known profiles; is that correct?

Ms. MCCAULEY. I cannot address that question, I would like to state that for the record.

Mr. HANNEL. Mr. Wilshusen, do you know?

Mr. WILSHUSEN. That would be correct. We are actually conducting an audit of Einstein at this point, our work is still ongoing. But just for Einstein itself, it needs to know, it identifies specific information that is known. If there is malicious software that is not yet known, such as zero days, it is likely that Einstein may not include it.

Mr. HANNEL. Thank you.

The CHAIRMAN. Thank you, thank you very much.

If there are no further questions. Again, I thank the witnesses and the audience for your patience, and thanks for this conversation today. And what I will do is I will adjourn the hearing. Thank you.

(Whereupon, at 3:45 p.m., the committee was adjourned.)

APPENDIX

PREPARED STATEMENT OF CHAIRMAN JEFF MILLER

The Committee will come to order.

Good afternoon everybody. I want to welcome you to today's Full Committee hearing.

As our hearings this summer revealed, data manipulation had become an accepted practice at many facilities within VA. Moving forward with our investigation, it has become clear that a common thread in these scandals continues to be weaknesses within VA's Office of Information & Technology (OIT) and the systems for which they are responsible.

For example, Committee investigators discovered VA briefing documents that reveal VA's medical information system, VISTA, allows for data manipulation. This internal briefing, given in April 2013 to senior VA officials, including VA's Chief Information Officer, described threats posed by anonymous user access to VISTA— the automated system that supports the day-to-day functions of VA's network of hospitals.

We continue to receive evidence from credible whistleblowers that at some sites there are no restrictions imposed on users and because their audit controls are not turned 'on', VA cannot determine who or when someone had access to patients' data within VISTA. Further, we have found that most VA facilities do not have audit policy settings configured and no one is assigned to monitor the audit logs necessary for determining individual accountability, reconstructing security events, and detecting intruders. To date, these issues remain unresolved in VA's network and according to GAO, VA's Network Security Operations Center, who provide continuous, around-the-clock monitoring of VA's network, did not have access to the system logs at VA's data centers which inhibited its visibility across VA networks and ability to confirm whether a security incident was fully contained and eradicated.

Because these audit controls are oftentimes inactive, employees and leadership are accessing veteran patient records against regulations and current law, including medical privacy rights under HIPAA. In addition, VA whistleblowers have confirmed that unauthorized access to employees' files is a common occurrence, but the office of information and technology has yet to prevent unauthorized access to employee files. Furthermore, these deficiencies could allow for the creation of bogus claims that authorize fraudulent payments to non-existing veterans as we showed VA during a member's brief last year.

In addition, during the phoenix wait time scandal, veterans who had been identified as "deceased" on the electronic wait list were resurrected to appear as though they were "alive". When this practice was revealed by us to the OIG, we were told that it was common because a death certificate had not been filed; therefore, the veteran had to be listed as "alive" until proven deceased. However, as whistleblowers described, the death certificate requirement was a newer policy that began December 17th, 2013, only after this matter was reported to VA's inspector general.

Other whistleblowers have reported that VA's system provides unauthorized access and modification of patient data because of the lack of a date and time stamp that would indicate when a record was modified and by whom.

VA's inspector general has already substantiated that VA employees were manipulating data by "zeroing out" the number of days for awaiting appointments. In truth, according to our evidence, the current it system is easy to manipulate and anyone can make a patient's wait time zero at any given moment to hide scheduling and patient backlog issues. The ability for such manipulation in the system requires immediate attention, but the Office of Information and Technology has yet to address it.

I should add that VA's Technology Office has greatly contributed to the problems of data manipulation by not addressing the long standing issues we have repeatedly brought to their attention, and these problems—and more—according to the Inspector General, have remained a material weakness for the 16th consecutive year.

These failures are not because of a lack of resources, as some VA senior officials want us to believe. Within the past decade, congress has provided over 28 billion dollars to VA's Office of Information and Technology to ensure its goals and actions are aligned with and driving the strategic goals of the agency. Given the availability of resources, it is apparent that this office's lack of success and repeated underperformance is a leadership failure.

Let me be clear, the failures aren't just a VA problem—they are a veterans problem. If a veteran cannot get access to healthcare because his or her eligibility claim is stuck—or because his or her claim is altered—or because the appointment has been altered, the veteran is prevented from obtaining healthcare and their hard earned benefits. Regrettably, I am concerned that VA lacks the technological foundation necessary to prevent these actions from reoccurring.

I thank you all once again for being here this afternoon.

With that, I now yield to Ranking Member Michaud for any opening remarks he may have.

PREPARED STATEMENT OF MR. STEPHEN WARREN

Introduction

Chairman Miller, Ranking Member Michaud, and Members of the Committee, thank you for the opportunity to appear before you today to discuss the Department of Veterans Affairs (VA) Information Security.

Scheduling

Before discussing how VA's information security posture has improved over the past year, it is important to make a distinction between access to care and VA's information technology (IT) security efforts.

To my knowledge, there have been no indications that unauthorized individuals accessed the software; rather, some authorized users allegedly made inappropriate changes. Thus, there is no causal relationship between alleged internal data manipulation by certain VA employees and findings in VA's Office of Inspector General (OIG) Federal Information Security Management Act (FISMA) audit. As recently pointed out in OIG's recent report the limitations of the software underlying the scheduling system is secondary to the need for additional resources to actually schedule—doctors, nurses, and other health professionals; physical space; and appropriately trained administrative support personnel.

The limitations of the scheduling system and associated practices are being addressed. Resourcing recommendations for IT investments are made by each of the Administrations (Veterans Health Administration (VHA), Veterans Benefits Administration, and the National Cemetery Administration) based on business priorities. VHA and the Office of Information and Technology (OIT) are working together to overhaul the outdated scheduling system and to bring an innovative scheduling program into VA's current electronic health record system—VistA. Empowering employees with the most useful and effective technology is key to transforming VHA. In the coming weeks, VA will release a Request For Proposal for acquiring new scheduling software, since the existing software was outdated and difficult to use. VA expects an interim milestone towards this acquisition in spring 2015. Through this process, VA held an Industry Day and engaged with VSOs for their input on what kind of a system would be best for Veterans.

The technology underlying the current scheduling system used by VA medical facilities is cumbersome and outdated. In addition, there is no audit capability in the scheduling application that will indicate whether users are manipulating data to meet wait time expectations versus making legitimate changes to appointment information. On May 12, 2014, as part of its investigation, the Office of the Inspector General (OIG) asked VA to enable audit controls on four Veterans Health Information Systems and Technology Architecture (VistA) files related to waiting lists. Once this request was received, VA immediately turned the auditing on for the requested items.

VA's current electronic health record, VistA, already has access and audit capabilities. VA is evolving its existing VistA system to meet or exceed all Federal information assurance requirements including the Federal Information Security Management Act (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, applicable National Institute of Standards and Technology special publications, and Federal Identity, Access and Credential Management policies.

Progress Made in Information Security

VA employs an extensive, layered, defense-in-depth strategy to protect the security and confidentiality of VA information and information systems and we continue to make great strides to keep up with ever-evolving threats. We have established appropriate technical, physical, and administrative safeguards to help ensure the security and confidentiality of Veteran records. Since the June 4, 2013, hearing before the House Veterans Affairs Committee's subcommittee for Oversight and Investigations, we have acquired new monitoring capabilities, increased desktop security, and enhanced our speed in detecting and combating challenges.

Before we activate systems within our network, and before any Veteran's information is put into those systems, we take steps that ensure the information is protected to the best of our ability. The process for issuing formal approval to operate systems on VA's network—known as "Authorities to Operate (ATO)"—has greatly improved in the last year. We have migrated from a manual, point-in-time, paper process to an electronic, automated, continuous monitoring capability with the help of the newly implemented Governance, Risk, and Compliance (GRC) tool, which went live in August 2013. We are the first (and the largest) cabinet level government agency to have moved to continuous monitoring. This new capability allows VA to detect vulnerabilities early and respond to threats rapidly.

The GRC tool is not the only new addition to VA's security infrastructure. VA has brought another more refined and powerful security tool into its enterprise. Working with our Federal partners, such as the Department of Homeland Security, we were the first cabinet level agency to implement Einstein 3, as well as the Office of Management and Budget's Trusted Internet Connection initiative. Numerous industry-standard scanning tools, firewalls, network and host intrusion prevention systems, and non-medical desktop and laptop encryption and anti-virus services protect the confidentiality, integrity, and availability of our data.

As an organization of more than 300,000 employees, however, our biggest vulnerability is not technical. Physical exposure of VA data is the most significant risk facing our information security posture. Over 98 percent of the sensitive data exposure at VA is due to paper or human error-based incidents. Network and system safeguards are not technical absolutes—we must constantly remain vigilant in preventing human error-such as an employee clicking a phishing link, mis-mailing a sensitive record, or losing an electronic device.

VA is addressing its ongoing challenge of protecting Veteran information on paper by focusing on our employees. Because VA employees are the first line of defense when it comes to information protection, VA is working to improve employee awareness of information protection through training and other measures. VA promotes an environment where all employee's and contractor's actions reflect the importance of information security accountability.

In addition, every VA employee, contractor, and volunteer is required to sign a "Rules of Behavior" statement that sets expectations and makes clear that users are accountable for the protection of sensitive information. Every employee, contractor, and volunteer is also required to take an annual Information Security and Privacy Training. System access is terminated if individuals are delinquent. If a security or privacy incident occurs involving an employee or group of employees, VA employs recovery activities that include re-training of those involved. In addition, VA runs an annual Information Security and Privacy Awareness Week and sends out monthly messages reminding employees about security and privacy best practices. Educating our workforce is an ongoing process that VA takes very seriously.

The Department has established a rigorous data breach notification process. Once a reported incident is evaluated by the Incident Resolution Team, it is forwarded to the Data Breach Core Team (DBCT). The DBCT performs a risk analysis on all reported data breach incidents and when they determine a potential breach may have occurred and may pose a reasonable risk of harm to the affected individuals, they recommend that those individuals be notified and, if appropriate, offered free enrollment in a credit monitoring service to mitigate any risk of identity theft or improper use of their information. This robust review process is complemented by the monthly posting on VA's Web site of notifications of any data breaches, and this material is also provided to Congress through VA's quarterly data breach reports.

FISMA

FISMA provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. OIG conducts annual FISMA audits of the agency's information security program. VA appreciates OIG's time and effort conducting its annual FISMA report, and appreciates that OIG finds VA's comments and corrective action plans as responsive to its recommendations. Although much work remains, VA has

made significant improvements in the last few years and strives to meet the highest standards in protecting sensitive information. We are constantly and continuously improving our information security posture so that we may be the best possible stewards of Veteran information.

Federal Information System Controls Audit Manual (FISCAM)

The Government Accountability Office FISCAM is designated to be used during financial and performance audits and may result in the identification of material weaknesses. The most recent FISCAM audit review reflects that we have closed out many of the observations from prior years, and are making considerable improvements each year. In a constantly changing threat landscape, we continue to evolve.

The number of FISCAM findings has decreased 29 percent since fiscal year 2011. Highlights of VA's accomplishments in this area include:

- VA has resolved its findings on contingency planning, as well as segregation of duties.
- VA reduced the amount of time needed to complete a scan of the entire enterprise from approximately 1 year to approximately 1 month.
- VA completed two-factor authentication for system administrators.
- VA strengthened passwords critical to accessing systems.

OIG noted our compliance in the above areas, and now looks to us to maintain consistency across the enterprise. VA leadership remains engaged in order to remediate the recommendations made by OIG.

Conclusion

Over the past year, VA has made demonstrable progress improving upon its defense-in-depth strategy to protect Veteran information and VA systems. VA has made progress in FISMA audits, in the tools we use to combat evolving cybersecurity threats, and in securing the systems our clinicians and employees use to serve Veterans. We continue to work to address the challenges we face, including continued work to close FISMA recommendations and better educating employees on handling sensitive information on paper. We will continue to ensure our IT systems, which are crucial to supporting our Veterans, are secure and our employees are responsible as we protect the information of the Veterans we serve.

STATEMENT OF
SONDRA F. MCCAULEY
DEPUTY ASSISTANT INSPECTOR GENERAL FOR AUDITS AND EVALUATIONS
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES
HEARING ON
"VA'S LONGSTANDING INFORMATION SECURITY WEAKNESSES ARE INCREASING PATIENT WAIT TIMES AND ALLOWING EXTENSIVE DATA MANIPULATION"
NOVEMBER 18, 2014

Mr. Chairman and Members of the Committee, thank you for the opportunity to discuss the Office of Inspector General's (OIG) work regarding VA's Office of Information and Technology's (OIT) management of its information security programs. Our statement today focuses on VA's effectiveness in implementing the configuration management controls, access controls, security management, and contingency planning necessary to protect its mission-critical systems from unauthorized access, alteration, or destruction. We base our conclusions on the OIG's past and ongoing audits of VA's information security program. We will also focus on the challenges VA faces overcoming several information security concerns not highlighted in previous years. I am accompanied by Mr. Michael Bowman, Director, OIG Information Technology and Security Audits Division.

BACKGROUND

Information Technology (IT) systems and networks are critical to support VA in carrying out its mission of providing medical care and benefits and services to veterans. Ensuring the secure operation of these systems and networks is essential, given the wide availability of hacking tools on the Internet and the advances in the effectiveness of attack technology. Lacking proper safeguards, the systems and networks are vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. VA previously reported a security incident in which sensitive information was compromised, including personally identifiable information (PII), potentially exposing millions of veterans and their families to the loss of privacy, identity theft, and other financial crimes.

INFORMATION SECURITY

This year, for the 15th consecutive year, the OIG's independent contractors who perform the annual audit of VA's consolidated financial statements have identified IT security controls as a material weakness. This work supports our requirements to perform 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 annual reporting requirements from the Office of Management and Budget.

In March 2012, 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 a result, in our report, *Federal Information Security Management Act Audit for Fiscal Year 2013* (May 29, 2014), we discussed more focused VA efforts to implement standardized information security controls across the enterprise. As part of the fiscal year (FY) 2014 Consolidated Financial Statement audit, we reported some additional improvements in VA's IT security management. However these improvements require time to be fully implemented across VA's large enterprise-wide infrastructure and to show evidence of their effectiveness. The improvements we noted are:

- VA has continued predictive scanning of its networks to facilitate identification of system and network vulnerabilities across its field offices.
- VA has used the IT Governance, Risk, and Compliance tool, implemented in August 2013, to improve the process for assessing, authorizing, and monitoring the security posture of the agency.
- VA has improved implementation of its role-based and security awareness training and contingency plan testing.
- VA has reduced the number of individuals with outdated background investigations.
- VA has ensured consistent compliance with *United States Government Configuration Baseline* standards across the enterprise.

Despite progress made, OIT was not fully effective in addressing systemic weaknesses or eliminating the material weakness identified in VA's information security program for FY 2014. We continue to see repeat information security deficiencies in type and risk level to our reported findings in prior years and an overall inconsistent implementation of the security program. Communication between OIT's CRISP team and VA site managers also needs improvement. We will issue our FY 2014 FISMA audit in the spring of 2015 and it will discuss control deficiencies in four key areas: configuration management controls, access controls, security management, and contingency planning controls.

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.
- The financial management system uses an unsupported database with several known critical vulnerabilities that cannot be updated with security patches, thus

preventing the implementation of effective security controls. Performance and security weaknesses are inherent with older versions of the system software.
- Change control policy and procedures for authorizing, testing, and approving system changes were not consistently implemented for networks and mission-critical system hardware and software changes.
- Several VA organizations were sharing the same local networks as other tenants at VA medical facilities and data centers; however, the tenant systems were not under the control of the local VA sites and often had critical or high-level vulnerabilities that weakened the overall security posture of the VA sites.
- Formal processes were lacking to monitor, prevent installation of, and remove unauthorized application software on VA systems.

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 work to date shows 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 fully 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 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.
- Monitoring of access was lacking in the production environment for individuals with elevated application privileges for a major application.
- Identification, notification, and remediation of security incidents were not consistently implemented to ensure incidents were resolved timely. In addition, network security event logs were not consistently maintained or reviewed across all facilities.
- Unknown and unmonitored system interconnections continued to exist and sometimes lacked valid Interconnection Security Agreements and Memoranda of Understanding to govern access to VA networks.

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. As part of the FY 2014 Consolidated Financial Statement audit, we reported:

- Security management documentation, including the Risk Assessments and System Security Plan, and Privacy Impact Assessments 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 Plans of Action and Milestones (POA&Ms) were updated without written justification and supporting documentation was not adequate to justify POA&M closures. VA has approximately 9,000 open POA&Ms in FY 2014 compared with 6,000 in FY 2013.
- VA did not effectively manage and monitor its systems hosted at a cloud service provider.

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:

- Backup tapes were not encrypted prior to being sent to offsite storage at selected facilities and data centers.
- Contingency plans did not reflect the current operating environment. Specifically, contingency plans had not been updated to reflect changes in system boundaries, roles and responsibilities, and lessons learned from testing contingency plans.

We continue to identify significant technical weaknesses in databases, servers, and network devices that support transmitting sensitive information among VA Medical Centers, Data Centers, and VA Central Office. For FY 2014 we once again found deficiencies where control activities were not appropriately designed or operating effectively. It is particularly disconcerting that a significant number of vulnerabilities we identified at VA data centers are more than 5 years old. In addition, inconsistent application of vendor patches designed to address such weaknesses jeopardize the data integrity and confidentiality of VA's financial and sensitive information.

Moving forward, VA needs to complete implementation of an enterprise-wide information security program and improve its monitoring process to ensure controls are operating as intended at all facilities. 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 architecture results 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. Effective communication between VA management and the individual field offices is critically needed to notify the appropriate personnel of identified security deficiencies so that they can timely implement corrective actions.

We expect to include in the FY 2014 FISMA audit a number of recommendations that remain unaddressed from prior years. Specifically, our FY 2013 FISMA report included 30 recommendations plus 5 unresolved recommendations from prior years'

assessments for a total of 35 outstanding recommendations. While OIT has made some initial effort, it has not provided sufficient information to support closing the recommendations. Overall, we recommended that VA:

- Address security-related issues that contributed to the IT material weakness that continues to be reported as a result of the annual audit of VA's consolidated financial statements.
- Remediate high-risk system security issues in its POA&Ms.
- Establish effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments.
- Implement effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.
- Institute procedures to oversee contractor management of cloud-based systems, ensure OIG access to those systems, and ensure information security controls are adequate to protect sensitive VA systems and data.
- Conduct periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and excessive or unauthorized accounts.

EMERGING INFORMATION SECURITY CONCERNS AT VA

This year, VA faces the added challenge of overcoming several information security concerns not highlighted in previous years such as cloud computing and foreign hackers. As appropriate, we have pursued these issues as a part of our FY 2014 FISMA audit work.

System Assessment and Authorization Process

Our FISMA testing for FY 2014 revealed potentially systemic deficiencies related to VA's system assessment and authorization process. We note that VA is maintaining production systems with "Temporary Authorizations to Operate" that are not based on completed reviews of security authorization packages, in accordance with National Institute of Standards and Technology standards. As a result, VA lacks assurance that system security controls are operating effectively, which could expose veterans' sensitive data to potential loss, fraud, or abuse.

OIG Hotline Allegations

We received a number of allegations through the OIG Hotline regarding ineffective VA information security management and controls that we evaluated as part of our FISMA audit. Specifically:

- VA was hosting medical devices containing sensitive patient information that are not effectively protected from unauthorized access, as required by VA's Medical Device Isolation Architecture.
- VA was misrepresenting information in preparation for the FY 2014 FISMA audit and this effort was consuming excessive resources within OIT.

- A software defect caused the self-service eBenefits portal to inappropriately display veterans' PII to other system users.
- Certain VA Medical Centers were hosting unauthorized systems and networks placing sensitive VA data at risk of loss or inappropriate disclosure.

We are currently working to finalize our analysis of these issues. We will provide conclusive determinations as to the merits of the allegations in our FY 2014 narrative FISMA audit report.

Veterans Health Information Systems and Technology Architecture

We have not evaluated all application modules within the Veterans Health Information Systems and Technology Architecture (VistA) as part of our FISMA audit. VistA was designed to provide an integrated inpatient and outpatient electronic health record for VA patients and administrative tools to help VA deliver medical care to veterans. As part of FISMA, we review selected controls within VistA supporting financial transactions; however, we did not assess the scheduling portion of the system.

The effectiveness of this patient scheduling system came into question as part of our review of allegations regarding inaccurate veteran wait times at the Phoenix VA Healthcare System. In late April 2014, we learned that certain audit controls within VistA were not enabled, which limited our ability to determine whether any malicious manipulation of the VistA data occurred. At our request, VA enabled this audit trail capability at Phoenix and nationwide. Inadequate use of system audit trails appears to be a systemic issue within VA. Specifically, as part of our FY 2014 consolidated financial statement and FISMA audits, we found that security event logs were not consistently maintained or reviewed across VA facilities. By not enforcing consistent use of audit logs for all systems, unauthorized system access and use may go undetected, placing sensitive VA data at unnecessary risk.

To facilitate our review of patient wait times, we also requested that OIT discontinue deleting VistA accounts for former employees and instead place these accounts in a disabled state so that we can evaluate system use and scheduling data. OIT complied with these requests. It may take VA several years to deploy the new patient scheduling system currently under development. The OIG is committed to performing additional scrutiny of the functionality and data integrity of this system as part of future reviews.

Cloud Computing

In February 2013, we communicated concerns to VA regarding its intent to migrate its email systems to a cloud service provider. Specifically, VA moved 15,000 email user accounts to a cloud-based system as part of a pilot study and planned to migrate the remaining 600,000 email user accounts to the virtual cloud environment thereafter. As a result, VA email messages were planned to be hosted on a contractor-owned and operated system.

Upon OIG review of the underlying contract, we noted the contract did not require the cloud service provider to allow OIG access to VA systems and data stored at the contractor facilities. Consequently, the OIG would not have legal access to VA systems

and data needed for investigative and oversight purposes. Further, the contract terms would potentially compromise our efforts to ensure that annual FISMA requirements are met. The contract lacked requirements for the cloud service provider to segregate VA sensitive data from other customer data, potentially impeding OIG investigations and creating new information security weaknesses involving VA electronic data. VA planned to adopt a policy to delete cloud-hosted emails greater than 90 days old in an effort to save costs with the cloud-based contract. Email is integral to the manner in which VA conducts day-to-day business. As such, retention of emails is critical to support VA work, OIG investigations and oversight reviews, and to defend VA actions in the administrative and judicial appellate systems.

In April 2013, the OIG issued a memorandum to the then-Deputy Secretary Scott Gould requesting that VA cease further contracting to put VA data in the cloud until all mission requirements of the OIG, VA General Counsel, and other VA administrations were met. Further, we requested that VA users not delete any email from any VA system until record management systems are established providing a minimum retention period of 7 years. We requested that all cloud-based systems be assessed at a "high" impact risk level to ensure that VA sensitive data are physically and logically segregated from other customer data hosted on the same virtual computer platforms. After several discussions with VA senior leadership, the then-Deputy Secretary directed that OIT terminate the email cloud-based contract because of concerns regarding retention of emails raised primarily by the OIG, as well as by General Counsel.

Foreign Hackers

In June 2013, we met with OIT to discuss whether VA networks have been compromised by foreign nation-state sponsored cyber espionage groups. OIT disclosed that since 2010, multiple external espionage groups have infiltrated VA networks and are actively attacking systems throughout the enterprise. Furthermore, OIT revealed that an Active Directory Domain Controller had been compromised, allowing malicious intruders to move laterally throughout the VA network. OIT stated that after identifying the compromised system, it devoted significant resources for more than a year in efforts to eradicate this threat, including requiring password resets for all affected systems. OIT admits that certain threat groups may still have access to VA systems using unauthorized user accounts. As such, OIT is still actively monitoring VA networks for evidence of system compromises today. We understand the Committee has asked the GAO to review whether the risks associated with foreign hackers on the VA network still exist. To not duplicate oversight efforts, we did not perform the additional tests needed to assess these risks.

PII Transmission Over Unsecure Internet Connections

In March 2013, we reported that VA was transmitting sensitive data, including PII and internal network routing information, over an unencrypted telecommunications carrier network.[1] VA disclosed that personnel typically transfer unencrypted sensitive data, such as electronic health records and internal Internet protocol addresses, among

[1] *Review of Alleged Transmission of Sensitive VA Data Over Internet Connections* (March 6, 2013).

certain VA Medical Centers and Community-Based Outpatient Clinics using an unencrypted telecommunications carrier network. OIT acknowledged this practice and formally accepted the security risk of potentially losing or misusing the sensitive information exchanged.

These risks continue to exist across VA's enterprise. Despite concurring with our report findings and recommendations, VA has not implemented the technical configuration controls needed to ensure encryption of sensitive data in accordance with 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.

CONCLUSION

Our work has demonstrated that VA continues to struggle to effectively secure its IT systems. Some improvements in information security management have been realized with the inception of CRISP. However, more work remains to be done. Until a proven process is in place to address the OIG's outstanding report recommendations and ensure control across the enterprise, the IT material weakness will stand and VA's mission-critical systems and sensitive veterans' data will remain at risk of attack or compromise. IT shortfalls mean not only exposure of millions of veterans to potential loss of privacy, identity theft, and other financial crimes, they also constitute poor financial stewardship of taxpayer dollars.

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

United States Government Accountability Office

GAO

Testimony
Before the Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at 1:30 p.m. ET
Tuesday, November 18, 2014

INFORMATION SECURITY

Additional Actions Needed to Address Vulnerabilities That Put VA Data at Risk

Statement of Gregory C. Wilshusen, Director
Information Security Issues

Chairman Miller, Ranking Member Michaud, and Members of the Committee:

Thank you for inviting me to testify at today's hearing on information security weaknesses at the Department of Veterans Affairs (VA). Securing its information and systems is particularly critical for VA because its mission of promoting the health, welfare, and dignity of our nation's veterans requires it to collect and maintain sensitive personal information in the course of, for example, providing medical care to veterans. While federal law, primarily the Federal Information Security Management Act of 2002 (FISMA),[1] requires federal agencies to implement an agency-wide information security program, protecting information and systems is a major challenge for the federal government. We first designated the protection of federal information systems as a government-wide high-risk area in 1997 and continued to do so in the most recent update to our high-risk series.[2]

As you know, VA has faced long-standing challenges in its efforts to secure its information and information systems. For example, as we have previously testified, VA has consistently had weaknesses in key information security control areas.[3] Moreover, reports of incidents affecting VA's systems highlight the serious impact that inadequate information security can have on the confidentiality, integrity, and availability of veterans' personal information. For instance, in January 2014, a software defect in a VA system used by veterans to access personal information and services allowed users to view the personal information of other veterans, potentially affecting 1,301 veterans or their dependents, according to a VA official.

My statement today will summarize the key findings from our November 13, 2014, report on VA's efforts to address previously identified information security vulnerabilities.[4] These weaknesses pertained

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

[2]GAO, *High-Risk Series: An Update*, GAO-13-283 (Washington, D.C.: Feb. 14, 2013).

[3]GAO, *Information Security: VA Needs to Address Long-Standing Challenges*, GAO-14-469T (Washington, D.C.: Mar. 25, 2014).

[4]GAO, *Information Security: VA Needs to Address Identified Vulnerabilities*, GAO-15-117 (Washington, D.C.: Nov. 13, 2014).

specifically to incident response efforts, vulnerabilities in key web applications,[5] and vulnerabilities in devices connected to VA's network.

To conduct our work, we reviewed the results of VA security testing; interviewed department officials; and reviewed policies, procedures, and other documentation. Further details on the objective, scope, and methodology of our review can be found in the report. The work on which this statement is based was conducted in accordance with generally accepted government auditing standards.

VA Has Not Fully Addressed Previously Identified Security Vulnerabilities

VA has taken actions to mitigate previously identified vulnerabilities, but more needs to be done to fully address these weaknesses:

VA could not demonstrate that its response to a security incident was effective. VA's Network and Security Operations Center (NSOC) took actions to address an incident involving intrusions by "malicious outsiders" identified in 2012. For example, it had identified hosts it believed were affected by the intrusion and taken steps to eradicate the effects from those hosts. The NSOC also documented actions taken to address the incident to the point where staff believed it had been successfully remediated.

However, VA could not demonstrate the effectiveness of its efforts because staff could not locate the associated forensics analysis report or other key materials. Officials explained that digital evidence for incident response was only maintained for 30 days due to constraints on storage space. Subsequently, VA established a standard operating procedure requiring forensics analysis reports to be maintained for 6 years, but allowing the associated digital evidence to be purged after 1 month. This is inconsistent with federal guidance, which calls for records related to security-incident handling to be maintained for 3 years.[6] Without preserving such evidence, VA will be unable to demonstrate the effectiveness of its incident-response measures, and may be hindered in

[5]A web application is software that performs a specific function directly for a user, and is run on a web server (as opposed to a user's desktop) and accessed through a web browser.

[6]National Archives and Records Administration, *General Records Schedule 24: Information Technology Operations and Management Records*, Transmittal No. 22 (April 2010).

assisting law enforcement agencies in investigating and prosecuting cyber crimes.

Moreover, VA had not yet addressed the underlying vulnerability that allowed the 2012 incident to occur. The agency had planned to implement a solution in February 2014 that would have corrected the weakness, but this had not been completed at the time of our review. VA did limit access to the affected system, but this is insufficient to prevent recurrence of such an incident.

With respect to incident response more broadly, we found that the department's NSOC did not have sufficient visibility into VA's computer networks, limiting its ability to detect and respond to incidents. This is because VA policy does not define the NSOC's authority to access activity logs collected at VA data centers. We previously raised the issue of defining incident response roles and responsibilities at VA in an April 2014 report[7] and recommended that VA define the incident response team's level of authority. VA concurred with this recommendation. Implementing this recommendation should include providing the NSOC with authority to review network activity logs.

The NSOC is taking actions to improve its incident response capabilities, such as analyzing how best to restrict access to VA's network and planning to purchase new tools. However, it has not established a time frame for completing these actions.

VA did not fully address weaknesses in key web applications. VA's NSOC had identified eight high-risk vulnerabilities affecting two key web applications that process veterans' sensitive personal information, as well as a critical vulnerability in one of the applications related to the protection of personally identifiable information. As of June 2014, VA had corrected six of the nine vulnerabilities. For example, the department validated that the critical vulnerability involving personally identifiable information had been corrected within 1 week. However, the VA had not validated corrective actions taken for the other three. One of these vulnerabilities had been outstanding for over a year. Further, the department had not developed plans of action and milestones for addressing these

[7]GAO, *Information Security: Agencies Need to Improve Cyber Incident Response Practices*, GAO-14-354 (Washington, D.C.: Apr. 30, 2014).

vulnerabilities, resulting in less assurance that they would be corrected in a timely and effective manner.

In addition, VA did not scan the software code in its web applications using "static analysis" tools, which can identify root causes of software security vulnerabilities.[8] Officials from VA's Office of Cybersecurity stated that the department had begun to use static analysis to conduct source code reviews in January 2013 and had drafted a policy requiring the use of such tools. But as of the time of our review, source code review was occurring for only one of the two applications we reviewed.

VA had not mitigated vulnerabilities in department workstations. VA periodically scans its network devices—predominantly workstations (for example, laptop computers)—for vulnerabilities that have been identified by software vendors. This is consistent with federal guidance and VA policy, which require periodic vulnerability scanning. Specifically, the NSOC scans workstations across the department's network at least monthly and summarizes the most critical vulnerabilities, such as those requiring patches to remediate them.

However, VA has not always addressed identified vulnerabilities in a timely fashion and consistent with department policy. That policy requires critical patches to be applied within 30 days or, in cases where patches cannot be applied or impact performance, the department is to develop compensating controls and/or plans to migrate to newer services that allow security patches and features to be applied. As of May 2014, the 10 most prevalent critical vulnerabilities identified by department scans were software patches that had not been applied. Regarding these missing patches,

- they had been available for periods ranging from 4 to 31 months;
- there were multiple occurrences of each missing patch, ranging from approximately 9,200 to 286,700; and
- each patch was intended to mitigate multiple vulnerabilities, ranging from 5 to 51, with a total of 301 vulnerabilities.

[8]Various tools, such as "static analysis" tools, can scan software source code, identify root causes of software security vulnerabilities, and correlate and prioritize results. The National Institute of Standards and Technology states that vulnerability analyses for custom software applications may require additional approaches, such as static analysis. This type of analysis can help developers identify and reduce or eliminate potential flaws.

While VA had decided not to apply the top three critical patches until testing could determine the effect they would have on various applications, this decision was made after the patches had been available for 3 to 10 months, exceeding the 30-day requirement for applying critical patches. Nor did the department describe compensating controls or plans to migrate to services that would support security features. For the other 7 patches, VA did not provide documentation of any decisions not to apply them.

In addition, scanning procedures VA uses may not identify certain vulnerabilities. Specifically, VA's scans of its non-Windows systems, such as Linux systems, were conducted in "unauthenticated" mode. This means that the scans did not test as a logged-in user of the systems, which would allow for the examination of additional security controls. Thus, vulnerabilities on these systems may go undetected.

VA has efforts under way to improve its vulnerability remediation. In May 2013 it established an organization tasked with overseeing processes for vulnerability remediation, among other things. Moreover, the organization has taken steps to carry out its responsibilities by, for example, planning to create a database to track remediation and patch implementation. However, the department has yet to establish specific actions, priorities, and milestones for the organization to carry out its tasks. Establishing such elements contributes to evaluating progress, achieving results, and ensuring effective oversight.

Implementing GAO's Recommendations Can Help VA Mitigate Weaknesses

In our report, we made eight recommendations to VA to address the previously identified security vulnerabilities:

- Update the department's standard operating procedure to require evidence associated with security incidents to be maintained for at least 3 years.
- Fully implement the solution to address the weakness that led to the 2012 intrusion.
- Establish time frames for completing planned actions to improve incident response.
- Develop plans of action and milestones to address critical and high-risk vulnerabilities in the two key web applications.
- Finalize and implement the policy requiring source code scans on key web applications.

- Apply missing security patches within established time frames or document compensating controls and/or plans to migrate to newer services that support security features.
- Scan non-Windows (e.g., Linux) network devices in authenticated mode.
- Identify actions, priorities, and milestones for tasks related to vulnerability remediation.

In comments on a draft of our report, VA stated that it generally agreed with our conclusions and concurred with our recommendations. VA also stated that it had already taken actions to address six of our eight recommendations and has plans in place to address the other two. However, we have not yet validated the actions described or determined whether they effectively address the issues raised in the report. Moreover, we are concerned that VA's described actions for two of the recommendations may not fully address the identified weaknesses. We intend to monitor VA's implementation of our recommendations.

In summary, while the department has taken steps to respond to incidents and identify and mitigate vulnerabilities, ensuring effective information security remains a challenge for VA. Shortcomings in its incident response activities, vulnerabilities in key web applications, and weaknesses in the management of security on its network devices place the sensitive personal information entrusted to the department at increased risk of unauthorized access, modification, disclosure, or loss. Our recommendations, if properly implemented, should help the department improve its security posture and better protect this information.

Chairman Miller, Ranking Member Michaud, and Members of the Committee, this concludes my statement. I would be pleased to answer any questions you may have.

Contact and Staff Acknowledgments

If you have any questions about this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or Dr. Nabajyoti Barkakati at (202) 512-4499. We can also be reached by e-mail at wilshuseng@gao.gov and barkakatin@gao.gov. Other key contributors to this testimony include Jeffrey Knott, Lon Chin, Harold Lewis, and Chris Warweg (assistant directors); Jennifer R. Franks; Lee McCracken; and Tyler Mountjoy.

GAO Highlights

Highlights of GAO-15-220T, a testimony before the Committee on Veterans' Affairs, House of Representatives

Why GAO Did This Study

VA relies extensively on information technology systems that collect, process, and store veterans' sensitive personal information. Without adequate safeguards, these systems and information are vulnerable to compromise. Further, VA has faced long-standing challenges in securing its systems, and reported incidents have demonstrated the impact of cyber-based threats on the confidentiality, integrity, and availability of veterans' personal information.

This statement summarizes GAO's November 13, 2014, report on VA efforts to address previously identified information security vulnerabilities. For its review, GAO focused on efforts to respond to a network intrusion, address vulnerabilities in key web-based applications, and remediate weaknesses in devices connected to the department's network. To conduct its work, GAO reviewed the results of VA security testing; interviewed department officials; and reviewed policies, procedures, and other documentation.

What GAO Recommends

In its report, GAO made eight recommendations to VA to fully address weaknesses in incident response, web applications, and patch management. VA concurred with GAO's recommendations.

View GAO-15-220T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov or Dr. Nabajyoti Barkakati at (202) 512-4499 or barkakatin@gao.gov.

November 18, 2014

INFORMATION SECURITY

Additional Actions Needed to Address Vulnerabilities That Put VA Data at Risk

What GAO Found

The Department of Veterans Affairs (VA) has taken actions to mitigate previously identified vulnerabilities, but it has not fully addressed these weaknesses:

- **Incident response:** VA took actions to contain and eradicate the effects of a network intrusion detected in 2012, but it could not show that these actions were fully effective. Specifically, the department's Network and Security Operations Center (NSOC) analyzed the incident and documented actions taken in response, but the department could not provide forensics analysis or digital evidence associated with its efforts. Thus, the effectiveness of its incident response could not be demonstrated. VA policy does not require evidence related to security incidents to be kept for at least 3 years, as recommended by federal guidance. This hinders the department's ability to show its efforts have been effective. Further, VA did not fully address the vulnerability that led to the original incident, increasing the risk that such an incident may recur. In addition, VA policy does not provide the NSOC with sufficient authority to monitor activity on the department's networks, limiting its ability to detect and respond to security incidents.
- **Vulnerabilities in web applications:** VA's NSOC identified nine significant vulnerabilities in two key applications that process veterans' personal information, and validated that the department had corrected six of them. However, corrective actions for the remaining three vulnerabilities had not been validated, and the department had not developed action plans to ensure they were addressed in a timely manner. VA also did not fully implement a type of testing that can identify root causes of security vulnerabilities in application source code.
- **Weaknesses on network devices:** VA periodically scans the devices (e.g., laptop computers) connected to its network for security vulnerabilities and summarizes the most critical vulnerabilities. For May 2014, the 10 most critical vulnerabilities were related to security patches that had not been applied to VA's network devices. These missing patches had been available for periods ranging from 4 to 31 months, even though department policy requires critical patches to be applied within 30 days. While the department documented decisions not to apply 3 of the patches, pending tests of the effect they could have on functionality, it did not document controls to compensate for not applying up-to-date security features. Further, the department did not document any reasons for not applying the other 7 patches. The department has established an organization tasked with remediating security vulnerabilities, but it has not developed specific actions, priorities, and milestones for this organization to carry out its responsibilities.

Until VA fully addresses identified security weaknesses, its systems and the information they contain—including veterans' personal information—will be at an increased risk of unauthorized access, modification, disclosure, or loss.