LEGISLATIVE HEARING ON H.R. 571, H.R. 593, H.R. 1015, H.R. 1016, H.R. 1017, H.R. 1128, AND H.R. 1129

HEARING

BEFORE THE

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

OF THE

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

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

THURSDAY, MARCH 19, 2015

Serial No. 114–11

Printed for the use of the Committee on Veterans' Affairs

U.S. GOVERNMENT PUBLISHING OFFICE

98–628 WASHINGTON : 2016

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
DAN BENISHEK, Michigan
TIM HUELSKAMP, Kansas
MIKE COFFMAN, Colorado
BRAD R. WENSTRUP, Ohio
JACKIE WALORSKI, Indiana
RALPH ABRAHAM, Louisiana
LEE ZELDIN, New York
RYAN COSTELLO, Pennsylvania
AMATA COLEMAN RADEWAGEN, American Samoa
MIKE BOST, Illinois

CORRINE BROWN, Florida, *Ranking Minority Member*
MARK TAKANO, California
JULIA BROWNLEY, California
DINA TITUS, Nevada
RAUL RUIZ, California
ANN M. KUSTER, New Hampshire
BETO O'ROURKE, Texas
KATHLEEN RICE, New York
TIMOTHY J. WALZ, Minnesota
JERRY MCNERNEY, California

JON TOWERS, *Staff Director*
DON PHILLIPS, *Democratic Staff Director*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATION

MIKE COFFMAN, Colorado, *Chairman*

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

ANN M. KUSTER, New Hampshire, *Ranking Member*
BETO O'ROURKE, Texas
KATHLEEN RICE, New York
TIMOTHY J. WALZ, Minnesota

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

CONTENTS

Thursday, March 19, 2015

Page

Legislative Hearing on H.R. 571, H.R. 593, H.R. 1015, H.R. 1016, H.R. 1017, H.R. 1128, and H.R. 1129 1

OPENING STATEMENTS

Mike Coffman, Chairman 1
Prepared Statement 36
Ann Kuster, Ranking Member 3
Jeff Miller, Chairman of the Full Committee 4
Prepared Statement 37

WITNESSES

Ms. Meghan Flanz, Director, Office of Accountability Review Department of Veterans Affairs 11
Prepared Statement 38
Accompanied by:
Dr. Michael Icardi, National Director of Pathology and Laboratory Medicine Services, VHA
Mr. Stanley Lowe, Deputy Assistant Secretary for Information Security and Chief Information Security Officer, Department of Veteran Affairs
Mr. Dennis Moisten, CC, Associate Executive Director, Office of Operations, Office of Construction and Facilities Management, Department of Veterans Affairs
Ms. Diane Zumatto, National Legislative Director, AMVETS 26
Prepared Statement 52
Mr. Frank Wilton, Chief Executive Officer, American Association of Tissue Banks 28
Prepared Statement 58
Mr. Daimon E. Geopfert, National Leader, Security and Privacy Consulting, McGladrey, LLP 29
Prepared Statement 62

STATEMENT FOR THE RECORD

American Legion 71

LEGISLATIVE HEARING ON H.R. 571, H.R. 593, H.R. 1015, H.R. 1016, H.R. 1017, H.R. 1128, AND H.R. 1129

Thursday, March 19, 2015

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

The committee met, pursuant to notice, at 8:10 a.m., in Room 334, Cannon House Office Building, Hon. Mike Coffman [chairman of the committee] presiding.

Present: Representatives Kuster, Lamborn, Roe, Benishek, Huelskamp, Walorski, O'Rourke, Rice, Walz, Miller, and Kirkpatrick.

OPENING STATEMENT OF CHAIRMAN MIKE COFFMAN

Mr. COFFMAN. Good morning. This hearing will come to order.

I want to welcome everyone to today's legislative hearing on H.R. 571, H.R. 593, H.R. 1015, H.R. 1016, H.R. 1017, H.R. 1128, and H.R. 1129. The latter two, H.R. 1128 and 1129, are bills suggested for this hearing by the minority. So I will ask Ranking Member Kuster to address them in her opening remarks.

I also welcome full committee Chairman Jeff Miller and ask unanimous consent that Ann Kirkpatrick, the previous Ranking Member of this subcommittee, be allowed to join us at the dais.

Ms. KUSTER. No objection.

Mr. COFFMAN. Okay. While we are at it, I would also like to ask unanimous consent that a statement from the American Legion be entered into the hearing record.

Hearing no objection, so ordered.

[The information follows:]

Mr. COFFMAN. Today we will address H.R. 571, the Veterans Affairs Retaliation Prevention Act of 2015, which was introduced by full committee Chairman Jeff Miller.

This bill will improve the treatment of whistleblower complaints by the VA by defining a set process for whistleblowers, to help correct problems at the lowest level possible, while creating necessary penalties for supervisors who retaliate against whistleblowers.

Second, H.R. 593, the Aurora VA Hospital Refinancing Construction Reform Act of 2015. It is a bipartisan bill I introduced along with the rest of the Colorado delegation. H.R. 593 would increase the authorization cap to help the VA to finally finish the Aurora Medical Center with the much-needed help of the Army Corps of

Engineers, in order to give Colorado veterans the state-of-the-art medical facility they deserve. Since this bill's introduction, the VA has announced that the Aurora project will cost at least $1.73 billion, a full $1.4 billion over the original costs found in GAO's report. This is simply outrageous and could very well make the hospital the most expensive in our nation's history.

Notably, according to GAO, the New Orleans VA Hospital construction project will top $1 billion as well. So mismanagement, cost overruns and delays are the norm of VA's construction program. For that reason, I question whether the VA should conduct its own major construction at all. While it is my top priority to get this hospital built so that Colorado veterans get the service they deserve, we simply cannot authorize the nearly $1 billion authorization cap increase without VA presenting the options it has to correct its own poor decisions with only half of a hospital to show for it.

The VA has reprogrammed a portion of the funds needed to finish the Aurora construction project, but it cannot continue to pull money from other projects, thereby robbing other veterans around the country of a timely completion of their hospital. Perhaps we could use VA bonuses to provide funding for this grossly mismanaged project.

But what is absolutely clear is that before any money is given to the VA to bail them out of this mess they created in Aurora, VA construction officials responsible for this travesty must be held accountable. These individuals should not be simply taken out of the chain of command for VA construction, they should be fired. If anyone in the private sector allowed a project under its supervision to get $1 billion over budget, the decision to fire them would be simple. That should happen here and I look forward to our discussion today with VA on ways forward.

Third, we will address H.R. 1015, the Protection of Business Opportunities for Veterans Act of 2015, sponsored by the Honorable Tim Huelskamp of Kansas.

H.R. 1015 will make tremendous strides at holding accountable the bad actors that attempt to defraud veteran-owned small businesses of crucial set-asides they receive in business.

Fourth, we will discuss H.R. 1016, the Biological Impact Tracking and Veterans' Safety Act of 2015, introduced by the Honorable Phil Roe of Tennessee.

This legislation requires the VA to implement a standard identification protocol for biological implants consistent with the FDA's system, which would improve VA's ability to prevent implantation of contaminated tissue, and also to notify veterans in cases of recalls.

Fifth, we will hear about H.R. 1017, the Veterans Information and Security Improvement Act, which was sponsored by the Honorable Jackie Walorski from Indiana.

This IT security directive is designed to assist VA in mitigating known weaknesses by identifying detailed actions that should be taken to address its longstanding information security challenges.

Once again, I would like to thank all those in attendance for joining us in our discussion today. And I now recognize Ranking Member Kuster for five minutes to issue her opening statement.

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

OPENING STATEMENT OF RANKING MEMBER ANN KUSTER

Ms. KUSTER. Thank you very much, Mr. Chair. And I want to say at the outset, I am delighted to be here with you and I look forward to our work together on the Oversight and Investigations Subcommittee.

Welcome our panel this morning. The subcommittee will hear the views of the VA and our witnesses regarding seven bills before us, as outlined by our chair. These bills address concerns over the VA's whistleblower protections, cyber security measures, tracking biological implants, and other important matters.

These legislative hearings are vital as the subcommittee begins our work to ensure that the important legislation moves forward, that requirements are measured, and ultimately that we are working to fix and improve the problems discussed today. None of us have all the answers. By hearing the opinions of many, we can better ensure that we are effectively addressing these problems at the VA that lend themselves to oversight and legislative fixes.

I thank the Chairman for including two measures introduced by my predecessor as ranking member on this subcommittee, Representative Ann Kirkpatrick, who will be with us this morning.

H.R. 1129 addresses the manner in which the VA investigates the complaints of whistleblowers, while ensuring cooperation and coordination with the Office of Special Counsel and the VA Inspector General. The VA has made great strides in setting up the Office of Accountability Review, but I am interested in exploring whether more needs to be done and whether the office primarily responsible for handling investigations outside the scope of the OSC or IG is better positioned outside the VHA. I am also interested in exploring whether the idea of centralizing complaints in a specific office could lead to better VA-wide accountability and responsiveness for our veterans.

H.R. 1128 is a response to cyber security concerns within the VA and how best to balance the competing interests of ensuring that the VA has the proper tools to fulfill its mission, while also ensuring that information is kept as secure as possible. Cyber security is an ever growing threat and problem and new tools and tactics are developed daily, both by those intent on improperly collecting information and the efforts of the Federal Government and the private sector to protect our information.

I look forward to working with the chairman and my colleagues as we look at these bills before us today and begin the process of matching solutions to problems in the most effective manner possible.

Ms. KUSTER. Thank you, and I yield back.

Mr. COFFMAN. Thank you, Ranking Member Kuster.

We will now hear from Chairman Jeff Miller from the State of Florida, who will be speaking in support of H.R. 571, the Veterans Affairs Retaliation Prevention Act of 2015.

OPENING STATEMENT OF CHAIRMAN JEFF MILLER OF THE FULL COMMITTEE

Chairman Miller.

Mr. MILLER. Thank you for the recognition, Mr. Chairman. It is a pleasure to be with you.

I want to echo your comments in your opening statement as it relates to the fiasco at the Aurora facility. Your Denver Post yesterday aptly headlined an editorial, "Still No Accountability," and I don't see any on the horizon. To think that this Congress would raise an existing legislative cap of $800 million by almost a billion more without a plan and a way ahead is absolutely ludicrous.

And we as a committee, both Republicans and Democrats, have been asking for an answer from VA for really months now, but the investigation, as you well know—and I salute you, your current ranking member and your former ranking member for delving into it deeply to try to get a solution out in front of the VA and, unfortunately, they did not heed many of the warnings that were given. Unfortunately, the individuals that were in charge are still employed by the VA, several of them receiving very generous bonuses for their ineptitude and their incompetence. And to still be employed by the taxpayers after this debacle is egregious. So I want to thank you for your diligence and the entire Colorado delegation in staying on top of the issue.

I want to talk about H.R. 571, which is the Veterans Affairs Retaliation Prevention Act of 2015. You know, we could name it anything, the Whistleblower Protection Act, whatever it may happen to be. But you all know during 2014 when the scandal erupted basically around Phoenix we found it was much more systemic, that retaliation and bureaucrat corruption really gripped the VA because people were fearful, but there were whistleblowers that were trying to come forward and do the right thing and let people know that there were problems that existed within the VA. And the hallmark of the culture that existed there remains really rampant today within the VA against VA employees who speak up to try to fix problems that exist within the agency.

So these problems were so widespread in 2014 that the Office of Special Counsel was inundated with more whistleblower complaints than all the other federal government agencies combined. Unfortunately, despite promises from the leadership at VA at that time that whistleblower retaliation would no longer be tolerated, occurrences continue within the agency and a lack of any meaningful accountability shows that it is really not the case. Proper oversight of any federal agency cannot be done effectively without employees within that agency informing the Congress and other oversight bodies of what is going on. Over the years, numerous federal statutes have been passed to provide added protection to whistleblowers, but many VA supervisors have found a way to really circumvent the law that is there to protect these individuals and hopefully encourage them to come forward and bring information to the bodies that need them to do their oversight. And this bill intends to put an end to the retribution and the repercussions.

Specifically, H.R. 571 would provide VA employees who seek to report potential government waste, criminal behavior or compromised healthcare services within the VA a set process to fix

problems at the lower level possible while affording them improved protection from retaliation. This legislation will also prohibit superiors from retaliating against employees who report or assist in reporting problems to the VA, to the Inspector General, to Congress, or the GAO. Employees who serve as a witness in investigations and those who refuse to perform illegal acts in the course of their employment will also be protected. To ensure accountability, this bill will provide meaningful penalties to VA employees who are found to have retaliated against another employee for filing, simply filing a whistleblower complaint.

Specifically, the retaliating employee should receive a suspension or removal from federal service, a fine to repay the expense borne by the Federal Government in defending their retaliatory behavior, a forfeiture of bonuses received while the retaliation occurred, and a prohibition of receiving future bonuses for a one-year period.

Finally, this legislation requires improved training to be provided to all VA employees on the protections that are afforded to employees that are making complaints and the repercussions that retaliating employees will face if they seek to suppress positive change.

Look, our American veterans deserve no more than the quality services that VA provides and those benefits that they have earned. So improvements of those services often come in the form of suggested fixes by employees. And this commonsense legislation, we all do commonsense legislation, this bill certainly is one of them, would provide the process to safely suggest these fixes while giving Secretary McDonald and all secretaries in the future the tools to hold accountable employees who seek to prevent change within their agency.

So I look forward to working with this subcommittee, our veterans service organization partners in the VA and other stakeholders on this bill, because protecting the conscientious VA employees who report waste and wrongdoing within VA must be among our constant priorities.

I appreciate you, Mr. Chairman, to the ranking member, Ms. Kuster, for holding this hearing and for your hard work and leadership on this Subcommittee on Oversight and Investigation. I appreciate really the opportunity to be with you this morning.

[THE PREPARED STATEMENT OF CHAIRMAN JEFF MILLER OF THE FULL COMMITTEE APPEARS IN THE APPENDIX]

Mr. MILLER. I yield back.

Mr. COFFMAN. Thank you, Chairman Miller.

Now we will hear from the Honorable Tim Huelskamp from the State of Kansas, who will discuss his bill, H.R. 1015, the Protecting Business Opportunities for Veterans Act of 2015.

Dr. HUELSKAMP. Thank you, Mr. Chairman, for the opportunity to testify in support of H.R. 1015, the Protecting Business Opportunities for Veterans Act.

Over the years, this committee has received testimony, Inspector General's reports and other reports of numerous entities who illicitly took advantage of set-asides rightly reserved for service-disabled-veteran-owned small businesses. As a member of this subcommittee, as well as the House Small Business Committee, I am very concerned about the fraud and abuse of these programs, and I think they need stricter oversight and enforcement. This act

would apply to those small business concerns owned and controlled by a veteran with a service disability, as well as small businesses controlled by veterans who received federal contracts from the VA.

The bill is fairly simply. It requires that as part of the contract, the VA must obtain a certification the business will comply with the requirements already written into the law, and it will specifically specify how they intend to meet the requirement 50 percent of the contracted service work be performed by a veteran-owned business or a service-disabled-veteran-owned business with this certification, as well as a requirement that the Office of Small Business and Disadvantaged Business Utilization and the VA's Chief Acquisition Officer will implement a process that will allow better oversight and enforcement of what we all intended in the law and that is to make certain these set-asides go to veterans.

With these changes, law enforcement will have the necessary tools to crack down on corrupt contractors who use these pass-throughs and other methods to take advantage of set-asides that should be and are lawfully reserved for veterans. I think the bill is necessary to direct the office and the VA chief acquisition officer to do what they should have been doing all along, and that is to monitor and enforce compliance.

We have had a hearing on this last year and moved this through the committee, and I am bringing it back forward because, again, I want to make sure these contracts are accessed and are taken advantage by deserving veterans and not some of these illicit contracts, Mr. Chairman. So I appreciate the opportunity to visit very quickly about it. Again, we have discussed this before and hopefully we can move forward again. I yield back.

Mr. COFFMAN. Thank you, Dr. Huelskamp.

We will now hear from the Honorable Phil Roe from the State of Tennessee, who will be speaking in support of his bill, H.R. 1016, the Biological Implant Tracking and Veterans' Safety Act of 2015.

Dr. Roe.

Dr. ROE. Thank you and the ranking member for allowing me to be here this morning and speak.

And just to reiterate what the Chairman said in the Aurora, I didn't think it was possible to make politicians speechless, but they have succeeded beyond my wildest expectations. And I look at a billion dollars at how much veterans' healthcare you can provide, physical therapy, medications, cancer surgery, whatever the therapy may be that is not available in a limited budget.

And I looked at this and, having helped run hospitals and medical practices, the interest payments alone on this if you were in the private world would be over $70 million a year. That is not paying it off. You would have to cash-flow that, your operating expenses, your salaries, your depreciation, all of those things. There is no way that this could possibly function. And I am one vote, but I am not going to vote for another penny until I go visit that place and I have some assurances that the veterans are going to get what they are paying—the taxpayers are going to get what they are paying for. I mean, I think we have to do that as a committee.

And I certainly commend you all for keeping an eye on this, Mr. Chairman, and I thank you for that. And, Doug, you too. I know you are frustrated and I am too, I share your frustration. But

thank you all and it is a pleasure to present H.R. 1016, the Biological Implant Tracking and Veterans' Safety Act, before this committee for consideration.

A frightening GAO report in January of 2014 found that the VA does not use a standardized process for tracking biological tissue from cadaver donor to living veteran recipients. In the event of a recall, it would be virtually impossible to track down which patient had received the contaminated tissue. The same GAO report detailed that the Veterans Health Administration does not always ensure they are purchasing tissue from biological implant vendors that have registered with the FDA and does not maintain an inventory system to keep the expired tissues from remaining in storage alongside unexpired tissues.

This GAO report and our VA committee staff had discovered that the VA often uses a loophole in Title 38 of the U.S. Code 8123 that allows it to buy biological implants on the open, unregulated market, which it does in 57 percent of its biological implant purchases. H.R. 1016 would require the procurement of biological implants from vendors on the federal supply schedules which have been appropriately vetted for biological implants not on the federal supply schedule but requested by clinicians. My bill requires justification and approval of open-market purchases under the federal acquisitions regulation on a case-by-case basis, rather than simply granting a blanket waiver as provided in Title 38.

H.R. 1016 would direct the Secretary of Veterans Affairs to adopt the FDA's unique device identification system for labeling of all biological implant tissue and implement an automated inventory system to track the tissue from donor to implant recipient. This legislation would also require all biological implant tissue to be procured through vendors that are registered with the FDA, accredited by the American Association of Tissue Banks, and use FDA's unique device identification system.

Mr. Chairman, the six million veterans served annually by VHA deserve the high standard of patient care in the nation. Implementation of H.R. 1016 would help establish the VA as an industry leader in biological implant safety and accountability.

I want to thank the Oversight and Investigation subcommittee staff for their help in developing this legislation, which truly puts veterans patients first.

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

Mr. COFFMAN. Thank you, Dr. Roe.

We will now hear from the Honorable Jackie Walorski from Indiana, who will be speaking about her directive, the Veterans Information and Security Improvement Act.

Ms. Walorski.

Ms. WALORSKI. Thank you very much, Mr. Chairman. Good morning to all my fellow colleagues.

This H.R. 1017 comes from feedback the committee received at a members-only briefing in December of 2013, which the VA, the VA's Office of Inspector General and the Government Accountability Office all attended. At this briefing, the committee provided an overview of VA's information security vulnerabilities using VA's own internal documents and previous testimony from VA's IG.

The committee has had numerous meetings, sent letters and held a hearing in November of 2014 to address IT security weaknesses. Unfortunately, VA's lack of cooperation has been a longstanding issue that continues to this day. Independent information security experts verified HVAC's findings about the VA's critical network vulnerabilities, including the following.

Within VA's 420,000 computers, there are five vulnerabilities on 95 percent of those computers. VA employs tens of thousands of outdated operating units. Because of VISTA's vulnerabilities, VA stated that a data breach to financial, medical and personal veteran and employee information will occur with no way of tracking the source of the breach. VA's network has been compromised at least ten times since March, 2010.

And finally, and probably most troubling, is that the VA recently proclaimed they had a clean bill of health on network security. However, the committee found that a state actor had penetrated VA's network around September of 2014. This was substantiated by another government entity, after which the committee briefed Secretary McDonald. VA was not aware of the intrusion, which by all accounts was then not detected by VA's CRISP Einstein 3 or by any active review being conducted by a third-party contractor.

Over the past 20 years, VA's independent auditor, the IG and the GAO have all reported numerous persistent weaknesses in the VA's security, placing veterans' personal information at risk. Despite the GAO's and IG's testimony and the committee's evidence that came from the VA itself, VA officials did not agree with our findings from the briefing. They will not acknowledge that critical security vulnerabilities exist.

It is important to understand the critical nature of the security failures we are discussing today. These failures are not due to a lack of resources, they are due to a lack of priorities, leadership and proper federal guidance. We need stronger, more focused action to ensure the VA fully implements a robust security program. That is why we need this bill.

I am confident this directive will provide VA with a clear IT roadmap and take away any guesswork in order to achieve a risk-based approach to addressing these challenges. GAO and a number of private sector companies also agreed and stated that if the directive is implemented it will allow VA to refocus its efforts on steps needed to improve the security of its systems and information.

This bill establishes an explicit plan of action to resolve VA's IT security weakness identified by the committee and others. The plan is taken from common federal and industry best practices.

Specifically, the bill directs the secretary to do the following. Reclaim, secure and safeguard VA's network; defend the work stations from critical security vulnerabilities; upgrade or phase out unsupported and outdated operating systems; secure Web applications from vital vulnerabilities; protect VISTA from anonymous user access; and comply with federal information security laws, OMB guidance and NIST standards.

To improve transparency and accountability, the bill also directs the secretary to submit to the committee a biannual report, including a description of the actions taken by the secretary to implement and comply with this directive. The IG will also be required to sub-

mit to the committee an annual report that includes a comprehensive review of VA's execution of this directive.

Finally, on a monthly basis the secretary will submit to the committee reports on any discovered security weaknesses.

Thank you, Mr. Chairman. I yield back.

Mr. COFFMAN. Thank you, Ms. Walorski.

We will now hear from the Honorable Ann Kirkpatrick from Arizona, who will discuss her bills, H.R. 1128, the Department of Veterans Affairs Cyber Security Protection Act, and H.R. 1129, the Veterans Whistleblower and Patient Protection Act of 2015.

Ms. KIRKPATRICK. Thank you, Chairman Coffman and Ranking Member Kuster. Members of the committee and staff, it is nice to see you this morning. And I really thank you for all you are doing for our veterans and I appreciate that you included my two bills in this hearing. So thank you very much.

H.R. 1128, the Department of Veterans Affairs Cyber Security Protection Act, and H.R. 1129, the Veterans Whistleblower and Patient Protection Act of 2015, are two bills that will improve the lives of veterans. They will bring much needed accountability to the VA and protect VA employees and patients who report wrongdoing.

The Cyber Security Protection Act aims to protect veterans' personal information and improve VA information security without compromising the VA's mission to provide healthcare benefits and services to veterans.

After reported VA network compromises in a GAO report last year that found VA IT networks were vulnerable to security breaches, I believe legislation is necessary to ensure the VA takes appropriate measures to safeguard veterans' personal information. This bill offers commonsense steps to do just that.

First, it requires the VA to report quarterly to Congress on actions and plans to address known information security vulnerabilities and provide a timetable for addressing them.

Second, it mandates a report on VA actions to hold employees accountable for data breaches. The report would include VA's proposed reorganization of its information security infrastructure.

Third, it requires the VA to develop an information security strategic plan that protects veterans' information and anticipates future cyber security threats. It requires the VA to recruit and train employees with skills and expertise in information security, and to update VA information technology.

This bill is not creating requirements that are so rigid that the VA is unable to perform vital services such as referring patients to other healthcare providers or granting veterans and families the benefits they deserve. I urge all of you to support this bill.

As a member of the House Veterans' Affairs Committee in the previous congress, I sat through hearing after hearing with many of you after whistleblowers at the Phoenix VA and other VA medical facilities exposed a VA-wide patient access crisis and the manipulation of patient access data. Last month I heard from two whistleblowers at the Phoenix VA, who reported mismanagement of the Phoenix VA's suicide prevention and substance abuse treatment program.

If not for the courage of these whistleblowers, it is unknown how long these practices would continue to persist. Unfortunately, many

VA employees or patients who attempt to report wrongdoing face retaliation.

The Veterans Whistleblower and Patient Protection Act of 2015 would encourage those who wish to report wrongdoing to come forward without fear of retaliation. This bill would ensure that the whistleblower retaliation reports and patient complaints are handled at the highest level in the office of the VA secretary. This ensures that anyone reporting wrongdoing does not risk retaliation from local supervisors who refuse to act.

This office of whistleblower and patient protection would equip the secretary with an investigatory arm to take action on allegations. The office would create one national hotline for VA employees and patients to anonymously report whistleblower retaliation or patient safety and treatment complaints, investigate patient claims, and serve as the only VA office permitted to investigate whistleblower retaliation complaints. It would report the results of its investigations and recommend actions to the VA secretary, and coordinate efforts between the VA Office of Inspector General and the Office of Special Counsel to ensure complaints are thoroughly investigated and to prevent duplicate investigations.

We can continue writing letter after letter to the VA secretary asking for the protection of VA whistleblowers' rights as more of our constituents come forward or we can pass legislation that will address this issue.

Again, I urge the members of the committee to support the bill. I know that many of you on the committee have similar legislation and I just want to say I look forward to working with you, so that we can merge this legislation into one good bill that we can pass out of the House of Representatives and really make a difference for our veterans. So thank you very much.

I yield back.

Mr. COFFMAN. Thank you, Ms. Kirkpatrick.

On our first panel, we will hear from Ms. Meghan Flanz, Director of the VA's Office of Accountability Review. She is accompanied by Dr. Michael Icardi, the National Director of Pathology and Laboratory Medicine Services for the Veterans Health Administration; Mr. Stanley Lowe, Deputy Assistant Secretary for Information Security and VA Chief Information Security Officer; Mr. Dennis Milsten, Associate Executive Director for the Office of Operations, Office of Construction and Facilities Management for the Department of Veterans Affairs.

Ms. Flanz, you are now recognized for five minutes to provide your opening remarks.

STATEMENT OF MEGHAN FLANZ, DIRECTOR, OFFICE OF ACCOUNTABILITY REVIEW, DEPARTMENT OF VETERANS AFFAIRS. ACCOMPANIED BY: DR. MICHAEL ICARDI, NATIONAL DIRECTOR OF PATHOLOGY AND LABORATORY MEDICINE SERVICES, VETERANS HEALTH ADMINISTRATION; STANLEY LOWE, DEPUTY ASSISTANT SECRETARY AND CHIEF INFORMATION SECURITY OFFICER, DEPARTMENT OF VETERANS AFFAIRS; DENNIS MILSTEN, ASSOCIATE EXECUTIVE DIRECTOR, OFFICE OF OPERATIONS, OFFICE OF CONSTRUCTION AND FACILITIES MANAGEMENT, DEPARTMENT OF VETERANS AFFAIRS

STATEMENT OF MEGHAN FLANZ

Ms. FLANZ. Good morning and thank you, Mr. Chairman, Ranking Member Kuster, and other members of the subcommittee.

We appreciate the opportunity to be here today to discuss VA's views on the seven bills that do cover a wide range of topics, whistleblower protection, how VHA handles biological implants, information technology, small business contracting, and VA's Denver hospital project.

Because the committee has our detailed written statement on the bills in hand, I will limit my remarks to our brief observations on each bill, so we can then focus our time on answering your questions.

Two of the bills today concern whistleblower rights and protections. VA has certainly had and continues to have problems ensuring that whistleblower disclosures receive prompt and effective attention, and that whistleblowers themselves are protected from retaliation. It is critical that all VA employees and supervisors share trust and mutual respect as they share information, especially if an employee is seeing something that is not working for the benefit of our veterans, something that is against the law, or something that is just not right.

VA is absolutely committed to ensuring fair treatment for employees who bring these deficiencies to light. We are collaborating closely with the Office of Special Counsel, the independent office responsible for overseeing whistleblower disclosures and retaliation claims, to ensure that all VA supervisors understand their roles and responsibilities and to speed assistance to any employee who may be experiencing retaliation.

Mr. Chairman, we believe strong leadership, effective training and close collaboration with OSC and with this committee are the keys to the cultural change the department requires. Our employees and the veterans we serve depend on the work you and our other stakeholders are doing to address our deficiencies head on. And of course we are eager to discuss these efforts with you and to get the benefit of your insights.

VA understands the urge toward legislative action in the wake of reports of troubling individual VA whistleblower cases. However, as we have detailed in our written testimony, we are concerned that some aspects of H.R. 571 would be unworkable in practice and could lead to unintended negative consequences. We are particularly concerned that the bill adopts a one-size-fits-all rule that would impose the same investigative, reporting and disciplinary re-

quirements on all VA supervisors regardless of their grade or function.

It is important to note that VA has more than 30,000 supervisors, fewer than 500 of whom are senior executives. Many of our first-level supervisors have only minimal education and are at relatively low pay grades. While of course all supervisors must respond appropriately to employees' disclosures and all must protect employees from retaliation, we believe the processes by which supervisors respond to employee disclosures must be calibrated to different supervisors' capabilities and roles. We also want to protect the trusting, well-balanced supervisor-subordinate relationships that do exist in many VA work units while correcting relationships that are out of balance or otherwise not working well.

H.R. 1129 focuses on a centralized process for investigation of disclosures. We are concerned that this bill might unnecessarily duplicate or replace existing functions now belonging to OSC, to VA's reconfigured Office of the Medical Inspector, or to the Office of the Inspector General.

Also on the agenda today is H.R. 593, which would extend the authorization for the replacement major medical facility in Denver and set out requirements for an agreement with the Army Corps of Engineers to carry that project to conclusion. Needless to say, VA is determined to overcome earlier setbacks in this project to put it on the best track for success for Colorado veterans. We understand that the committee has questions and concerns about that project and Mr. Milsten is prepared to address those in detail.

Also on the agenda are two bills regarding information technology, particularly information security. We appreciate the goals of H.R. 1017, but as we have stated, we are concerned that detailed statutory requirements for management of IT operations might prove too inflexible for VA to respond effectively to the constantly evolving cyber security landscape.

H.R. 1128 does use a less prescriptive approach. VA appreciates and supports the goals of the bill and has no objection to some of the reporting requirements, but is concerned that some requirements might be quite onerous relative to the benefits they would yield. VA will be glad to work with the committee on those aspects of H.R. 1128 that appear problematic.

H.R. 1016 would require VA to adopt specific systems and protocols for the procurement and tracking of biological implants, and would set requirements for inspections and audits. As our written testimony has stated, VA agrees with the general purpose of the bill, but has concerns about some specifics. Dr. Icardi can address those matters in detail.

Finally, VA has reviewed H.R. 1015, the Protecting Business Opportunities for Veterans Act of 2015. While we support the goal of the bill, we would like to clarify some technical issues and ambiguities before we set out a position on it. I know VA's small business program and procurement specialists will be glad to follow up with the committee on that bill.

Mr. Chairman, thank you again for the opportunity to testify. We are now glad to answer questions the members of the committee may have.

[THE PREPARED STATEMENT OF MEGHAN FLANZ APPEARS IN THE APPENDIX]

Mr. COFFMAN. Thank you, Ms. Flanz.

Mr. Milsten, yesterday the VA issued a new cost estimate to complete the new VA hospital in Aurora, Colorado now at $1.73 billion. As the Associate Executive Director of the Office of Construction and Facilities Management, please explain how VA went from a cost not too long ago, actually last year the estimate was $604 million and now we are at $1.73 billion. How did we get here?

Mr. MILSTEN. In my opinion, we got here by not getting those requirements right the first time that we started this project back in 2004 when noted the project that was a joint facility with the University of Colorado and DoD. As this project continued to grow through its processes, it did not have the benefit of a good, rigorous requirements development program and a good, rigorous program to control requirements growth as it went through the design process.

As we entered into the construction contract with the contractor, we established a ceiling and we rushed to get to a firm target price with the contractor as we saw the market in Denver continuing to escalate. The problem we had at that point was the design was not complete. The design continued to evolve and now we find ourselves at this crossroads.

Mr. COFFMAN. I think that probably an easier explanation would be pure incompetence, pure incompetence.

Mr. Milsten, what are the funding options VA is considering to finally complete the Aurora construction project for Colorado veterans?

Mr. MILSTEN. VA has considered many different funding options, including transfer authority, looking at where we can take it from other options within the department, and we are committed to working with Congress to find the funding available for this project.

Mr. COFFMAN. Mr. Milsten, when will VA hit the authorization cap on the project?

Mr. MILSTEN. We expect to hit the authorization cap of 880, which is ten percent above the 800, mid-May of 2015, this year.

Mr. COFFMAN. What is the updated completion date of the Aurora construction project now?

Mr. MILSTEN. In a meeting yesterday with both KT and the Corps there was a discussion about late summer of '17, if we can continue and get to a construction contract between the Corps of Engineers and KT this summer. So that would be about 24 to 30 months after that.

Mr. COFFMAN. Will VA seek funding again in fiscal year 2016?

Mr. MILSTEN. I know that the '16 President's budget has already appeared and the opportunity to amend that I am not prepared to talk about.

Mr. COFFMAN. Okay. After the gross mismanagement that occurred in Aurora, why shouldn't the Army Corps of Engineers or someone else build all major construction projects for VA? I mean, I think that the personnel involved in this project, you being one of them, simply in my view, let me use a Marine Corps phrase of couldn't lead starving troops to a chow hall. And there is no way

that the American taxpayers should have any confidence in you, the veterans of this country should have any confidence in you.

At this point in time, are you prepared to relinquish that authority or at least is VA taking a position that somebody else, the Army Corps of Engineers or some other qualified entity, ought to be taking over these major construction projects from the Department of Veterans Affairs?

Mr. MILSTEN. We are committed to looking at the opportunities that exist with using somebody like the Corps of Engineers as the construction agent. We have convened and asked the Corps to come in and study our processes, our procedures, to see what improvements can be made, and to offer an opinion on whether it is the appropriate process to go forward or look at other options. We as a department have not ruled out the possibility of turning construction management over to the Corps of Engineers, especially where it is appropriate, and we are doing that in the Denver project.

Mr. COFFMAN. Ranking Member Kuster.

Ms. KUSTER. Thank you, Mr. Chairman.

First let me say that I share across the aisle here the shock and on behalf of all of the veterans and all of the taxpayers outside of the great state of Colorado, not only is this a tragedy because of the request that you are coming forward to ask for a billion dollars and I join Dr. Roe in what that money could be used for. We like to say in the Granite State, we are frugal Yankees, we don't throw taxpayer money around. But what I am most concerned about is that these are facilities that can't be built elsewhere. There are lots and lots of veterans in need all across our country.

And so I want to get at a more basic question, which is whether or not the VA is up to the task or has the capacity to take on these modern-day facilities and whether we shouldn't revamp—because this is not the first example. I mean, this is, I have to say, the most shocking example, but I can remember in my first term these were the most troubling hearings we attended talking about facilities in other parts of the country. And I would like your comment, if you would, candidly, about whether it makes any sense at all for the VA to try to be building these facilities.

I can't imagine this kind of money in the private sector. I mean, Dr. Roe has more experience with hospitals, but I know what hospitals cost in New Hampshire, it is not a billion dollars and it is certainly not—you are going to get up to close to $2 billion here by the time you are done.

So I would welcome your comments on that.

Mr. MILSTEN. As I stated earlier, the department is committed to looking at whether it is appropriate for us to continue. That is why we have asked the Corps of Engineers to come in and conduct a study of our processes and procedures, and to come back and offer an opinion. And I know that the leadership of the department is committed too if it makes sense for the Corps of Engineers or some other federal agency to become our construction execution agent, we will be prepared to execute that.

Ms. KUSTER. Well, I guess my question goes beyond that, and maybe this is for another day and maybe meetings with Secretary McDonald. I am not talking about bringing the Army Corps in on

this project, I am talking about whether the VA should be in the business of building hospitals at all.

But let me ask a different question, because my time is limited. My question goes to, you used the term, transfer authority. Has there been any discussion at all with either the University of Colorado or the Department of Defense taking over the construction of this facility, owning this facility, you selling this facility?

I just feel like, with all due respect and it is not that people haven't tried, I just feel like people are out of their league here. Is there somebody else in Denver—and I am not as familiar with this situation obviously as my chair—has there been discussion about simply the VA not being the party that owns this facility?

Mr. MILSTEN. There have not currently been any discussions. There was discussions early on about a shared facility between DoD and the University of Colorado Hospital System, that was back in——

Ms. KUSTER. And is that no longer happening? That is no longer the——

Mr. MILSTEN. Back during that period, it was deemed that the voice from veterans that wanted veteran identity, because one of the things about our hospitals is that it is more than the treatment of our veterans, it is a place they go for their camaraderie. And the other issue was the issue of shared governance of a facility and that caused——

Ms. KUSTER. And I certainly do appreciate and I have heard from my own veterans in New Hampshire about veteran-centered care and all of that.

I guess I would just close by saying, on behalf of the taxpayer, I feel that we can do better by our veterans without building the Taj Mahal, and with all due respect to Aurora, Colorado.

So I yield back.

Mr. COFFMAN. Thank you, Ranking Member Kuster.

Mr. Lamborn of Colorado.

Mr. LAMBORN. Thank you, Mr. Chairman. And I will be very brief, because I am just still stunned by the news that this was going to cost so much over what the original cost was—not just the time delay, but the cost increase. So I will just say I back up my Chairman's position a hundred percent. I am still staggered and stunned by what is going on.

And there has to be accountability, we have to change the way things are done in the future. Somehow we have to find the money, who knows where, to finish a decent facility. Maybe not everything that was on the drawing board, but a decent facility so that veterans can start getting their care, without sacrificing the facilities around the country. You know, they have legitimate needs also and that money is going to hurt someone else's project. That is not good. We are just in an impossible situation here and it is extremely frustrating and angering.

Mr. Chairman, I yield back.

Mr. COFFMAN. Thank you.

Mr. Walz.

Mr. WALZ. Well, thank you, Mr. Chairman, and thank you all for being here.

Again, I am not going to pile on this, but I am going to express, I think you get it. Today as we sit here, tens of thousands of veterans are going to be treated with the highest quality professional care, get what this country promised them, what they have earned and deserve, and that is going to be distracted by what is absolutely indefensible.

And I am going to answer the question for them. The answer is no, you cannot do the construction. My concern—and I am not going to argue this point, I don't think we should be in a double-wide trailer and I do believe an atrium is a gathering space. And my question is, that could have been incorporated into the original design and pay for it what we pay for it. You don't need to overrun it to get the aesthetics, we have proved that time and time again.

And my concern now starts to be is because I understand this, construction of medical facilities is very specific and involves the involvement especially of the practitioners. So my question is, if these things are botched, what do the operating suites look like? When are we done? Are the walls too close? Does the gurney not come out? We have seen these things happen in some of our facilities.

And then I am back to this point—and I know this is all of you, you are getting the brunt of a lot of frustration that is coming on this, now we are caught in this conundrum much like IT. We have time and time and time again allocated money to IT that is absolutely necessary, absolutely critical and absolutely needs to be done. And when you come and testify and say there are gaps in our IT, I believe you. Our problem is this now, we are caught in a half-finished project that has us so frustrated and we are going to be asked to give more money. And I am in the same point as many of them, I have said this about IT, not one damn penny until you prove that you can use it wisely. And I am in that same boat with this and it is frustrating.

So if there is anything all of you can do to convey that. I know there is reasons, but there is no excuse for this. And at this point in time, I think what you are seeing on this is you are no longer going to get to decide whether you build hospitals or not, that is where this is headed. So what we need is your help in how do we transition this, how do we get the best practices, how do we move to make sure that happens?

I want to move to just one other subject before I go back. Mr. Miller's bill. I think all of us feel very strongly about the ability of employees to be able to speak freely, the ability to be able if there is a problem to come forward, and I think whistleblower protection is absolutely crucial. I am concerned and I ask your opinion on this. I know sometimes when you do this, though, is there a chance we are going in creating an atmosphere of fear, of mistrust amongst employees? Is the best laid plan and intentions actually going to have another chilling effect on how this happens?

Ms. Flanz, it is a somewhat subjective question, but if you could help me understand what it will do to the culture.

Ms. FLANZ. I would certainly like to try. Thank you.

The underlying purpose of all of the whistleblower protection laws and schemes is to encourage the candid disclosure of information. And there also over the years have needed to be added to that

a process for penalizing those who retaliate against individuals who do bring something forward. Our concern is about balancing the punitive measures in such a way that the entire structure doesn't actually act contrary to the underlying purpose.

And our concern with this particular bill is mostly about the relationship between the front-line staff and that first-level supervisor. That relationship is often carried out right in the middle of patient care, right in the middle of providing memorial services. It is where our veterans are, where our mission is carried out is right there.

Our concern is in creating a relationship through a process that may be necessary to ensure retaliation doesn't take place. We don't want to create a relationship where we are transferring the fear maybe from that front-line staffer to the first-level supervisor who may be so concerned about, oh, my goodness, I am now going to need to create this record to go back to this person who has made a disclosure, I have got a two-day window to do that, what if I don't do that right. What if later I am in the course of supervising this individual, I do something that causes the individual to believe he or she has been retaliated against. There becomes a different culture and relationship around that supervisor-subordinate exchange that may not actually be as supportive of the free flow of information as we would like to see those relationships be.

Mr. WALZ. Well, I think that is a valid point. I would be interested in seeing if there are some suggestions on this, because this is that touchy balance between due process and protecting that whistleblower's right, and I would say encouraging them to be able to come forward. And it is deep, it is cultural, it is about trust, and we want to make sure we get those pieces right.

Thank you, Chairman. I yield back.

Mr. COFFMAN. Thank you, Mr. Walz.

Dr. Phil Roe.

Dr. ROE. Thank you, Mr. Chairman.

Just to dovetail off what Mr. Walz was saying. In my office at home, we have a bulletin board full of requirements that we have to put up with. Wage and hour requirements, OSHA, on and on and on. And all of those federal regulations and rules, I can't get away with the excuse of, well, I have 30,000 people who are not as well paid and they are not all this or not all that, I have to comply. And I don't see why you can use that as an excuse when you expect the private sector to comply—not you, but we the government, we the Congress, expect the private sector to comply with these things.

So I don't think that is a valid reason. I understand it is hard, I do get that. As an employer for 30 years, I got that, but we have to do that. And we expect the VA to do the same thing that the private sector is doing.

Now, just a quick comment. The VA does a lot of things extremely well, there is no question about that. I got a letter from a lieutenant colonel yesterday who was very appreciative. He is a Korean War veteran and a Vietnam veteran, he said he survived both. He was actually thanking the VA and the government for his care. And I am writing him a letter back thanking him for his service. We should be thanking him, not the other way around. Building hospitals ain't one of them that they do well. And I said this

at a hearing not long ago, I don't think the VA ought to be allowed to build another hospital.

I look at $930 million, my Lord, I could build a palace in Tennessee for that, I could build two palaces for that, maybe three for that much money. And that would be to put places—we go out where we live to try to find places that save the government money. I have got a CBOC at home that pays $1 a year in rent, $1. We have hunted out trying to save that. And it is not just it is harming veterans in Colorado and veterans who may move to Colorado, it is harming veterans in Tennessee and Kansas and Indiana and all around—New Hampshire and around the country. So I think we have got to look at that.

I want to get to my bill just a little bit and, Dr. Icardi, if you would help me a little bit. Are there any issues with that bill that you can see from a VA standpoint that would be unreasonable to be able to take a piece of tissue that is implanted into a person, a patient, and then be able to follow that in case there is a recall, an infection with it?

And one of the reasons that we brought this up was that I saw what a poor job the VA did in notifying the veterans based on what happened with colonoscopies. And this was I guess five, four or five years ago. And other issues where notification didn't take place. If you don't have a tracking system, that veteran, that patient may never know and we may never be able to find them, that individual that got that specific piece of tissue.

So do you see any problem with this? Just implementing a tracking system so you can notify people, you get it from a certified tissue bank, any problems there?

Dr. ICARDI. Yes. First, Doctor, I want to thank you for bringing this up again, because this is an important issue and by bringing this bill up you have kept it in the limelight and I want to personally thank you for that.

One of the major issues that you have with tracking something is how do you identify it and, unfortunately, for tissue right now there is not a really uniform identifier that will follow the tissue from the donor to the final disposition. And there is a large number of steps that go through there. In the previous bill that we had, we were waiting to hear what the FDA was going to do with the UDI and now we have what the FDA wants to do with the UDI, and that doesn't quite allow us to do the level of tracking that we were looking for.

Dr. ROE. I guess is the problem, I mean, if you get my cornea or whatever it may be as I—and there probably is nothing on me worth using, but if there is they can use it and, if there is anything that is worth using, you are welcome to it. But when you transfer it, there is a way to do that and to transfer where that tissue came from, where it goes to and who it goes to. Isn't that available now?

Dr. ICARDI. There is, but what happens is the way it is identified can change on each leg of the journey. So what that means is, the way the UDI is set up, that is a number that gets used by the manufacturer. It may go to a distributor, that distributor may need to assign a different number to it. It could then go to a secondary distributor. It may then go out to a hospital, which then sends it out to a CBOC or that kind of thing. And the UDI is really specific for

one small leg, it is not specific for the entire process. So what can happen is—and a great example is what happened during the first Gulf War with blood, where the blood supply was mobilized, you had units come in from all over the country each with their own unique identifiers, but there was no commonality between them. And that actually leaves that sometimes you can actually have a number that is the same from one collection facility as with what is in another collection facility, so you can't really identify it by that. You are then going to have to do some sort of re-labeling or some sort of a reassignment of a number to track it through the system.

Dr. ROE. But for patient protection, isn't that important? I mean, I would think if I had an implant of some kind—well, actually I do have lens implants—that we should be able to—that is why I can see you, I had both lenses implanted—and I think if there were a recall on that, I would like to know what the problem is and my doctor or his clinic be able to identify that and to let me know. We should be able to do that for patients.

Dr. ICARDI. I agree 100 percent with that. We should be able to do that and we shouldn't have to go through a process where you have to trace things back link by link and take in some cases six months from when a problem is actually identified to track all those parts down by this system, which is inefficient.

Dr. ROE. I am going to yield, because I am over time. But the fact that it is hard doesn't mean we shouldn't do it.

Dr. ICARDI. And I agree as well. And that is why what we have been doing for the VA is looking at this, this is not just a VA problem, this is a national problem with the entire system. And for us to be able to fix it for the VA, we need to fix it for the nation. And so we have been working with Health and Human Services, FDA, DoD, and the other agencies, and there will be a conference on this in April that we will look to try and push this forward.

Dr. ROE. Okay.

Dr. ICARDI. But there is a solution.

Dr. ROE. I would like to continue our conversation. My time is expired.

Mr. COFFMAN. Thank you, Dr. Roe.

Ms. Rice, you are now recognized for five minutes.

Ms. RICE. Thank you, Mr. Chairman.

So, Ms. Flanz, I would just like to go back to the comments that some people were making about the whistleblowers. I mean, it is clear that the VA is not protecting whistleblowers to the extent that they need to at this point. And while I may agree that maybe a two-day investigative period, given the time constraint and the other responsibilities that that supervisor might have might be something that we need to tweak, I really hope that you would be willing to sign off on however we revamp this bill, because if you can't—I mean, clearly the VA has not been able to protect whistleblowers and you should want to be able to do that.

And I know that it is not just putting that responsibility on supervisors, it is an appropriate training program so that people understand exactly what the parameters are. So I hope that you would agree to be open to some changes that would require an in-

ternal system to ensure the protection of a whistleblower for a real problem that needs to be addressed.

Ms. FLANZ. I couldn't agree more. I know the secretary agrees as well. This is a matter of great interest, it is a top priority for the secretary and the deputy secretary. And we have been working in unprecedented collaboration with the Office of Special Counsel on a number of things.

Fundamentally, it is a leadership issue. Leadership must set the tone that disclosures need to be immediately addressed. Supervisors in a good, healthy work environment will welcome the information, because that is what leads to process improvement. That is how we ensure that veterans are treated safely, that our processes are efficient and are compliant with the law. Only good things flow from that exchange of information. When we get into trouble is when supervisors either don't know the rules or react inappropriately, because they haven't seen appropriately modeled to them the right behavior.

So we absolutely are open. We have been working very closely with members of this committee and staff on issues with respect to individual whistleblowers and to the process we are using across the board to make the changes that really are critical. So absolutely, we are open to and need your help.

Ms. RICE. Well, I agree that the best chance that we have is with Secretary McDonald, who has shown an interest in ensuring the protection of whistleblowers. And coming from someone who has run a DA's office, you are right, the tone is set from the top. And if people feel that by complaining they are going to be penalized, no one is going to complain. And that is where the neglect or the abuses become more insidious.

So I just—and this might be a repetitive question, maybe I didn't understand, I just want to go back to Mr. Milsten. So you are coming and asking for a lot more money. My question is really, I think it is simple. Maybe it was asked before and I wasn't here, I don't know, or I didn't hear it in your explanation before. I would like specifics as to why $800 million, the initial estimate, was not enough to finish this project—or 600—is that what it was, 600? Sorry. I gave you a $200 million cushion there I didn't mean to give. What happened that made this project incapable of being completed?

So I want specifics about people, about who didn't do what they were supposed to do, about inaccurate estimates, specifics that we know going forward how is this not going to happen again with the other billion dollars that you are asking for. Because there is no way this government, at least I am not in the business of throwing good money after bad and it seems like that initial $600 million, as well intentioned as it may have been, is falling under that category.

So please make the case. And I have to say that I also don't think that the VA should be in the business of building hospitals, but that is really an issue that we as a committee will have to discuss. If you can just lay out with real specificity what happened and how it is not going to happen again.

Mr. MILSTEN. Okay. I will be happy to attempt that.

First of all, the VA owns this, we own this fiasco that we created. It is nobody else's fault, but I am going to tell you that there are some other people that played a part in it. And I can tell you that we are looking at our role of oversight of those processes to figure out how and why they broke down.

Number one, we hire a designer who is responsible for designing a facility to meet the requirements that we set forth. Early on, we develop some programmatic estimates in-house, and then we rely on the designer to design the project to the budget that we have told him that we have. So in this case we had a designer we charged with delivering a design that could be built for just under $600 million. That designer provided us with estimates of how that could happen. And I can tell you that our breakdown was that we did not do the proper amount of due diligence on that estimate, we did not dig in far enough detail to actually go in and figure out that it could or couldn't be done. We relied on that and we moved forward. When we got advice from our construction contractor that the budget may not be billable, we chose unfortunately to listen to the designer.

And these are changes that we are making in our process now. We are bringing in independent construction management firms to help us review estimates, to review schedules. Not just relying on the word of one firm representing what the requirements will cost, but relying on multiple firms to make sure that we get the best and correct answer.

And we are also looking at how we change our culture to say that construction contractors are not always the enemy, if you will. Too often we engage in siding, if you will, with the designer and not listening to our sound advice from the actual builders of the facility.

Ms. RICE. So if I can just say, that is exactly why the VA should understand their strengths and their weaknesses. And because you shouldn't be in the business of building hospitals, that should be left to an expert. That may be why that oversight was not as robust as it should have been. No offense to you.

But if I could just ask you, because what I think that we need is a very detailed report of exactly what went wrong, when it went wrong, and who you hold responsible for those mishaps and miscalculations and all of those kind of things. I mean, you are coming and asking for money and that I think has to be laid out, not so much in this forum, because we have limited time, but if you could by next week prepare a document that details exactly what the shortcomings were, so that we can understand what happened, that would be——

Mr. MILSTEN. The department has seated an administrative investigation board, that is their sole responsibility to go through these details and find the accountability. It looks at the mismanagement potentials and misbehavior potentials for people involved in the project. And I will turn it back over to——

Ms. RICE. So there is a report that exists?

Mr. MILSTEN. No, ma'am. A panel has been set. I am going to turn it over to Meghan to talk about the outcome, the expected outcome and time frame for that.

Ms. FLANZ. Very quickly. There are two ongoing processes and I will do my best to outline both very quickly. I know that the deputy secretary had phone calls with a number of members of this committee within the last couple of days, so I apologize if I am covering for you ground that has already been covered.

But we have an administrative board of investigation, which that is an activity that my office owns. That group looks at individual accountability, who did what or failed to do what that needed to happen. At the leadership level, who knew and acquiesced in either actions or omissions by people below them. So that board looks at who is responsible for what error or omission that may have led us here.

The second and equally important piece of VA's process of understanding what happened is the study that the Army Corps of Engineers is leading for us that is bigger than Denver, that is, really gets I think at some of the fundamental issues. Does VA have the expertise and the capability to continue to build hospitals? What are some of the systemic issues that have led to cost overruns or delays in projects, to include Denver, but not exclusive to Denver. Those two processes are ongoing. We absolutely share the frustration and the sense of urgency that I hear in the members today. We need these answers now, we needed them before the project went the way that it did.

Having said that, the process of collecting evidence about decisions made over the course of a many-year program takes time. So I hear the request for a written report next week. The process that my team is working on will take more like a month than a week, but we are working to get those answers just as soon as we can pull the evidence together.

Ms. RICE. The problem is if the money runs out in May of 2015.

Thank you, Mr. Chairman.

Mr. COFFMAN. Thank you, Ms. Rice. Dr. Huelskamp, you are now recognized for five minutes.

Dr. HUELSKAMP. Thank you, Mr. Chairman. I guess you used up my five minutes. I guess I am done, so I—just kidding. Thank you, Mr. Chairman, and I will note I appreciate the questions on Aurora and that situation. Actually, it might not seem pertinent to Kansans, but that would be the closest VA facility for a large share of the northwestern corner of my district. It is only 188 miles from Kansas. Do not forget it is 200, 300, or 400 miles the other way for some of mine, so I watch this very closely, because I will have Kansans traveling, hopefully one day, to this facility.

I have a couple questions. First, Ms. Flanz, on my bill, I understand that you support the concept, but are you willing to work with my staff, Subcommittee staff, to fix a few of the technical issues that you have expressed?

Ms. FLANZ. Absolutely, it is my understanding that our folks have already reached out to your staffers to set up a conversation to do exactly that.

Dr. HUELSKAMP. Absolutely. You want to make certain that these set-asides obviously go to those veterans that should be qualifying for these particular contracts. So thank you for that commitment. We will continue to move forward and hopefully we will fix a few of those technical issues.

I do have a few other questions on the other bills or some of the statements here. First, for Mr. Lowe, in reference to the IT—and I appreciate my colleague from Indiana and her work on this, and I was in some of these hearings—do you believe that the IT system at the VA is secure today?

Mr. LOWE. Congressman, it is as secure as we can possibly make it. There is nobody in any position that—or anybody that sits in my position that can definitively state that their system is completely secure, because there are just too many unknowns. But based upon the information that I have today, I have to say that we are as secure as we can be.

Dr. HUELSKAMP. Is there any independent assessment outside the VA that can——

Mr. LOWE. Well, you know, the IG conducted an independent assessment. GAO conducts an independent assessment. You remember hearing in——

Dr. HUELSKAMP. Yeah, and their assessment was not very good the last I saw. My question is, outside of the VA, outside of the government, have you brought in any independent——

Mr. LOWE. Oh, yes, we——

Dr. HUELSKAMP [continuing]. Contractors saying, "Yes, this system is secure at a standard for the industry that we believe is"——

Mr. LOWE. We had an independent assessment come in and take a look at the domain controllers, which we briefed the staff on, and it was specific to the domain controllers. And they did not—and that was specific to the instance that the Committee was concerned about that happened in 2010, and they found that, you know, the remediation activities that took place in 2010 were effective.

Dr. HUELSKAMP. All right. Well, I appreciate that and look forward to that information as we move forward ahead.

And one other question on the issue of whistleblowers, and I know I speak for all the committee members that we have been stunned and shocked, particularly by the response from the Department at differing levels. We have had a series of secretaries that have promised to make certain whistleblowers were never retaliated against, and somehow that did not get down to other 320,000 folks working in the Department. How many outstanding cases of alleged whistleblower retaliation are still ongoing?

Ms. FLANZ. I do not have a number at hand. The Office of Special Counsel sends those cases to us in kind of two different batches, two levels of priority. We did work out with them last summer an agreement that if they prioritize a particular case because an individual employee who claims to be subject to whistleblower retaliation has a pending personnel action, something adverse is happening, those come over on an expedited basis. Our attorneys work with the supervisors and managers of those people to ensure that those—whatever adverse action is going on is stayed.

Then there is another larger group of cases where the Office of Special Counsel hears from an individual who believes that he or she is the subject of retaliation, but there is either nothing immediate pending or the Office of Special Counsel is not as convinced based on the evidentiary record that they have that retaliation has, in fact, taken place. So those take a little bit longer.

Dr. HUELSKAMP. So in order, though—I just have a few seconds left—in order to determine whether we have made progress or not—whether you have made progress or not—do you have any comparison baseline of what it was, maybe before you came on board, where it was three years ago? Can you provide those numbers to the Committee, so we can get a sense are we making progress?

Ms. FLANZ. Certainly. I will be happy to provide specific numbers, and I can tell you that we had an expectation when we entered into that agreement for this expedited process that the number of complaints that would be sent through that process would be quite high. It has actually been lower than I think either the Office of Special Counsel or our staff——

Dr. HUELSKAMP. It is low, but you do not know what the number is today?

Ms. FLANZ. It is——

Dr. HUELSKAMP. It is my understanding it is over 100 outstanding cases of alleged retaliation. Is that in the ballpark?

Ms. FLANZ. That was the number that we were given at the time we entered into the agreement last summer. I think it is a much smaller number, more on the order of closer to ten that has come through the expedited process. But I would—I will be happy to get you precise numbers, so we can begin to have that kind of trend analysis.

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

Mr. COFFMAN. Thank you, Dr. Huelskamp. Ms. Walorski.

Ms. WALORSKI. Thank you, Mr. Chairman. Mr. Lowe, in your written statement you quote the following from the GAO that you were just speaking about, "In a dynamic environment, where innovations and technology and business practices supplant the status quo, control activities that may work today may not work in the future." Are you aware the GAO actually supports this bill, and they actually worked with us in adding Section 10 to the bill on flexibility?

Mr. LOWE. No, ma'am, I am not.

Ms. WALORSKI. And in another statement you talk about—you point out that, "A review must be performed on any patches to ensure the operability of the particular application or system to ensure the patch does not have a harmful impact to services that VA provides. My legislation instructs VA to perform the risk assessments and to also test patches within two days of availability." How long of an evaluation period would you need?

Mr. LOWE. That is a technical question. I will have to ask the operational guys. I would be happy to get back to you on that.

Ms. WALORSKI. Okay.

Mr. LOWE. And, you know, we really—we have a unique opportunity now to actually drive what the nation is doing. I mean, legislating operations is problematic, because it does take away some of the flexibility. But I think we have all got the right idea, and we have got—we are all after the same endpoint, but there are a number of bills going through Congress right now that I think that we could probably squeeze all this together and come up with one legislation, so we are not having to deal with 20 or, you know, so different pieces of legislation that are coming out, not just specific to

the VA, but specific to the government-wide. And I think that we have a really unique opportunity in time right now to be able to affect what the rest of the government does and what the rest of the nation does.

And I would be happy to work with your folks to be able to come up with an awesome bill that not only this Committee could support, but the entire Congress and the Senate and the rest of the federal government can support.

Ms. WALORSKI. And I appreciate that, and I would hope so as well. I just—if you are going to get back to me on the evaluation period of the assessments on the patches, could you also add to that? You talked about VA cannot phase out outdated or unsupported systems, because they would impact physicians at the point of care. My bill provides VA 90 days to come up with a migration transition plan to move to secure operating systems. If you could just add to the list how much more time would the VA need.

Mr. LOWE. Sure. A lot of those operating systems are attached to medical devices, so we would actually have to, you know, a large number of the medical devices that are currently produced by manufacturers. And I think Dr. Roe probably knows a little bit more about this than I do, is the, you know, most of the medical devices that are in use, and most facilities today are running off of Windows XP. And so they had that FDA certification around that particular image.

So I, you know, working with medical device manufacturers and replacing all that and upgrading those, whether or not the systems, actually themselves, that the operating can run it, that will be a long—I will—we will actually have to have a long conversation about how we do that, because we are going to have to work with not only the FDA, but the medical device equipment manufacturers.

Ms. WALORSKI. That is fine. And if you could just add that to the list of—just sending it back at some point.

Mr. LOWE. Absolutely.

Ms. WALORSKI. And then I just want to, in response to your suggestion, I can tell you, I would hope so, that we can find a way to move this bill and to move actual verifiable accountability into the issue of the IT with the VA.

And, you know, I am only starting my third year here, and from day one when I got here and we started talking about IT, and it all started back in the day when we talked about why cannot we get a electronic medical record and connect the DoD to the VA, and I sat in a subcommittee hearing even then with these same issues of domain controllers, of outside entities on domain controllers. And, you know, my concern was the breaches that have taken place with our veterans nationwide. And, you know, money has never been an issue. And when we talked about issues before with some of the—I do not know if they work for you, around you, I do not know how your whole group flows, the folks who have been in here testifying on it—but the reason I am pursuing it is because veterans' information is so critical, and the bad actors that have been embedded and have been impacted inside of this domain controller—and we might have to just agree to disagree—but not only are they—not only is just their personal information available, but

when these bad actors get in and disallow us from connecting to the DoD because of VA not having a secure website, you know, what happens if a bad actor gets in there and scrambles medical records?

What happens if, you know, they just decide to go in and look at 30 million veterans and say, "How can we completely mess up this system?" And I think every veteran that served not only deserves the best of everything they were promised, but when they come back from fighting and they come back into our country, especially in my state, in the State of Indiana where we are over the top patriotic and we are over the top in sending folks to fight, they—I just am fighting for them to say at some point, "Let's get beyond this."

And so I just wanted to make sure that we have some kind of level of understanding of House bill—of our bill 1017. I appreciate your comments in writing in the coming days. Thank you. I yield back my time.

Mr. COFFMAN. Thank you. Mr. O'Rourke, you are recognized for five minutes.

(No response.)

Mr. COFFMAN. Mr. O'Rourke passes. I would like to thank the panel for your testimony. You are now dismissed. I now welcome our second and final panel to the witness table. On this panel, we will hear from Ms. Diane Zumatto, National Legislative Director of AMVETS; Mr. Frank Wilton, Chief Executive Officer of the American Association of Tissue Banks; Mr. Daimon E. Geopfert, National Leader, Security and Privacy Consulting for McGladrey, LLP. All of your complete written statements will be made a part of the hearing record. Ms. Zumatto, you are now recognized for five minutes.

STATEMENT OF DIANE ZUMATTO

Ms. ZUMATTO. Thank you, Mr. Chairman and distinguished Committee Members. I am pleased to have this opportunity to sit before you today to share our comments on pending veteran legislation. Before I get into our specific positions on these bills being considered, I would like to share a few general introductory remarks.

AMVETS is, in general, a fiscally conservative organization which supports the interests of our veterans and military men and women. Our members want to see a balanced federal budget, and I have major concerns surrounding the ever-increasing federal deficit. Additionally, our membership would like to see an increase in federal accountability, especially within the Department of Veterans Affairs, as well as a decrease in government bureaucracy.

AMVETS does not support the concept of indiscriminately throwing money at problems. While some of our colleagues are shocked by this notion, AMVETS acknowledges that there are certainly programs that would benefit from increased funding. However, we believe that before those increases are made, they should first be fully justified and only come after a thorough review of the organizational structure of each program or agency with an eye to identifying system efficiencies, maximizing all current resources, both human and financial, minimizing waste, and eliminating redundancies.

And as far as legislation today, AMVETS supports H.R. 571, which would provide whistleblower protection for folks within the VA. If we expect employees to be willing to take actions to prevent fraud, illegal acts, et cetera, then those employees are going to have to feel confident that if they do step forward, they will be safe from any form of retaliation, either personal or professional, that the information they provide will be acted on in a confidential and appropriate manner, that the information will also be handled in a timely manner.

AMVETS applauds Chairman Miller's continued efforts to ensure that VA employees, many of whom are veterans, have an equitable and safe environment within which to better serve all American veterans.

AMVETS supports H.R. 593. There has been a lot of discussion about that this morning, and there is really not much more I think that needs to be added. Something needs to be done. It is obvious that the status quo is not adequate. So we do support H.R. 593.

We also support H.R. 1015. It is a pretty simple and straightforward solution. And there, you know again, I do not really have too much to say to this. I do realize that there is some monitoring that is going on. And I am aware also that the IG, you know, finds cases of abuse almost daily, so we know that there is a problem. And I think this is a pretty simple way to rein that in.

We support 1016, which, you know, would require the VA to adopt and implement a standard identification protocol. And I have listened to the testimony all morning, and I understand that there are a lot of difficulties, but this does not seem like an insurmountable problem. It is a matter of logistics, and I would really encourage the VA to—if every provision in this bill does not work for whatever reason, I would hope that they would be willing to work towards a solution.

We also are supportive of H.R. 1017 and 1128, both of which are related to information security. As a veteran, I shudder to think about the vulnerability of the VA system. I know they are aware of the problem, and I think there has been plenty of beating up on the VA lately. I just would really stress that this is critically important to AMVETS that this problem be taken care of. I would also like to applaud Representatives Walorski and Kirkpatrick for their efforts in this area.

AMVETS also—I hesitate on 1129, even though it is also a whistleblower bill. And we hesitate only because of my introductory remarks. We hesitate to condone an increase in bureaucracy. My read of this is that there is going to be the creation of a new agency that would handle this problem, and we think that there is already probably enough between the IG and the Office of Special Counsel that there is probably no need to create another agency.

That concludes my testimony at this time, and I yield back.

[THE PREPARED STATEMENT OF DIANE ZUMATTO APPEARS IN THE APPENDIX]

Mr. COFFMAN. Thank you, Ms. Zumatto. Mr. Wilton, you are now recognized for five minutes.

STATEMENT OF FRANK WILTON

Mr. WILTON. Thank you, Subcommittee Chairman Coffman, Mr. O'Rourke, distinguished Members. Thank you for the opportunity to come before you today in support of H.R. 1016, the Biological Implant Tracking and Veterans Safety Act of 2015.

For those who are unfamiliar with my organization, the American Association of Tissue Banks is a professional, not-for-profit scientific and educational organization. It is the only national tissue banking organization in the United States, and its membership totals more than 125 accredited tissue banks and approximately 850 individual members. These banks recover tissue from more than 30,000 donors annually and distribute in excess of two and a half million allografts for more than one million tissue transplants performed in this country annually. The association was founded in 1976 by a group of doctors and scientists, who had started in 1949 our nation's first tissue bank, the United States Navy Tissue Bank.

H.R. 1016 directs the Secretary of Veterans Affairs to adopt a standard identification system for use in the procurement of biological implants by the Department of Veterans Affairs. By building upon the success of the implementation of the unique device identifier, or UDI, this legislation will ensure that biological implants used within the Department can be appropriately tracked from human tissue donor all the way to recipient. This critical capability for track-and-trace efforts will enhance patient safety, expedite product recalls when necessary, assist with inventory management, and improve overall efficiencies.

This legislation takes a bold step to expand the UDI to all tissue products. In addition to human tissue devices which are already covered by the UDI, the legislation adds another product category—certain biological implants, or as termed by the Food and Drug Administration, 361 human cells, tissues, and cellular and tissue-based products, or HCTIPs. While many of the biological implants do have company-specific barcoding information by requiring a standardized format for those barcodes as outlined in this legislation, it will be easier for the Department of Veterans Affairs' medical facilities to utilize the universal barcoding conventions and to realize the full benefit of the unique identification system.

Finally, by applying a system that has been developed for devices to biological implants, such a solution would also be applicable to other healthcare settings and other healthcare systems such as the Department of Defense healthcare system or the private sector.

While I understand your skepticism in requesting the VHA attempt a VITAS-like enterprise in this legislation after failing to do so before, I would note that a lot has changed since 2008 when the VHA first envisioned VITAS. First, there is now a UDI benchmark, which allows those developing the necessary software for data capture to move from a design incorporating dozens of different barcoding technologies to only three different ones.

In addition, the VHA is not alone in trying to develop a system for integrating the UDI-like information directly into the medical record. For instance, the Office of the National Coordinator for Health Information Technology is currently focused on ways in which UDI can be better operationalized to ensure its adoption into key standards. As part of those efforts, ONC is initially focused on

implantables, the very focus of the legislation that we are discussing today. Therefore, the VHA will not be attempting to establish the system alone, but can partner with other governmental entities to ensure its success.

In addition, AATB is pleased that the language, as introduced, ensures that our veterans receive the high quality implants by requiring that biological implants only be sourced from tissue processors accredited by the AATB or similar national accreditation organizations. With this change, the VHA will be joining the ranks of leading medical centers of excellence which currently require all tissue to be sourced from AATB-accredited banks.

AATB is also pleased that the introduced language clarifies that human tissue procured by the VHA can be labeled with any of the three systems already identified by the Food and Drug Administration to be appropriate for biological implants. Under the UDI final rule, FDA has done just that by providing for multiple entities called issuing agencies.

At this time, FDA has provided for three different issuing agencies, GS1, the Health Industry Business Communications Counsel, or HIBCC, and ICCBBA. By maintaining this appropriate flexibility, the VHA will ensure a more competitive marketplace. AATB strongly supports this legislation and urges you to favorably report it out of the Subcommittee. I welcome your questions and yield back the remainder of my time.

[THE PREPARED STATEMENT OF FRANK WILTON APPEARS IN THE APPENDIX]

Mr. COFFMAN. Thank you, Mr. Wilton. Mr. Geopfert, you are now recognized for five minutes.

STATEMENT OF DAIMON E. GEOPFERT

Mr. GEOPFERT. Thank you. First, Chairman and Members of the Committee, thank you for the opportunity to discuss the Department of Veterans Affairs Information Security Programs.

My name is Daimon Geopfert, and I was asked to speak today as a veteran and as a security expert with experience in both the government and corporate worlds. I served the United States Air Force Office of Special Investigations as a computer crimes investigator, the Air Intelligence Agency, three years as a DoD contractor, and now eight years as a security consultant within the corporate world.

Also, like many of my peers, I have also received a letter from the VA stating that they failed to protect my personal information. I am here today quite simply for a call to accountability. Men and women in the armed services are held to account for every action they perform or fail to perform. And they expect that same mentality to be applied to the entities that control their sensitive personal and medical data. However, all indications are that the VA has failed in this duty.

What is most frustrating to the veterans is this is not a singular failure but rather a long-running, repeated systemic series of failures. Passing legislation such as H.R. 1017 would provide a detailed roadmap for the VA to follow in addressing these issues. The VA has a widely reported history of non-compliance with a variety

of regulations. We recently learned that for the 16th year in a row, they failed a major security audit.

The VA's own internal risk assessments, using their exact terms, state that a data breach of its primary VISTA system is practically unavoidable. It would result in a exposure of financial, medical, and personal data with no way of tracking the source of the breach. The VA has stated that physical loss of data and user error is their primary risk and accounts for 98 percent of the known incidents.

However, extensive reporting and the consistent theme of the audits indicates that the VA mostly likely does not have the capability to know, or prove, that data was not taken by hackers.

A specific example involved foreign infiltrators known to have extracted materials out of the VA environment, but because of the lack of logging and monitoring by the VA and use of encryption by the foreign party, it will never be known what the contents of that data were. Scenarios such as this allow the VA to continue to state that the organization is unaware of any major data loss as a result of hackers. But this is likely a factor of the failure and lack of capabilities of their monitoring, rather than success of any preventative controls.

These widely known and extensively reported issues simply would not be tolerated in the corporate world, largely because of the existence and enforcement of explicit legislation and industry standards. If examinations of a private sector organization produced similar results as those identified within the VA, that entity would face substantial fines and penalties. There is little doubt that the officers and directors of such an organization would face serious personal consequences. The VA, for all practical purposes, is exempt from any of the legal penalties that force its corporate peers into compliance, and the results of that situation is self-evident.

H.R. 1017 provides the VA with clear detailed technical requirements and governs mechanisms to address this issue. The FFIEC would not tolerate this of a bank. The SEC would not tolerate this of a broker/dealer. State attorneys general would not tolerate this under anybody within their purview without very harsh criminal and civil repercussions. The veteran community is reasonably curious why the VA is held to such a drastically different standard.

It cannot be forgotten that the true risk in this scenario is the health and well being of the generations of veterans the VA serves. The most obvious risk is identity theft, which results in additional stress within a population already dealing with a variety of significant physical, emotional, and financial pressures. While this is the most obvious risk, it is not the exclusive one.

What if beyond identity theft, some actor managed to perform a mass alteration or destruction of medical records out of sheer malice? Do you think this would beyond the pale for a variety of hacking groups, or hacktivists, that align themselves with rogue nations or terrorist groups? It could conceivably disable the entire VA infrastructure, interrupting services to millions of veterans. It would be a direct, highly visible strike against the veterans that fought them. The men and women who have served our country, as well as their dependents, deserve and expect to have their welfare pro-

tected by organizations like the VA that play such a vital role in their lives.

This legislation is sorely needed and would be one of the first of its kind to provide such detailed prescriptive guidance. The protection of the personal information of veterans should be a bipartisan issue. So our community hopes that this will be quickly passed and enforced. Targeted appropriate legislation is needed to force compliance and provide veterans and their families with the security they deserve.

This legislation should explicitly require proper preventative, detective, and corrective controls along with required oversight and reporting. The VA, and the bodies that oversee it, have an obligation to Veterans to finally take decisive actions demonstrating the resolve to do the right thing. And, Mr. Chairman, that concludes my statements.

[THE PREPARED STATEMENT OF DAIMON GEOPFERT APPEARS IN THE APPENDIX]

Mr. COFFMAN. Thank you, Mr. Geopfert. Let me do a question for you. There has been concern that the IT security directive is too detailed. It might not be applicable in the coming years due to the inherent changing nature of technology. What is your view regarding this potential issue?

Mr. GEOPFERT. I think it is a very limited view. The drift in the corporate world has been from generalist regulation and oversight to very prescriptive, simply because the generalist style of guidance has proven to be very ineffective. The other style, the competing bill that is very generalist in nature, essentially puts another wrap around a lot of items that the VA is already supposed to be doing but has failed to do. What is viewed as prescriptive in this bill is interesting, because most of this is what they are required to be doing already. It is just basically done in a more regimented manner. This is already an existing legislation in the corporate world. So the idea that it is too prescriptive to be effective is a bit misleading. Obviously, there can be tweaks made if there are specific points.

Mr. COFFMAN. Okay. Mr. Wilton, VA has indicated that it wants to limit the issuing agencies solely to ISBT 128. Is that a good idea?

Mr. WILTON. We do not think it is, Mr. Chairman, for a couple of simple reasons. First and foremost, the FDA has looked at this fairly closely and recommended that all three systems be used.

Secondarily, we would be concerned if the VA limited it to one system. There may well be tissue banks who decide to align themself with another system, and therefore would not be in a position to bid on business with the VA, which we think could limit the ability for the VA to source the best tissue for our veterans.

So the FDA has ruled on this and, you know, in talking with our accredited banks, there does not seem to be a unanimity in terms of which system they are going to go with, so we do not think it is a good idea for the VA to limit that.

Mr. COFFMAN. Ms. Zumatto, can you give us an example of something that could be a reform that could be done to the Veterans Administration to make it more efficient with respect to both the taxpayers and veterans?

Ms. ZUMATTO. Wow.

Mr. COFFMAN. What would be your top concern?

Ms. ZUMATTO. Honestly, from both being a person who is an advocate for veterans' issues and being in the VA system, I think the biggest problem is that veterans actually do not come first in the system. It does not feel that way when I am at the VA Medical Center.

And if there was a way—and I understand the new Secretary says, you know, "Veterans first." And that's the motto essentially, "We care for veterans." But it does not actually feel that way to me personally. So if there was a way to change that so that it really is about veterans first, and about VA and VA employees and contractors and everybody else secondarily, I think that would go a long way to making some positive changes. And I do not think that—if those changes—they have to be modeled at the top. But if it does not drift down to every single layer, and there are many layers, then nothing is really going to change, unfortunately.

Mr. COFFMAN. Thank you for your answer. Mr. O'Rourke, five minutes.

Mr. O'ROURKE. Thank you, Mr. Chairman. I want to thank the witnesses for their testimony today. To have the perspective of a veteran service organization and then the subject matter experts on two issues that I do not have a lot grounding in, I think is very helpful, and I think helpful for the committee, as well.

And I think you have also touched on what I think is the core issue that we need to resolve within the VA, which is accountability. And I think each of these pieces of legislation, to some degree, tries to correct that, and I want to thank the committee members and the staff who have worked on these bills and you all for your feedback on these.

You know, Ms. Zumatto, when we talk about throwing money at problems, which, you know, we couldn't agree more with you that, that is not the solution. We are glad that, that is your position and that of your organization.

You have to conclude that if Aurora were to have taken place within a private hospital corporation like HCA or Tenet, that there would be consequences, or that that would not even happen in the first place, because at some point, that would have been caught and fixed. And to go from 600 million to 800 or 900 to 1.1 to maybe 1.7, to me is just unconscionable and completely out of line with what we would expect to see in the private sector.

And Mr. Geopfert, you mentioned that the IT protocols and the data and information security that we have within the VA today, at least by your description, does not track with what we would expect from the private sector. And you mentioned that there is legislation and industry standards that, you know, most corporations hue to, to ensure that they protect the data of their customers and clients. It is not always completely successful, but you are making a case for a higher standard that the VA does not adhere to.

Mr. Wilton, from your testimony, it was not completely clear to me whether or not the VA in tracking biological implants and this issue of—the other issues that you raised—is so far out of track from what the national standard is, but it may be that I don't completely understand the issue, so I just want to give you a minute

or two to elaborate on that and talk about the difference between the VA standard and the national standard.

Mr. WILTON. Yes. So this is an evolving issue, Congressman. But it is one that we see the VA actually taking a leadership role on. One of the very important things about all tissue is it is recovered and tracked from the donor through the distribution. Once it gets to the final location, the hospital, the doctor, then sometimes that chain is broken, and we want to work with the VA so that they can maybe take a leadership role in this and then, as I mentioned, we can take it out to the Department of Defense, to the private sector.

We think this is something that can be done. We look forward to working with the VA on any challenges they might have. But we think this is just, quite frankly, the best way to do it, and I think our veterans deserve the best. And, you know, God forbid there is an incident of a recall or something like that, we should be able to get back to them in a timely fashion, and we think that this type of system will do that.

Mr. O'ROURKE. So this is potentially a positive point coming out of today's testimony and the issues that are here in terms of an opportunity for the VA not just to catch up to the rest of the country and other sectors, but actually potentially to lead, innovate, and set the standard for others?

Mr. WILTON. Absolutely. And we commend Dr. Roe for introducing the legislation. We look forward to working with all the parties to make this happen.

Mr. O'ROURKE. Yeah. For Mr. Geopfert, I want to make sure I understand that legislation that the private sector must adhere to and those industry standards—and I realize we cannot get into detail—but is it simply a matter of the VA matching those? Or are there some intrinsic differences in our systems, in our customers and clients, that should allow for some difference or distinction between the two systems? Or is it simply a matter of the VA just admitting that it needs to catch up to the rest of the country and follow that law?

Mr. GEOPFERT. It does not repeat, but it rhymes. A lot of the industry standards are going to have their own names, and norms and references to how they do security, but they are very, very similar. You are probably 80 to 90 percent similar across all industries. And what is in the bill essentially captures that. Again, a lot of this, while they viewed it as prescriptive, is considered best practice and normal network hygiene in many other industries.

There is going to be tweaks simply based on the size, composition, legacy systems, how they interact with others. There needs to be some give and take in there around risk and how they do specific things, but the vast majority of what is going on in private industry would directly translate to what they are doing. And they simply are just not being held to account to that right now.

Mr. O'ROURKE. Thank you. Thank you each. I will yield back.

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

Ms. WALORSKI. Thank you, Mr. Chairman, and thank you to all of you for being here today. We appreciate it. Mr. Geopfert, do you believe this bill allows for flexibility and that Section 10 does allow a risk-based approach?

Mr. GEOPFERT. I believe there can be some clarification in the language. Based on their earlier testimony, they were specifically calling out two points——

Ms. WALORSKI. Yes.

Mr. GEOPFERT [continuing]. Around patching and legacy systems. In the bill as it is right now, there is a caveat around doing risk assessments. I think their comment that they might take some additional time—your point that is in there now is two days—48 hours is a very common norm for critical, high-risk patches.

Ms. WALORSKI. Okay.

Mr. GEOPFERT. Stuff that is rated lower might be 15, 30, 90 days, depending on what it is. Legacy systems, they have a valid point. We work in a variety of industries where it is the norm to have legacy unsupported systems that they have to maintain for some reason, similar to the VA. But they have to document why they are still on the network. They have to put in compensating controls to limit the risk. They have to isolate the system, and they have to begin planning on when and, if possible, they are going to remove them out of the environment. They do not just say we have to deal with them, so they are there.

Ms. WALORSKI. Sure. Do you think it is safe for VA to be running on all these outdated operating systems? And then secondarily, how big of a risk would it be to have isolated computers on the network running on unsupported and outdated operating systems?

Mr. GEOPFERT. The safest, obviously, would to get rid of it, but it might not be feasible. Their comment is very common in the industry around a lot of the legacy systems are medical devices. They have no direct control over those. Those come from vendors.

But the point still states, if it is a legacy system, meaning it is not maintainable anymore, any exploit that comes out from here going forward, that system will be vulnerable to—you are basically embedding a permanent vulnerability on the environment. If it needs to be there, it needs to be isolated. It is going to be a minor risk. But you are treating it essentially as infected, a radioactive. You are isolating it as far as it can be, and still be operational. There are ways to go about it. I guess I will put it that way.

Ms. WALORSKI. Okay. And then given the current information security requirements already in place, would you say that the directive duplicates existing federal guidance?

Mr. GEOPFERT. I do not. A lot of the federal guidance out there is laid out as almost a recommendation style.

Ms. WALORSKI. Okay.

Mr. GEOPFERT. And it is very high level. And as noted earlier, in the private sector there is a very heavy trend towards much more prescriptive guidance, because they have years of incidents demonstrating that the statements generally go be secure, and here is some recommendation. It just does not work.

And so while the VA is going to say is that is onerous for them, all the other industries are saying the same thing. It does not matter. They are being held to account. And it is a little bit of an oddity that the private sector is expected to comply with no question whatsoever, and no excuses. And for someone in a government entity to say it is onerous, so therefore I don't want to do it.

Ms. WALORSKI. Okay. I appreciate it. And thanks. And I am just thankful for your support and, ma'am, for yours, as well. I yield back my time, Mr. Chairman. Thank you.

Mr. COFFMAN. Thank you, Ms. Walorski. I would like to thank the panel for your testimony. You are now excused. And I did want to thank everyone for their participation today. The input and feedback provided today is an important contribution as the subcommittee crafts legislation to improve the quality of service VA provides to our nation's veterans. With that, I ask unanimous consent that all members have five legislative days to revise and extend their remarks and include extraneous materials. Without objection, so ordered. This hearing is now adjourned. Thank you.

[Whereupon, at 9:51 a.m., the subcommittee was adjourned.]

APPENDIX

PREPARED STATEMENT OF CHAIRMAN MIKE COFFMAN

Good morning. This hearing will come to order.

I want to welcome everyone to today's legislative hearing on: H.R. 571; H.R. 593; H.R. 1015; H.R. 1016; H.R. 1017; H.R. 1128; and H.R. 1129.

The latter two, H.R. 1128 and 1129, are bills suggested for this hearing by the Minority, so I will ask Ranking Member Kuster to address them in her opening remarks. I also welcome Full Committee Chairman Jeff Miller and ask unanimous consent that the Honorable Ann Kirkpatrick, the previous Ranking Member of this Subcommittee, be allowed to join us on the dais. While we are at it, I would also like to ask unanimous consent that a statement from the American Legion be entered into the hearing record. Hearing no objection, so ordered.

Today, we will address H.R. 571—The Veterans Affairs Retaliation Prevention Act of 2015, which was introduced by Full Committee Chairman Jeff Miller. This bill will improve the treatment of whistleblower complaints by the VA by defining a set process for whistleblowers help correct problems at the lowest level possible, while creating necessary penalties for supervisors who retaliate against whistleblowers.

Second, H.R. 593—The Aurora VA Hospital Financing and Construction Reform Act of 2015 is a bipartisan bill I introduced along with the rest of the Colorado delegation. H.R. 593 would increase the authorization cap to help the VA to finally finish the Aurora Medical Center, with the much-needed help of the Army Corps of Engineers, in order to give Colorado veterans the state-of-the-art medical facility they deserve. Since this bill's introduction, the VA has announced that the Aurora project will cost at least $1.73 billion, a full $1.4 billion over the original cost found in GAO's report. This is simply outrageous and could very well make this hospital the most expensive in our nation's history. Notably, according to GAO, the New Orleans VA hospital construction project will top $1 billion as well, so mismanagement, cost overruns, and delays are the norm for VA's construction program. For that reason, I question whether VA should conduct its own major construction at all.

While it is my top priority to get this hospital built so that Colorado veterans get the service they deserve, we simply cannot authorize a nearly $1 billion authorization cap increase without VA presenting the options it has to correct its own poor decisions with only half of a hospital to show for it. VA has reprogrammed a portion of the funds needed to finish the Aurora construction, but it cannot continue to pull money from other projects thereby robbing other veterans around the country of a timely completion of their hospital. Perhaps we could use VA bonuses to provide funding for this grossly mismanaged project. Perhaps we could amend the Choice Act so that some of the $5 billion authorized for minor construction could be used to finish this project.

But, what is absolutely clear is that before any money is given to the VA to bail them out of the mess they created in Aurora, VA construction officials responsible for this travesty must be held accountable. These individuals should not be simply taken out of the chain of command for VA construction; they should be FIRED. If anyone in the private sector allowed a project under their supervision to get $1 billion over budget, the decision to fire them would be simple. That should happen here and I look forward to our discussion today with VA on ways forward.

Third, we will address H.R. 1015—The Protecting Business Opportunities for Veterans Act of 2015 sponsored by the Honorable Tim Huelskamp of Kansas.

H.R. 1015 will make tremendous strides at holding accountable the bad actors that attempt to defraud Veteran Owned Small Businesses of crucial set asides they receive in business.

Fourth, we will discuss H.R. 1016—The Biological Implant Tracking and Veteran Safety Act of 2015 introduced by the Honorable Phil Roe of Tennessee. This legislation requires the VA to implement a standard identification protocol for biological implants, consistent with the FDA's system, which would improve VA's ability to prevent implantation of contaminated tissue and also to notify veterans in cases of recalls.

Fifth, we will hear about H.R. 1017, The Veteran Information Security Improvement Act, which was sponsored by the Honorable Jackie Walorski from Indiana. This IT Security directive is designed to assist VA in mitigating known weaknesses by identifying detailed actions that should be taken to address its longstanding information security challenges.

Once again, I would like to thank all those in attendance for joining us in our discussion today, and I now recognize Ranking Member Kuster for five minutes to issue her opening statement.

PREPARED STATEMENT OF CHAIRMAN JEFF MILLER OF THE FULL COMMITTEE

Thank you, Chairman Coffman.

It is a pleasure to be here today with you to discuss my bill, H.R. 571, the Veterans Affairs Retaliation Prevention Act of 2015. During the 2014 VA scandal that this Committee uncovered, a culture of retaliation and bureaucratic corruption gripped the department. The hallmark of that culture was and remains the rampant retaliation against VA employees who speak up to fix problems within the VA.

These problems were so widespread that, in 2014, the Office of Special Counsel became inundated with more whistleblower complaints than all other agencies in the federal government combined. Unfortunately, despite promises from VA leadership that whistleblower retaliation will no longer be tolerated, continued occurrences of retaliation and the lack of any meaningful accountability show that is not the case. Proper oversight of any federal agency simply cannot be done effectively without employees within that agency informing the congress and other oversight bodies of specific problems.

Over the years, numerous federal statutes have been passed to provide added protections to whistleblowers, but many VA supervisors have managed to consistently circumvent these laws, without repercussion, to the detriment of good employees. My bill seeks to put an end to that.

Specifically, H.R. 571 would provide VA employees who seek to report potential government waste, criminal behavior, or compromised healthcare services within the VA a set process to fix problems at the lowest level possible while affording them improved protection from retaliation. This legislation will also prohibit superiors from retaliating against employees who report or assist in reporting problems to the VA, the Inspector General, Congress, or the GAO.

Employees who serve as a witness in investigations and those who refuse to perform illegal acts in the course of their employment will also be protected. To ensure accountability, H.R. 571 will provide meaningful penalties to VA employees who are found to have retaliated against another employee for filing a whistleblower complaint.

Specifically, the retaliating employee would receive: A suspension or removal from federal service; a fine to repay the expense borne by the federal government in defending their retaliatory behavior; a forfeiture of bonuses received while the retaliation occurred; and a prohibition of receiving future bonuses for a one year period.

Finally, this legislation requires improved training to be provided to all VA employees on the protections afforded to employees making complaints and the repercussions that retaliating employees will face if they seek to suppress positive change. America's veterans deserve the highest quality services provided by the VA. Improvements to those services often come in the form of suggested fixes by its employees.

This commonsense legislation would provide the process to safely suggest those fixes while giving Secretary McDonald, and all secretaries in the future, the tools to hold accountable employees who seek to prevent change.

I look forward to working with Committee members, our VSO partners, the VA, and other stakeholders on this bill, because protecting the conscientious VA employees who report waste and wrongdoing within VA must be among our constant priorities.

Thank you once again, Chairman Coffman, for holding this hearing and for your hard work and leadership of the subcommittee on oversight and investigations. I appreciate the opportunity to be with you all today.

With that, I yield back.

STATEMENT OF
MEGHAN FLANZ
DIRECTOR
OFFICE OF ACCOUNTABILITY REVIEW
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE
COMMITTEE ON VETERANS' AFFAIRS
U.S. HOUSE OF REPRESENTATIVES

MARCH 19, 2015

Good morning Chairman Coffman, Ranking Member Kuster, and Members of the Committee. Thank you for inviting me here today to present our views on several bills on matters of whistleblower protection, VA's hospital construction project in Denver, Colorado, information technology, procurement and management of biological implants, and Veteran and service-disabled Veteran-owned small businesses. Joining me today are Dr. Michael Icardi, VHA's National Director of Pathology and Laboratory Services, Stan Lowe, who serves as VA's Deputy Assistant Secretary for Information Security as well as its Chief Information Security Officer, and finally Dennis Milsten, VA's Associate Executive Director, Office of Operations, of VA's Office of Construction and Facilities Management.

H.R. 571 Veterans Affairs Retaliation Prevention Act of 2015

H.R. 571 would add a new subchapter to title 38, U.S. Code on whistleblower complaints. The new section 721 would define a "whistleblower complaint" to include not only a VA employee's disclosure of wrongdoing, but also a complaint made by a VA employee assisting another employee to disclose wrongdoing.

Section 722 would establish a process for employees to file whistleblower complaints with their immediate supervisors; require supervisors to notify employees in writing, within two business days of receiving a complaint, whether the disclosure meets the statutory definition of whistleblowing; require supervisors to notify employees of actions taken to address their complaints, and permit employees to elevate complaints if the employee determines the action taken was inadequate; and require the Secretary to notify whistleblowing employees of the opportunity to transfer to another position.

Section 723 would require the Secretary to discipline any employee found to have committed an offense listed in subsection 723(d), with a first offense punishable by at least a 14-day suspension and a second offense punishable by removal, and would limit the notice and reply period associated with such discipline to not more than five days. Section 723 would also limit the appeal rights of employees who are removed so

that they would match the limited appeal rights of VA Senior Executives under 38 U.S.C. § 713. Section 723(b) would require the Secretary to charge employees found to have committed any offense listed in subsection 723(d) a fee to recoup the costs borne by the government as a result of the offense.

Section 724 would require the Secretary to consider protection of whistleblowers in evaluating supervisors' performance, prohibit payment of an award to a supervisor within a year after the supervisor is found to have committed an offense listed in subsection 723(d), and require the Secretary to recoup an award paid to a supervisor during a period in which the supervisor committed such an offense.

Section 725 would require the Secretary to coordinate with the Whistleblower Protection Ombudsman to provide annual training to all VA employees on whistleblower rights and protections, including the right to petition Congress regarding a whistleblower complaint. Section 726 would require annual reports to Congress on the number and disposition of whistleblower complaints filed with VA supervisors and through other disclosure mechanisms, and would also require the Secretary to notify Congress of whistleblower complaints filed with the Office of Special Counsel (OSC).

VA is absolutely committed to correcting deficiencies in its processes and programs, and to ensuring fair treatment for whistleblowers who bring those deficiencies to light. Secretary McDonald talks frequently about his vision of "sustainable accountability," which he describes as a workplace culture in which VA leaders provide the guidance and resources employees need to successfully serve Veterans, and employees freely and safely inform leaders when challenges hinder their ability to succeed. We need a work environment in which all participants – from front-line staff through lower-level supervisors to senior managers and top VA officials – feel safe sharing what they know, whether good news or bad, for the benefit of Veterans.

In recent months the Department has taken several important steps to improve the way we address operational deficiencies, and to ensure that those who disclose such deficiencies are protected from retaliation. Last summer, the Secretary reorganized and assigned new leadership to the VA Office of the Medical Inspector (OMI), the component of the Veterans Health Administration that reviews whistleblower disclosures related to VA health care operations. Also last summer, the Secretary established the Office of Accountability Review, or OAR, to ensure leadership accountability for whistleblower retaliation and other serious misconduct. VA has also improved its collaboration with the Office of Special Counsel, which is the independent office responsible for overseeing whistleblower disclosures and investigating whistleblower retaliation across the Federal government. VA has negotiated with OSC an expedited process to speed corrective action for employees who have been subject to retaliation. That process is working well, and we are now beginning a collaborative effort with OSC's Director of Training and Outreach to create a robust new training program to ensure all VA supervisors understand their roles and responsibilities in protecting whistleblowers.

While we appreciate the Committee's efforts to assist the Department in these endeavors, we believe the specific whistleblower disclosure and protection procedures provided by this bill would be unworkable. We also believe they are duplicative of the long-standing system of OSC authorities, remedies and programs specifically created to address claims of improper retaliation in the workplace. We believe these current whistleblower protections are effective, and as noted above VA is working closely with OSC to ensure the Department and its employees are gaining the maximum benefits from its remedies and protections.

First, turning to what we see as likely unintended consequences of H.R. 571, the bill's strict notification requirements, short timelines, and severe penalties may create an adversarial relationship between supervisors and subordinates that would likely hinder rather than foster sustainable accountability. The bill would require the supervisor to notify the employee within two days after receiving a disclosure to indicate whether the supervisor has determined that the disclosure meets the statutory criteria for whistleblowing and, if so, what specific actions the supervisor will take to address the complaint. Two days would be inadequate in many cases for a supervisor to come to an informed conclusion that "there is a reasonable likelihood that a complaint discloses a violation of any law, rule, or regulation, or gross mismanagement, gross waste of funds, abuse of authority, or substantial and specific and danger to public health and safety," in the terms of the bill. The fact that there are substantial "downstream" effects from these two-day determinations will in our view create unpredictable and destabilizing effects in a workplace where collaboration and trust is paramount.

The bill would also impose specific penalties on supervisors found to have engaged in retaliation and would significantly limit the time those supervisors have to defend themselves against the imposition of those penalties. The bill would also require VA supervisors to reimburse the government for the costs associated with retaliation, a requirement unparalleled in any other Executive Branch agency. While well-intentioned and designed to protect VA whistleblowers, we believe the cumulative effect of these provisions, in combination with the two-day notification requirement, would not only raise a host of constitutional and other legal issues, but would also leave supervisors too fearful about the possible penalties for retaliation to effectively manage their employees. We also believe that imposing onerous new requirements on VA supervisors, alone in government, would significantly impede the Secretary's efforts to recruit and retain the talented leaders needed to improve service to Veterans.

From a legal perspective, our analysis suggests that portions of H.R. 571 present due process problems and conflicts with other laws. We'd be happy to share those concerns with you in greater detail. VA is unable to estimate the costs for H.R. 571 at this time.

H.R. 593, the Aurora VA Hospital Financing and Construction Reform Act

Section two of the bill would extend the authorization of the major medical facility project to replace the VA Medical center in Denver, Colorado, in an amount not to exceed $1,100,000,000.

Section three of the bill would require within thirty days of enactment that VA enter into an agreement with the U.S. Army Corps of Engineers (USACE) to obtain, on a reimbursable basis, the services of USACE for "construction agent responsibilities" for VA's Aurora, Colorado medical facility project (the "Aurora Project"). The section further sets out responsibilities under the agreement, including performing the project, design, contract and construction management necessary to complete the Aurora Project.

Section three further requires VA to submit a report to the House Veterans Affairs Committee within 180 days after reaching the agreement that includes detailed plans and cost estimates, and then requires progress reports on the Aurora Project every 180 days. It also contains provisions to ensure VA provides USACE with documents and information it determines necessary to carry out the agreement, as well as any other assistance, to be provided at no cost to USACE.

Mr. Chairman, we appreciate your continuing engagement and collaboration with VA to move this project forward in the wake of the setbacks that we are all familiar with. We will continue to depend on open communication and collaboration, working together to ensure that the hospital is completed in good order to meet the needs of Colorado Veterans. I know that VA leadership has been regularly briefing you and others on the progress we have made in conjunction with USACE to move the project forward.

Before commenting on H.R. 593, we'd note that the views presented here are those of VA, and not those of the USACE, who would bear significant responsibilities under the legislation.

We appreciate and support the inclusion of authorization language in section two of the bill. Based on the USACE's estimate to complete construction, VA estimates that that the final cost of the project will total $1.73 billion, which is larger than the amount that would be authorized in H.R. 593. Therefore, we would like to work with the Committee to ensure any enacted authorization addresses the full estimated cost of the project.

Turning to section three, while we support the intent of this section, we are concerned that the legislation is duplicative of actions already underway and may result in unintended consequences for us as well as USACE. VA has not waited for legislation to begin the process of bringing USACE on as our construction agent for the Aurora Project. VA has engaged USACE through the Economy Act to provide support at the project site as we continue under the interim agreement. In addition, VA and USACE entered into an agreement to begin transitioning the construction agent duties to USACE. USACE has had full access to the planning documents, the designer, the

construction contractor and all VA staff. Members of USACE staff are now located at the project site and participate in progress meetings, work authorization meetings, partnering meetings, and are included in the Executive Program Review meetings. VA and USACE are finalizing the agreement that will allow USACE to award and administer the construction and all ancillary contracts necessary to complete the construction and commissioning of the Aurora Project.

VA remains committed to completing the Aurora Project for our Veterans as soon as practical; at the best value to taxpayers, given where we are today. We welcome the opportunity to discuss our concerns with H.R. 593 with the Committee. VA is unable to estimate the costs for H.R. 593 at this time.

H.R. 1015 Protecting Business Opportunities for Veterans Act of 2015

This bill seeks both to improve oversight and ensure Veteran-owned small businesses (VOSBs) and service-disabled Veteran-owned small businesses (SDVOSBs) actually perform the majority of contract requirements awarded to them. It would import into VA's Veterans First legislation the performance requirements currently applicable to other small business programs under the Small Business Act.

As amended by the National Defense Authorization Act for Fiscal Year 2013, the Small Business Act requires that when small businesses perform contracts awarded under a sole-source or set-aside authority, they may not subcontract out more than 50% of the total contract cost to other firms, except firms with the same socioeconomic profile as the prime contractor (i.e., a "similarly situated firm"). This Government-wide performance requirement applies to contracts where the prime contractor received the award through a set-aside or sole source process. Because the prime contractor received the award based in part on its socioeconomic status, the Small Business Act does not permit the firm then to subcontract out most of the work to firms that would have been ineligible to receive the award.

The proposed bill would update the VA counterpart to this provision to apply the same cost-based formula for performance as adopted in the Small Business Act. However, it would apply to all awards to SDVOSBs and VOSBs that count toward those goals, not just set-asides or sole source awards under the Veterans First Contracting Program. VA, like other Federal agencies, awards contracts through myriad acquisition authorities, and applying this contract clause in all cases will likely have unintended consequences.

While supportive of the goal of improving the program's oversight and performance, there are other technical matters and ambiguities that VA would like to discuss with the Committee in order to provide a position on the bill. VA will be pleased to discuss these issues further with staff, and provide technical assistance where requested, to aid the Committee in crafting language to carry out the Committee's intended purposes. VA is unable to estimate the costs for H.R. 1015 at this time.

H. R 1016 Biological Implant Tracking and Veteran Safety Act of 2015

Section 2 of H.R. 1016 would add a new section 7330B to title 38, United States Code, to require the Secretary to adopt and implement the unique device identification system developed by the U.S. Department of Health and Human Services, Food and Drug Administration (FDA) for medical devices (or else a comparable standard identification system) for use in identifying biological implants intended for utilization in VA medical procedures. Section 2 would require that VA permit a vendor to use any accredited agency identified by the FDA as an issuing agency pursuant to section 830.100 of title 21 of the Code of Federal Regulations (C.F.R.). Section 2 would also require the Secretary to implement, not later than 180 days after the date of enactment, a system for tracking biological implants from donor to implantation and implement a system of inventory controls compatible with such system. The inventory controls would need to enable the Secretary to notify, as appropriate (based on an evaluation of the risks and benefits provided by appropriate VA medical personnel), VA patients who are in receipt of biological implants that are subject to recall by the FDA.

In addition, section 2 of the bill would provide that in cases of conflict between the proposed revision to Title 38 and a provision of the of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 301 et seq.) or sections 351 or 361 of the Public Health Service Act (42 U.S.C. § 262) (including any regulations issued under such Acts), the provision of the Federal Food, Drug, and Cosmetic Act or the Public Health Service Act (including any regulations issued under such Acts) would apply.

For purposes of section 2, the term "biological implant" would be defined as any human cell, tissue, or cellular or tissue-based product: (1) under the meaning given the term "human cells" in 21 C.F.R. § 1271.3 (or any successor regulation); or (2) that is regulated as a device under section 201(h) of the Federal Food, Drug, and Cosmetic Act. With respect to biological implants defined in the former case (definition of "human cells"), the standard identification system would have to be implemented not later than 180 days after the Act's enactment. With respect to those defined in the latter case (product that is regulated as a device), the Secretary would be required to adopt or implement such standard identification system in compliance with the (compliance) dates established by the FDA pursuant to section 519(f) of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. § 360i(f)).

Should the tracking system for biological implants not be operational by the 180-day deadline described above, the Secretary would be required to submit a written

explanation to the Congressional Committees on Veterans' Affairs on the impediment to such implementation, the steps being taken to remediate such impediment, and the target dates for a solution. The reporting requirement would continue for each month until such time as the system is operational.

Section 3 of H.R. 1016 would add a new section 8129 to title 38 to govern the procurement of biological implants. Section 3 of the bill would limit procurement of human biological implants to vendors that use the standard identification system set forth in section 2 and have safeguards to ensure that a production identifier has been in place for each step of distribution from its donor. This section would require that each vendor and any tissue distribution intermediaries or tissue processors are appropriately registered with the FDA. The Vendor would also have to ensure donor eligibility determinations and any other required records required by the Secretary accompany each biological implant at all times regardless of the country of origin of the donor. The vendor would also have to consent to inspection and audit, which would include the accuracy of records and handling of products. Vendors would be required to cooperate with FDA and other recalls and provide adverse event reports or warning letters to the Secretary within 60 days. Records of procurement would have to be maintained for at least 5 years. In addition, the vendor would be required to provide biological implants only from tissue processors that maintain active accreditation with the American Association of Tissue Banks or similar national accreditation.

Section 3 of the bill would also limit procurement of non-human biological implants to vendors that use the standard identification system set forth in Section 2. This section would require that each vendor and any tissue distribution intermediaries are appropriately registered with the FDA. The vendor would also have to consent to periodic inspection and audit, which would include the accuracy of records and handling of products. Vendors would be required to cooperate with FDA and other recalls and provide adverse event reports or warning letters to the Secretary within 60 days. Records of procurement would have to be maintained for at least 5 years. Section 3 would require the Secretary to procure biological implants under the Federal Supply Schedules (FSS) of the General Services Administration, unless such implants are not available under such schedules. The measure would also require the Secretary to accommodate reasonable FSS vendor requests to undertake outreach efforts to educate VA medical professionals about the use and efficacy of such FSS biological implants. It would further provide that section 8123 of title 38 (related to procurement of prosthetic appliances) does not apply to the procurement of biological implants. For biological implants not available on the FSS, the Secretary would be required to procure these items using competitive procedures in accordance with the Federal Acquisition Regulations and applicable law.

Section 3 would establish penalties for an agency employee who is found responsible for procuring a biological implant with the intent to avoid or with reckless disregard of the requirements of this section. Specifically, such an individual would be ineligible to hold a certificate of appointment as a contracting officer or to serve as the representative of an ordering officer, contracting officer, or purchase card holder.

Section 3 defines 'biological implant' as it would be defined in section 7330B(d). A "production identifier" would be defined as a distinct identification code that relates a biological implant to the human donor and to all records of the implant, and includes information designed to facilitate effective tracking and satisfy the requirement of sub-section (c) of section 1271.290 of title 21 of the C.F.R. The term 'tissue distribution intermediary' is an agency that acquires and stores human tissue for further distribution but performs no other tissue banking functions. Lastly, 'tissue processor' is defined as an entity processing human tissue for use in biological implants.

The bill states that the effective date of section 8129 of title 38 would be 180 days after the date on which the tracking system required in subsection (b) of section 7330B is implemented.

Lastly, this section contains a special rule for cryopreserved products which allows a three-year period after the effective date of section 8129 of title 38 for VA to utilize previously produced and labeled biologics without relabeling under section 7330B.

While VA agrees with the general purpose of the first two components of the H.R. 1016, i.e., to adopt a standard identification system and to implement a tracking system, VA does not support the bill, which we find both unnecessary and limiting to those purposes. The bill while recognizing a fundamental difference between human and non-human biologics requires VA to use the FDA's unique device identification (UDI) or comparable standard for both. H.R. 1016 does recognize the need for a higher standard for human biologics as indicated by the requirement for a vendor to ensure safeguards are in place for the use of a production identifier at all stages in production; however, it then prohibits VA from using such an identifier to track the human biologics it possesses, transfers, or implants. Section 2 also states that the Secretary shall permit vendors to use any of the FDA accredited entities identified as an issuing agency for adopting or implementing a standard identification system for biological implants. This effectively limits VA to the use of the FDA's UDI and its minimum standards. For VA's purposes, those standards are not sufficient to provide the Donor to Final disposition tracking of human derived biologics, nor enable implementing a standard system.

VA currently has a tracking system for recalls through VHA Directive 1068 that extends to suspending use of the recalled product. The tracking system proposed in H.R. 1016 is tied to the FDA UDI component and to that extent is premature and not inclusive to all biologic implants as indicated by the numerous exceptions present in 21 C.F.R. § 1271.3. Further the UDI is only manufacturer specific and as a result when present on a device will not be assured of being unique within the VA's system. This will create unnecessary difficulties and delays compared to an already well-functioning system for blood and pharmacy products fields by VA Division of Quality and Safety.

Section 3 discusses VA performance of inspections and audits. We believe these should be functions of FDA. While it is typical that VA asks for the ability to inspect paperwork and facilities with which it contracts, this section seems to go further,

indicating that the VA asking for consent for periodic inspections and audits of both documentation and handling practices. When coupled with section C this implies that the VA would need to verify periodically the documentation and practices involved in procurement of tissue by a contractor and any intermediaries by direct inspection This should be a function of the FDA which registers the vendor and intermediaries.

Section 3 discusses the retention of records associated with procurement of an implant for five years and is not consistent with the record retention requirement by FDA. FDA requires retention of donor records for 10 years after administration. See 21 C.F.R. § 1271.55(d)(4). Similarly AATB requires 10 year retention. It should be noted that some institutions permanently retain these records. In particular some types of biologic may be stored for extended periods prior to use and it may take several years for an adverse outcome to manifest. Disposal of records, in particular, the actual production identifier and donor documentation will prevent the ability to track human derived biologics to their donor and ensure the presence of biologics in the VHA which cannot be reliably tracked back to the original donor.

VA also disagrees with the requirement that biological implants be procured from FSS sources (unless the products are not available from these sources) and the prohibition against using VA's authority in 38 U.S.C. § 8123 to purchase biological implants. The first unduly restricts VA's authority to determine the hierarchy of sources. All biological implants are not currently available on the FSS and clinicians are not involved in the decision to place these products on contract. Additionally, VHA has determined that these should be available through national contracts that would take precedence over FSS. VA is developing an appropriate initial contract vehicle to acquire such products.

Removing these products from the scope of section 8123 would, we believe, unduly interfere with a clinician's authority to determine the particular device (biological implant) that best meets the patient's individual medical needs by restricting VA's authority to acquire that particular device. Like other procurements under section 8123, quality assurance and regulatory compliance could be achieved here through internal acquisition processes and controls, avoiding needless treatment delays due to the federal contracting process.

Finally, H.R. 1016 would limit VHA purchases to contracted products or through competitive processes from vendors meeting the listed procurement requirements and would provide penalties to procurement employees of the Department who may need to purchase products off contract to meet the immediate needs of the patient and provider. In addition, vendors with single source or multi-source products may not choose to contract with the VA under the proposed requirements, thereby eliminating or limiting availability of these products to our patients. Shortages of biologic products could also affect the ability of VHA to obtain products under contract or through competitive processes. As a result, the medical care of Veterans could be delayed or interfered with. VHA must maintain the ability to provide safe, effective and timely care to Veterans. VA is unable to estimate the costs for H.R. 1016 at this time.

H.R. 1017, the Veterans Information Security Improvement Act

The bill would add section 5723A to 38 U.S.C. with a series of required processes for the management of VA's information technology (IT) portfolio. H.R. 1017 would require implementation of specific processes related to the management and security of VA's critical network infrastructure, computers and servers, operating systems, web applications, and VistA, the electronic health record. The bill prescribes specific operational controls, procedures, monitoring and testing. It also requires VA to increase existing transparency through increased reporting, certification of compliance with all relevant laws and regulations regarding information security, and an additional Office of Inspector General report on implementation the Act.

According to Government Accountability Office (GAO) testimony from March, 2014, "in a dynamic environment where innovations in technology and business practices supplant the status quo, control activities that are appropriate today may not be appropriate in the future." The GAO testimony also states that legislation should emphasize specific "security-related actions should be taken based on risk." Information Security: VA Needs to Address Long-Standing Challenges (GAO-14-469), before the Subcommittee on Oversight and Investigations, Committee on Veterans Affairs, House of Representatives (March 25, 2014).

VA opposes H.R. 1017 because while many provisions are well-intended, they would impede the flexibility necessary for effective and nimble IT management to meet mission-critical needs. As Veterans' needs change, as laws change, and as the threat environment changes, VA must have flexibility in managing its IT resources to support care and services provided to Veterans.

VA's unique mission of delivering care and benefits to Veterans relies upon a considerable IT enterprise that must remain flexible in a risk-based world. VA works tirelessly to ensure it is doing everything possible to protect Veteran information and VA systems through its defense-in-depth security posture, while understanding that risks and vulnerabilities exist. To provide high quality services we must remain agile both in responding to the needs of the Veterans and in our ability to adopt evolving technology and best practices. Our management of risks and vulnerabilities demonstrates the maturity of our IT organization and our commitment to both deliver on our mission to serve Veterans with our obligation to protect Veteran information.

In a dynamic environment where innovations in technology and business practices are frequent, practices that are appropriate today may well be less than ideal when compared to alternatives in the future. VA must have the flexibility to adjust to the natural evolution of security practices as circumstances warrant. VA is concerned that very detailed legislation prescribing those practices could impede our ability to quickly adapt to the constantly changing security environment.

Section 4(b)(2) for example would not allow for flexibility or necessary risk-based decisions. It requires VA to implement automated patching tools and processes that ensure security patches are installed for any software or operating system on a computer by not later than 48 hours after the patch is made available. That timeline would preclude VA from reviewing patches to ensure they do not interfere with systems utilized to provide care and services to Veterans. Indiscriminately implementing software patches would increase the likelihood of system crashes and outages to VA's 45,000 applications. An automated patching tool would prevent authorized personnel from conducting in-depth analysis of the patches prior to implementation. As VA has experienced, patches received from the vendor may cause unanticipated operability issues with VA systems. An evaluation must be performed on any patches to ensure the operability of the particular application or system to ensure the patch does not have a deleterious impact to services that VA provides.

Section 5(a) is another example of how H.R. 1017 could preclude an effective review or risk-based decision process. It requires VA to upgrade or phase out outdated or unsupported operating systems to protect computers of the Department from harmful viruses, spyware, and other malicious software that could affect the confidentiality of sensitive personal information of Veterans. While this requirement appears straightforward, in literal application we believe there would be unintended consequences. VA utilizes many systems that are necessary to the operational and mission needs of the Department that could be defined as "outdated" or "unsupported."

VA has isolated all systems that are operating on operating systems that could be considered "outdated" or "unsupported" due to unique mission needs, to ensure they are not accessible to unauthorized users. Indiscriminately phasing out "outdated" or "unsupported" systems would impact physicians at the point of care. Many of these systems serve specialized purposes and their function cannot simply be transitioned without proper testing and migration planning to other, newer systems without impact. Indiscriminate mandates which force migration of these systems to newer, supported operating systems would undoubtedly affect patient care and the broader VA mission.

Another reason VA cannot support H.R. 1017 is because many of the operational mandates have already been promulgated through Executive Branch policies, Executive Orders and other policy guidelines. With few exceptions, the processes and tasks prescribed in sections 2 through 7 are already either complete, underway, or planned in a variety of efforts. For example, VA Directive and Handbook 6500 is consistent with VA's information security statutes, 38 United States Code (U.S.C) §§ 5722-5727; the Federal Information Security Management Act (FISMA), 44 U.S.C §§ 3541-3549; and Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

These directives establish policy and responsibilities for incorporating National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach;* SP 800-39, *Managing Information Security Risk:*

Organization, Mission, and Information System View; and SP-800-53, *Recommended Security Controls for Federal Information Systems and Organizations.* These requirements we believe are fully adequate to ensure appropriate security for VA information technology assets that store, process, or transmit VA information.

In addition VA continues to work with the Office of Inspector General to ensure full compliance with FISMA requirements. VA has established robust and comprehensive plans of actions to carry out many OIG suggestions, in addition to establishing a permanent project team to maintain its Continuous Readiness in Information Security Program (CRISP). Placing many of these mandates in law would we believe hinder the ability of VA to quickly and effectively respond to the constantly changing cybersecurity environment.

Each year VA methodically improves our defense-in-depth security posture by introducing and refining technologies and procedures that enhance our ability to protect VA networks and devices in response to constantly changing threat environments. These efforts ensure VA employees, contractors, and other staff using VA computing devices are compliant with mandatory privacy and security training requirements and provide responsive and timely submissions to various legislative reporting requirements.

VA understands and appreciates the Committee's interest in this critical area, and its responsibilities for oversight. VA has an obligation to safeguard the data we hold on Veterans — and takes that obligation seriously. As VA faces ever-evolving threats in an increasingly complex IT landscape, VA is constantly refining its ability to protect Veteran information. VA continuously employs progressive security measures to protect data and secure the VA network and its IT systems. We look forward to working with the committee to ensuring Veteran information and VA systems are protected, and the Department is eager to work with the committee on solutions that will serve Veterans. VA is unable to estimate the costs for H.R. 1017 at this time.

H.R. 1128, the Department of Veterans Affairs Cyber Security Protection Act

H.R. 1128 would require VA to submit on a quarterly basis VA plans for addressing known information security vulnerabilities and plans for replacing outdated operating systems, including detailed timelines with specific milestones. It would also include in the enumerated responsibilities of the Assistant Secretary for Information and Technology the requirement to ensure that any software or Internet applications used by VA are as secure as practicable from known vulnerabilities that could affect the confidentiality of Veterans' sensitive personal information.

H.R. 1128 would require VA within 60 days to submit a report on third-party validation of VA information security, with a description of steps VA has taken to provide a systemic and ongoing evaluation of VA information security by a non-Department entity. The bill would add a new section 5727 to title 38 which would require quarterly reports on incidents of failure to comply with established IT policies, and VA's response

to those incidents. The new section would also require a detailed discussion of whether recommendations of the National Institute of Standards and Technology, the Office of Management and Budget, or the Department of Homeland Security have been implemented.

The bill would add a new section 5728 to title 38 to require a strategic plan for improving the information security and information technology infrastructure of the Department. There are other provisions relating to requirements for certain VA contracts relating to information security threats. Finally, H.R. 1128 would require within five years a report on VA information security protections and the accountability of VA for information security breaches.

VA appreciates and supports the goals of the bill, and believes some of the reporting requirements may be useful for both VA and the Congress. However, some elements of the bill would be particularly onerous in practice, and one provision applying to VA contractors would provide weaker protection than is already present in the Federal Acquisition Regulation, and thus we cannot support the bill as drafted. We would appreciate the opportunity to work with the committee to ensure the reporting requirements are feasible and useful for the committee's oversight responsibilities. VA is unable to estimate the costs for H.R. 1128 at this time.

H.R. 1129 Veterans' Whistleblower and Patient Protection Act of 2015

H.R. 5054 would amend title 38, chapter 3, of the U.S.C. to add a new section 319A. The bill would establish an Office of Whistleblower and Patient Protection within VA to receive, investigate, and recommend actions to address, whistleblower disclosures and retaliation complaints filed by VA employees, patients, and other individuals. The bill would require that all covered complaints – defined as complaints regarding alleged Prohibited Personnel Practices described in section 2302(b)(8) or section 2302(b)(9)(A)(i), (B), (C), or (D) of title 5, or regarding the safety of a patient at a VA medical facility – be referred to this new office, and not to VHA's Office of the Medical Inspector.

The bill would require the Secretary to appoint a career Senior Executive as Director of the Office, to appropriately resource the Office with a sufficient number of attorneys, investigators, and other personnel, and to report to Congress every 180 days the number of covered complaints received, investigations commenced, and allegations sustained, among other matters. The bill would require the Director of the Office to refer complaints, as appropriate, to the Attorney General, Special Counsel, or VA Inspector General, and to coordinate with the Special Counsel and Inspector General to ensure that the actions of the Office do not duplicate those of the other entities.

As with H.R. 571, VA appreciates and shares the Committee's interest in ensuring that whistleblower disclosures are effectively investigated and addressed for the benefit of Veterans. As noted with respect to the prior bill, however, we believe that

our current processes, and those of our partners at the Office of Special Counsel, are adequate to meet the need. VA works closely with OSC to ensure that disclosures are promptly and properly investigated, that substantiated issues are corrected, and that whistleblowers are protected from discriminatory conduct.

In the specific context of patient safety issues, VA's newly reorganized Office of the Medical Inspector provides expert, unbiased, and credible investigations and recommends appropriate action to correct substantiated issues. We believe there is no need to establish a separate office to carry out those functions. VA is unable to estimate the costs for H.R. 1129 at this time. We are of course glad to discuss these important issues with the Committee at any time.

SERVING
WITH
PRIDE

A M V E T S

NATIONAL
HEADQUARTERS
4647 Forbes Boulevard
Lanham, Maryland
20706-4380
TELEPHONE: 301-459-9600
FAX: 301-459-7924
E-MAIL: amvets@amvets.org

TESTIMONY OF

DIANE M. ZUMATTO
AMVETS NATIONAL LEGISLATIVE DIRECTOR

BEFORE THE

HOUSE COMMITTEE ON VETERANS' AFFAIRS, SUBCOMMITTEE
ON OVERSIGHT AND INVESTIGATIONS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS
FIRST SESSION

CONCERNING

A LEGISLATIVE HEARING ON:

HR: 571, 593, 1015, 1016, 1017, 1128 & 1129

THURSDAY, 19 MARCH 2015
0800
334 CANNON HOUSE OFFICE BUILDING

Chairman Coffman, Ranking Member Kuster and distinguished committee members, I am pleased to have this opportunity to sit before you today to share our comments on pending legislation.

HR 571, the Veterans Affairs Retaliation Prevention Act of 2015: AMVETS supports this important piece of legislation which would provide much needed protections for those who step forward with knowledge of problems within the VA.

If we expect VA employees to take actions to prevent fraud, illegal acts, etc. those employees must have the confidence that: they will be safe from any form of retaliation, either personal or professional; that the information they provide will be acted on in a confidential and appropriate manner; and that the information they provide will also be handled in a timely manner.

This proposed legislation would also help to:

a. improve the process of filing whistleblower complaints;
b. expand and clarify the prohibitions in whistleblower cases;
c. expand the penalties related to whistleblower cases, including:
- suspension/termination of employment for offenders;
- the development of a fee schedule accounting for the cost to the government of committing prohibited practices; and
- the limitation of bonuses to those who commit prohibited practices.
- better educate VA employees, via annual training and the website, about the whistleblower process and the proper ways of dealing with these cases.

AMVETS applauds Chairman Miller's continued efforts to ensure that VA employees, many of whom are veterans, have an equitable and safe environment within which to better serve all American veterans.

HR 593, Aurora VA Hospital Financing and Construction Reform Act of 2015: AMVETS supports this legislation, if enacted, would hopefully bring some long-awaited closure to several years of endless blunders, mismanagement, cost overruns, etc. It is obvious that the status quo is not working and it is therefore unacceptable.

This proposed legislation would:

a. increase the funding for this project to $1,100,000,000;
b. transfer Construction Agent responsibilities to the Army Corps of Engineers giving them the authority to perform the project, design, contract and construction management necessary to complete the remaining work at the Aurora medical facility;
c. require the submission of detailed completion plans, including estimated costs, to congress (HVAC/SVAC), for the completion of construction of the Aurora medical center;
d. require periodic progress reports be made to congress (HVAC/SVAC); and
e. require the VA to provide to the Army Corps of Engineers, at no cost, any assistance necessary to carry out the project

HR 1015, the Protecting Business Opportunities for Veterans Act of 2015: AMVETS supports this legislation that would improve the oversight of contracts awarded by the VA to small business concerns owned and controlled by veterans.

HR 1016, the Biological Implant Tracking & Veteran Safety Act of 2015: AMVETS supports this legislation that would require the VA to adopt and implement a standard identification protocol for use in the tracking and management of biological implants. This legislation would help to ensure that biological implants such as, tendons, bones, ligaments, skin, eyes, or whole organs, used within the VA could be more easily and appropriately tracked from all the way from the donor to the recipient.

This critical capability to "track and trace" implants should help increase patient safety in case of product recalls (if necessary), assist with inventory management and accountability, and improve efficiencies through the implementation of a standard identification protocol.

Just as importantly, this legislation puts safeguards in place stipulating the requirements that vendors must meet in order to provide VA with both human and non-human biological implants.

HR 1017 and HR 1128, the Veterans Information Security Improvement Act and the Department of Veterans Affairs Cyber Security Protection Act, respectively: AMVETS supports these desperately needed bills which would address previously identified

security weaknesses, as well as, help to prevent, detect and limit damage from unauthorized breaches of the VA's information security system.

Anyone who has had the opportunity to review the latest GAO report on VA's Information Security, knows that, among other things: the integrity of the VA network has been compromised on more than one occasion; that thousands of VA computers are using out-of-date operating systems; and that VA's current information security system is riddled with vulnerabilities. AMVETS finds all of these problems, which make veterans personal and health information ripe for picking by hackers, unacceptable and we applaud Reps. Walorski and Kirkpatrick for her efforts to address these insufficiencies.

Additionally, the VA recently flunked its 16th consecutive cyber security audit indicating that it once again failed to meet the standards of the Federal Information Security Management Act. Both bills make specific recommendations which would increase accountability and go a long way towards strengthening the security of the VA's information systems.

HR 1129, the Veterans' Whistleblower and Patient Protection Act of 2015: while AMVETS has concerns about increasing federal bureaucracy, we do support the intent of this legislation - to protect whistleblowers and patients - by providing a framework for investigating complaints through the establishment of an Office of Whistleblower and Patient Protection within the VA.

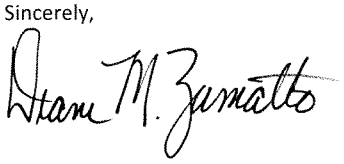
16 March 2015

The Honorable Representative Mike Coffman, Chairman
U.S. House of Representatives
House Committee on Veterans' Affairs
Subcommittee on Oversight and Investigations
335 Cannon House Office Building
Washington, D.C. 20510

Dear Chairman Coffman:

Neither AMVETS nor I have received any federal grants or contracts, during this year or in the last two years, from any agency or program of the federal government.

Sincerely,



Diane M. Zumatto
AMVETS National Legislative Director

Biographical Sketch

Diane M. Zumatto

AMVETS National Legislative Director

Diane M. Zumatto of Spotsylvania, VA joined AMVETS as their National Legislative Director in August 2011. Zumatto a native New Yorker and the daughter of immigrant parents decided to follow in her family's footsteps by joining the military. Ms. Zumatto is a former Women's Army Corps/U.S. Army member who was stationed in Germany and Ft. Bragg, NC, was married to a CW4 aviator in the Washington Army National Guard, and is the mother of four adult children, two of whom joined the military.

Ms. Zumatto has been an author of the *Independent Budget* (IB) since 2011. The IB, which is published annually, is a comprehensive budget & policy document created by veterans for veterans. Because the IB covers all the issues important to veterans, including: veteran/survivor benefits; judicial review; medical care; construction programs; education, employment and training; and National Cemetery Administration, it is widely anticipated and utilized by the White House, VA, Congress, as well as, other Military/Veteran Service Organizations.

Ms. Zumatto regularly provides both oral and written testimony for various congressional committees and subcommittees, including the House/Senate Veterans Affairs Committees. Ms. Zumatto is also responsible for establishing and pursuing the annual legislative priorities for AMVETS, developing legislative briefing/policy papers, and is a quarterly contributor to '*American Veteran*' magazine. Since coming on board with AMVETS, Ms. Zumatto has focused on toxic wounds/Gulf War Illness, veteran employment and transition, military sexual trauma, veteran discrimination and memorial affairs issues.

Zumatto, the only female Legislative Director in the veteran's community, has more than 20 years of experience working with a variety of non-profits in increasingly more challenging positions, including: the American Museum of Natural History; the National Federation of Independent Business; the Tacoma-Pierce County Board of Realtors; The Washington State Association of Fire Chiefs; Saint Martin's College; the James Monroe Museum; the Friends of the Wilderness Battlefield and The Enlisted Association of the National Guard of the United States. Diane's non-profit experience is extremely well-rounded as she has variously served in both staff and volunteer positions including as a board member and consultant. Ms. Zumatto received a B.A. in Historic Preservation from the University of Mary Washington, in 2005.

AMVETS, National Legislative Director
4647Forbes Blvd, Lanham, MD 20706
301-683-4016 / dzumatto@amvets.org

STATEMENT OF FRANK WILTON
CHIEF EXECUTIVE OFFICER
AMERICAN ASSOCIATION OF TISSUE BANKS
MCLEAN, VA

FOR PRESENTATION BEFORE THE
HOUSE COMMITTEE ON VETERANS' AFFAIRS
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS
HEARING RELATED TO H.R. 571, H.R. 593, H.R. 1015, H.R. 1016, H.R. 1017, H.R. 1128, AND H.R. 1129
MARCH 19, 2015

Subcommittee Chairman Coffman, Ranking Member Kuster, and Distinguished Members of the House Committee on Veterans' Affairs Subcommittee on Oversight and Investigations:

Thank you for the additional opportunity to come before you today in support of the H.R. 1016, the "Biological Implant Tracking and Veteran Safety Act of 2015." This critical legislation directs the Secretary of Veterans Affairs to adopt a standard identification system for use in the procurement of biological implants by the Department of Veterans Affairs. By building upon the success of the implementation of the Unique Device Identifier, or UDI, this legislation will ensure that biological implants used within the Department can be appropriately tracked from a human tissue donor all the way to the recipient. This critical capability for "track and trace" efforts will enhance patient safety, expedite product recalls when necessary, assist with inventory management, and improve efficiencies.

This legislation takes the bold step of expanding the UDI to all tissue products. In addition to human tissue-devices (which are already covered by the UDI), the legislation adds another product category: certain biological implants or, as termed by the Food and Drug Administration (FDA), 361 human cells, tissues, and cellular and tissue-based products, or HCT/Ps. While many of the biological implants do have company specific bar coding information, by requiring a standardized format for those bar codes, as outlined in this legislation, it will be easier for the Department of Veterans Affairs' medical facilities to utilize universal bar coding conventions and to realize the full benefit of a unique identification system. Finally, by applying a system which has been developed for devices to biological implants, such a solution should also be applicable to other health care settings and other health care systems (such as the Department of Defense health care system or the private sector).

In addition, the organization I represent – the American Association of Tissue Banks or AATB – is pleased that the language, as introduced, ensures that our veterans receive high quality implants by requiring that the biological implants only be sourced from tissue processors accredited by the AATB or similar national accreditation organization. With this change, the Veterans Health Administration (VHA) will be joining the ranks of leading medical centers of excellence which currently require all tissue to be sourced from AATB accredited tissue banks. We are also pleased that the introduced language clarifies that human tissue procured by the VHA can be labeled with any of the three systems already identified by the FDA to be appropriate for biological implants. Under the UDI final rule, FDA has done just that by providing for multiple entities called "issuing agencies." At this time, FDA has provided for three different issuing agencies: (1) GS1, (2) Health Industry Business Communications Council (HIBCC), and (3) ICCBBA. By maintaining this appropriate flexibility, the VHA will ensure a more competitive marketplace.

For those of you unfamiliar with my organization, the AATB is a professional, non-profit, scientific and educational organization. It is the only national tissue banking organization in the United States, and its membership totals **more than 125 accredited tissue banks and approximately 850 individual members**. These banks recover tissue from more than **30,000 donors** and distribute in excess of **two and half million allografts for more than one million tissue transplants performed annually in the U.S**. The vast majority of tissue banks that process tissue maintain AATB accreditation, and the AATB estimates that only 5-10% of the allografts distributed are from tissue donors who were not determined to be suitable by the medical director of an AATB-accredited tissue bank. The AATB does not have a similar estimation for tissue distributed by tissue distribution intermediaries.

The Association was founded in 1976 by a group of doctors and scientists who had started in 1949 our nation's first tissue bank, the United States Navy Tissue Bank. Recognizing the increasing use of human tissue for transplant, these individuals saw the need for a national organization to develop standards, promote ethics and increase donations.

Since its beginning, the AATB has been dedicated to improving and saving lives by promoting the safety, quality and availability of donated human tissue. To fulfill that mission, the **AATB publishes standards and guidance documents, accredits tissue banks, and** certifies personnel. The Association also interacts with regulatory agencies and health authorities, and conducts educational meetings.

First published in 1984 and presently in its 13th edition, the AATB's *Standards for Tissue Banking* are recognized in both the United States and around the world as the **definitive guide for tissue banking**. These Standards are the only private tissue-banking standards published in the United States, and they are the most comprehensive and detailed tissue-banking standards in the world. As such, the **AATB's Standards have served as the model for federal and state regulations as well as several international directives and standards.** Currently, the statutes and/or regulations of 19 states (i.e., California, Connecticut, District of Columbia, Florida, Georgia, Idaho, Illinois, Kentucky, Maryland, Montana, New Jersey, North Carolina, Ohio, Oklahoma, Pennsylvania, Texas, Utah, Virginia, and Wisconsin) reference AATB's Standards, institutional accreditation, or individual certification. And, these Standards are the basis of our accreditation process.

Human tissue is used in a wide variety of medical procedures in the VHA facilities, ranging from wound care management to hernia repair to orthopedic procedures. Human tissue is also used in a wide array of dental services, such as bone augmentation and gum tissue grafting procedures. In fact, according to a Government Accountability Office (GAO) report to this committee, biologics accounted for approximately $75 million in VHA acquisitions in fiscal year 2013. That same GAO report noted that one Veterans Affairs Medical Center (VAMC) had a high percentage of purchases missing serial numbers or lot numbers (16 percent in the first three quarters of fiscal year 2013).[1] I'm hopeful that this legislation will appropriately address this outstanding concern, without providing an undue burden on the health care system. For this and many other reasons, AATB supports this critical legislation.

I realize that some of you may be concerned that this legislation is duplicative and more burdensome than the FDA UDI requirements. If that were the case, it would be difficult for my organization to support its implementation. Rather, as I outlined earlier, the legislation is not duplicative of FDA's efforts because it expands the standard identification system from only devices to also cover 361 HCT/Ps. Thus, it goes beyond what Congress directed FDA to do with respect to the UDI. However, in

[1] http://www.gao.gov/assets/670/660105.pdf

talking to executives of the tissue banks who currently have products on the Federal Supply Schedule (FSS), all are strongly considering expanding the unique identifier to their entire product line because they acknowledge that it is an appropriate value-added benefit for hospitals and other facilities who procure tissue and, ultimately, patients, including veterans.

While I do not have any specific information on the implementation cost of the UDI related to tissue banks, according to a Booz-Allen Hamilton report, the primary cost of the UDI to manufacturers relates to the need to modify or replace information technology or IT systems. For manufacturers, the cost is estimated to be anywhere between $100,000 and $100,000,000, depending on the size and scale of the changes required. Given this broad range, my expectation is that, at least for tissue banks, due to their size, it's more likely that the change will be toward the lower end of the spectrum. That being said, because there is no return on investment, it is likely that tissue banks will need to increase the fee for tissue products to cover the cost of those changes.

But, such an increased cost to the VHA is worth the end result of enhancing patient safety. As the VHA has acknowledged with the previous efforts to create the Veterans Implant Tracking and Alert System or VITAS, there are current gaps in the information collection process for biological implants. As you know, VITAS was designed to track and retrieve identifying information—including the lot and serial number—of surgical implants placed in patients VHA-wide. Therefore, VITAS was developed to address shortcomings in VHA's existing ability to "track and trace" surgical implants. And, without additional developments, VHA's ability to identify and locate patients who received an implant in the event of a manufacturer or FDA recall may be limited. Unfortunately, as outlined in a recent GAO report, due to data-reliability and interoperability challenges, VITAS was suspended at the end of fiscal year 2012. And, as of December 2013, VHA had not decided whether to resume the development of VITAS.

While I can understand your skepticism in requesting the VHA attempt a VITAS-like enterprise in this legislation after failing to do so before, I would note that a lot has changed since 2008 when the VHA first envisioned VITAS. First, there is now a UDI benchmark which allows those developing the necessary software for data capture to move from a design incorporating dozens of different bar coding technologies from all of the AATB-accredited tissue banks to only three different ones outlined by the three different issuing agencies. Thus, the task is much easier. In addition, the VHA is not alone in trying to develop a system for integrating the UDI-like information directly into the medical record. For instance, the Office of the National Coordinator for Health Information Technology (ONC), which is the principal federal entity charged with coordination of nationwide efforts to implement and use the most advanced health information technology and the electronic exchange of health information, is currently focused on ways in which the UDI can be better operationalized to ensure its adoption into HL7 standards – the key standards for the exchange, integration, sharing, and retrieval of electronic health information. As part of those efforts, ONC is initially focusing on implantables – the very focus of the legislation we are discussing today, suggesting that this is an area of potential "low hanging fruit" in which a small investment can reap a big reward. Therefore, the VHA will not be attempting to establish such a system alone but can partner with other governmental entities to ensure its success.

As I hope you can ascertain from my comments, the AATB strongly supports this legislation and urges the subcommittee to favorably report out the bill.

I welcome your questions.

I yield back my time.

ONE PAGE SUMMARY OF FRANK WILTON'S STATEMENT

Thank you for the additional opportunity to come before you today in support of HR 1016, the "Biological Implant Tracking and Veteran Safety Act of 2014." This critical legislation directs the Secretary of Veterans Affairs to adopt a standard identification system for use in the procurement of biological implants by the Department of Veterans Affairs. By building upon the success of the implementation of the Unique Device Identifier, or UDI, this legislation will ensure that biological implants used within the Department can be appropriately tracked from a human tissue donor all the way to the recipient. This critical capability for "track and trace" efforts will enhance patient safety, expedite product recalls when necessary, assist with inventory management, and improve efficiencies.

This legislation takes the bold step of expanding the UDI to all tissue products. In addition to human tissue-devices (which are already covered by the UDI), the legislation adds another product category: certain biological implants or, as termed by the Food and Drug Administration (FDA), 361 human cells, tissues, and cellular and tissue-based products, or HCT/Ps. While many of the biological implants do have company specific bar coding information, by requiring a standardized format for those bar codes, as outlined in this legislation, it will be easier for the Department of Veterans Affairs' medical facilities to utilize universal bar coding conventions and to realize the full benefit of a unique identification system. Finally, by applying a system which has been developed for devices to biological implants, such a solution should also be applicable to other health care settings and other health care systems (such as the Department of Defense health care system or the private sector).

In addition, the organization I represent – **the American Association of Tissue Banks or AATB – is pleased that the language, as introduced, ensures that our veterans receive high quality implants by requiring that the biological implants only be sourced from tissue processors accredited by the AATB or similar national accreditation organization.** With this change, the Veterans Health Administration (VHA) will be joining the ranks of leading medical centers of excellence which currently require all tissue to be sourced from AATB accredited tissue banks. **We are also pleased that the introduced language clarifies that human tissue procured by the VHA can be labeled with any of the three systems already identified by the FDA to be appropriate for biological implants.** Under the UDI final rule, FDA has done just that by providing for multiple entities called "issuing agencies." At this time, FDA has provided for three different issuing agencies: (1) GS1, (2) Health Industry Business Communications Council (HIBCC), and (3) ICCBBA. By maintaining this appropriate flexibility, the VHA will ensure a more competitive marketplace.

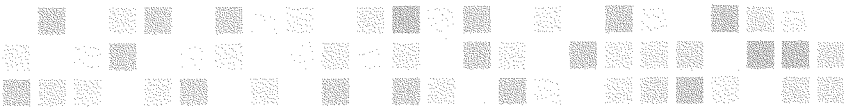
AATB is a professional, non-profit, scientific and educational organization. AATB was founded in 1976 by a group of doctors and scientists who had started in 1949 our nation's first tissue bank, the United States Navy Tissue Bank. It is the only national tissue banking organization in the United States, and its membership totals **more than 125 accredited tissue banks and approximately 850 individual members**. These banks recover tissue from more than **30,000 donors** and distribute in excess of **two million allografts for more than one million tissue transplants performed annually in the U.S.**

AATB strongly supports this legislation and urges the committee to favorably report it out of the subcommittee.

Please review AATB's full written testimony for additional information.

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

Legislative Hearing on H.R. 571, H.R. 593, H.R. 1015, H.R. 1016, H.R. 1017, H.R. 1128, and H.R. 1129



Statement of Daimon E. Geopfert

Principal and National Leader of Security and Privacy, McGladrey LLP

March 19, 2015

Background

Mr. Chairman and Members of the Committee, thank you for the opportunity to discuss the Department of Veterans' Affairs (VA) Office of Information and Technology's (OIT) management of its information security programs. My name is Daimon Geopfert, and I was asked to speak today as a veteran, as well as a security expert with experience in both the government and corporate worlds. I have 15 years of experience with the Department of Defense (DoD) including 12 years active duty Air Force, officer and enlisted, as well as three years as a defense contractor building Security Operations Centers (SOCs). While on active duty I was a communications specialist, an agent with the Air Force Office of Special Investigations (AFOSI), and an IT specialist within the Air Intelligence Agency.

Since leaving the DoD, I have spent the last eight years as a security consultant, initially with a "Big 4" firm and now as a principal with McGladrey LLP, serving corporations ranging from the Fortune Top 10 to the middle market, as well as federal, state, and local government entities. I have conducted hundreds of security assessments and breach responses in my career within networks of almost every size and composition. My specializations include ethical hacking, security monitoring, digital forensics, incident response, and malware analysis. Like many of my peers, I have also received a letter from the VA notifying me that the organization failed to protect my personal information.

Purpose

I am here today, quite simply, to make a call for accountability, and to draw attention to the continued need for the VA to resolve and strengthen their information security capabilities. Men and women in the armed services are held to account for almost every action they perform or fail to perform, and they expect the same mentality to apply to those people and entities that control critical aspects of their lives, such as their sensitive medical records or personal data. These veterans have a justifiable expectation that the VA will be held to account for its performance in the

same way that they would have been. However, all indications are that the VA has failed in this duty. What is most frustrating for veterans is that this is not a singular instance of failure, but rather a long-running, systemic version of failure of technologies, processes, and leadership. When veterans were in uniform, this level of non-compliance with their expected duties would not have been tolerated. Passing legislation such as "HR 1017 – The Veterans Information Security Improvement Act" would provide a detailed roadmap for the VA to follow in addressing these issues.

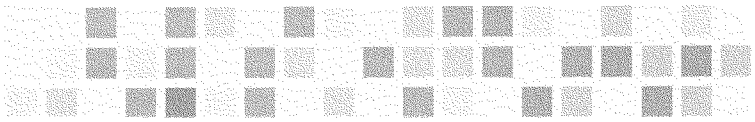
VA History

The VA has a widely reported history of non-compliance with regulations such as FISMA and HIPAA. Testimony by Mrs. Sondra McCauley, currently the Assistant Inspector General for Information Technology Audits at the Department of Homeland Security Office of Inspector General, before this Committee in November of 2014 stated that the VA has had 15 straight years of material weaknesses within its information systems controls with a total of 35 significant findings in the prior audit, five of which are unresolved from previous years. [1] It has been reported that, after the most recent audit, this timeline now spans 16 straight years of material weaknesses. These reports documented an extensive list of weaknesses and vulnerabilities within thousands of systems and applications, as well as within required core security processes and competencies.

The VA's own internal risk assessments state that a data breach of its primary VistA system is "practically unavoidable" and would result in exposure of "financial, medical, and personal Veteran and employee protected information" with "no way of tracking the source of the breach". [2] This risk was noted as being from the point of view of an average user, but it also applies to hackers or rogue users. A primary goal for any hacker gaining access to a target environment is to stop looking like a hacker. Hackers want to acquire valid credentials and fade into the background so that their activities look like those of an approved user; therefore, the moment they gain access to any user system these "unavoidable" vulnerabilities are now available to them.

Based on many of the VA's public comments, reports, and testimony, the focus of its efforts to protect VA systems seems to have been on managing attacks by foreign adversaries at a nation-state level. This is understandable because the VA network can be used as a stepping stone into other DoD environments using direct exploitation or "watering-hole" style attacks that have been utilized against high-tech and financial industries. However, while this focus on foreign adversaries is critical, almost any advanced skill or technology that is exclusively in the realm of nation-state level actors very quickly makes its way into the hands of criminal attackers focused only on monetary gain. In addition, as has been pointed out in numerous security research papers, there is ample evidence showing that nation-state level hackers often end up working on personal projects for their own gain. It is naïve to assume that these individuals would not utilize the skills, tools, and access granted to them during their day jobs to gather sensitive data for their own enrichment at a later time.

In a recent interview Stephen Warren, the VA's Executive in Charge and Chief Information Officer, stated that physical loss of data and user error were the VA's most significant risks, accounting for some 98 percent of known security incidents. [3] Some of the most significant findings for the recent VA audits center around the concepts that VA security procedures are lacking in auditing,



logging, and monitoring of the environment, making it highly likely that the VA would not have the capabilities to know that it has suffered a cyber-breach. [4] The OIG identified, and the VA stated in recent testimony, that its networks contain unknown and unmonitored systems and network connections, which would undo almost any effort to deploy effective monitoring. [1] In this same vein, CIO Warren stated that the VA has no evidence to show that data had been exfiltrated after a recent breach, but extensive reporting indicates that the VA would most likely not have the capability to prove, or even know, the truth of such statements. To support this point, it should be noted that CIO Warren later qualified his statements with a specific example of foreign infiltrators known to have extracted materials out of the VA environment, but because of the lack of logging by the VA and the use of encryption by the adversaries the contents of that data are unknown. Scenarios such as this allow the VA to continue to state that the organization is unaware of any theft of data by hackers, but it is likely a factor of the apparent lack of monitoring capabilities rather than the success of any prevention efforts.

Corporate Comparisons

These widely known and extensively reported issues would simply not be tolerated in the corporate world, largely because of the existence and enforcement of explicit legislation and industry standards. If examinations of a commercial organization produced results similar to those identified within the VA, the organization would be rated at the lowest levels of maturity for security governance, grossly out of compliance, and at a critical risk of suffering a breach. An organization in the private sector with this history would face substantial fines and penalties in addition to suffering reputational impact resulting from public scrutiny. There is little doubt that in the corporate world, the officers and directors of such an organization would face serious personal consequences.

It should be noted that the VA is understandably struggling with legacy systems, massive quantities of sensitive data, high levels of interconnections with other entities, and any number of technical and architectural issues. These are significant, often overwhelming issues; however the VAs corporate peers often operate under the same conditions and are expected to perform.

The Office for Civil Rights, the Health and Human Services (HHS) division responsible for enforcing the Health Insurance Portability and Accountability Act (HIPAA), has been levying fines of millions of dollars on companies for issues ranging from exposing the private health information of only a few hundred or thousand individuals to events that violated required controls but were not shown to have actually resulted in lost data. An investigation showed that the VA committed over 14,000 HIPAA violations over a three-year span, but that must be caveated because the same investigations showed that approximately only one out of every 365 violations was actually reported to OIG. [5] This likely makes the VA the largest HIPAA offender in the U.S., for which it has never been fully held to account. Would the FFIEC-OCC tolerate this from a bank? Would the SEC tolerate this from a broker dealer? Would State Attorneys General tolerate this from anyone under their purview without harsh civil or criminal repercussions? If the answer to those questions is "no," then the veteran community is reasonably curious as to why the VA is held to a different standard.

The VA is, for all practical purposes, exempt from many of the legal penalties that force its corporate peers into compliance, and the results of this situation are self-evident. HR 1017

provides the VA with governance mechanisms to address this issue. I understand that there is a competing Bill – HR 1128. However, on review it is clear that it provides high level requirements that will not provide the detailed instruction needed for VA to address its longstanding information security weaknesses. HR 1128 simply adds additional general requirements to the existing list of 'general' requirements. The trend within other industries is the shift from general to specific security and privacy guidance. The recent shift from the Payment Card Industry (PCI) 2.0 standard to the 3.0 standard is an example within retailers, and the SEC's OCIE cyber security initiative is an example within the broker dealer space. It is time to provide a clear and concise set of requirements to the VA in order to provide the appropriate guidance, structure, and oversight necessary to break this cycle of non-compliance.

Impact to Veterans

While most of the testimony to this point has been on the various issues with the VA environment, it cannot be forgotten that the true risk in this scenario is to the health and well-being of generations of veterans. The most obvious risk is identity theft, which results in enormous financial and mental stress. It goes without saying that introducing any type of additional stress into this population could be extraordinarily damaging. Many of the individuals that would be affected by a data breach within the VA are already at heightened risk because of a variety of injuries—both physical and mental.

By the VA's own estimation, 22 veterans a day take their own lives because of a complex set of physical, mental and financial conditions. While it might sound bombastic to tie identity theft to suicide, it is a fairly straightforward scenario. Many of the veterans interacting with the VA are already under immense pressure from transitioning to civilian life while dealing with a variety of mental and physical conditions, which often impacts their personal finances. For a veteran in this situation, waking up one morning to find out that someone has fraudulently opened a $50,000 home equity loan without his or her knowledge would be devastating.

Organizations like the VA will often state that it cannot be proved that data stolen from its environments led to identity theft, but this is a symptom of the nature of identity theft not a demonstration of a direct relationship. The repercussions of having personal data stolen might not materialize for years, and when an individual does become aware that something is wrong, it is essentially impossible to specify the source of the leak.

The VA often contains "full identities" of individuals: information such as a veteran's or dependent's name, address, Social Security Number, phone number, and other items that can be used to prove someone's identification. This type of data is the premier target for hackers. If someone steals your credit card number, it can be cancelled. If someone steals your identity, they can impact your financial safety for essentially the rest of your life.

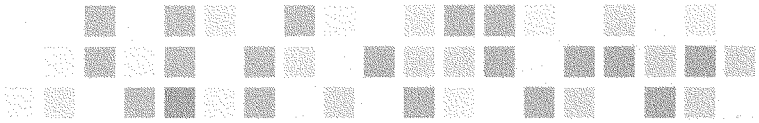
While this is the most obvious risk, it is not the exclusive one. What if beyond identity theft, some actor managed to perform a mass alteration or destruction of medical records out of sheer malice? Do you think this would be beyond the pale for various hacktivist groups or hacking crews that claim allegiance to various countries or terrorist groups? It could conceivably disable the entire VA infrastructure, interrupting services to millions of veterans. It would be a direct, highly visible strike against the U.S. veterans that fought them.

This is not an outlandish scenario. In fact, the capability to do this was demonstrated by the recent data manipulation scandal and the review of the affected systems. If such data alterations were available to standard users, they are available to attackers.

Conclusion

The men and women who have served our country, as well as their dependents, deserve and expect to have their welfare protected by organizations like the VA that play such a critical role in their lives. This legislation is sorely needed, and would be one of the first of its kind to provide such detailed, prescriptive guidance. The protection of the personal information of veterans should be a bipartisan issue, so our community hopes that this will be quickly passed and enforced. For more than a decade, the capability of the VA to protect the sensitive data of veterans has been in question with well-documented, significant, systemic, long-running failures. While legislation and standards already exist that provide high-level guidance on how this data should be protected, this history of non-compliance demonstrates conclusively that a new approach is necessary. Targeted, appropriate legislation is needed to force compliance and provide veterans and their families with the security they deserve. This legislation should explicitly require proper preventative, detective, and corrective controls, along with required reporting and oversight. The VA, and the bodies that oversee it, have an obligation to veterans to finally take decisive actions demonstrating their resolve to do the right thing.

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



Works Cited

[1] S. F. McCauley, "Testimony - VA'S LONGSTANDING INFORMATION SECURITY WEAKNESSES ARE INCREASING PATIENT WAIT TIMES AND ALLOWING EXTENSIVE DATA MANIPULATION," 2014.

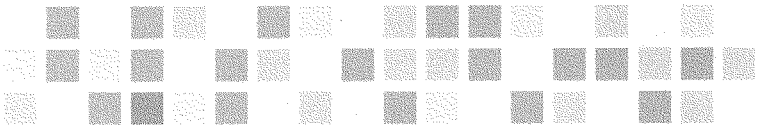
[2] "ERM-20130702.005R-OIS.001 - VistA Anonymous User Access," 7/2/2013.

[3] M. S. Warren, "VA's Longstanding Information Security Weaknesses Continue to Allow Extensive Data Manipulation," 2014.

[4] V. OIG, "Department of Veteran Affairs - 2013 FISMA Audit," 2013.

[5] C. Prine, "Privacy breaches in VA health records wound veterans," Pittsburgh Tribune-Review, 2013.

The views expressed herein are those of Mr. Geopfert, and are not necessarily those of McGladrey LLP.



McGladrey

Daimon E. Geopfert

National Leader, Security and Privacy Consulting
Technology Risk Advisory Services
McGladrey LLP
Chicago
daimon.geopfert@mcgladrey.com
312.634.4523

Summary of Experience

Daimon Geopfert is a Principal with the risk advisory services group at McGladrey LLP. He specializes in penetration testing, vulnerability and risk management, security monitoring, incident response, digital forensics and investigations, and compliance frameworks within heavily regulated industries. Daimon has over 20 years of experience in a wide array of information security disciplines. He serves as the firm's national leader for the security and privacy practice, responsible for the development of the firm's overall strategy related to security and privacy services and applicable methodologies, tool kits and engagement documentation.

Daimon is a regular presenter for organizations such as Information Systems Audit and Control Association (ISACA), InfraGard, the Certified Fraud Examiners and SC Magazine's World Congress. He has been quoted in a variety of publications, including The Wall Street Journal, Fortune Magazine, The Washington Post and the Kansas City Business Journal.

Representative Experience

- Information systems security assessment
  Daimon has served as the manager and lead technician for security assessments performed on some of the largest corporations and government entities in the world. He has designed and implemented testing frameworks and methodologies used to properly capture and communicate the technical, operational and regulatory impact of identified security weaknesses.

Daimon's experience in this area includes analyses and reviews of the following:

- Security testing across the enterprise: network, host, application and database
- Wireless, Voice over Internet protocol (VoIP), cellular, modem/telco assessment
- Security operations structure and effectiveness
- Social engineering testing, including phishing/pharming, phone and physical
- Corporate security policies and procedures
- Application secure architecture and coding analysis

- Incident response, forensics and security monitoring
  Daimon acts as the lead developer for McGladrey's forensic and monitoring service offerings, and has designed and deployed incident response and security monitoring programs within several highly regulated clients. These frameworks are based on customized versions of National Institute of Standards and Technology (NIST) SP800-81, ISO 18044:2004 and the SANS IR 6 Step. Daimon previously served as a special agent with the Air Force Office of Special Investigations – Computer Crimes Investigations, as a researcher with the CIA's Directorate of Science and Technology, and deployed and ran Security Operations Centers for the Department of Defense (DoD).

- Security program management
  Daimon has managed and performed a myriad of security program engagements across a variety of industries. The purpose of these projects was to assist organizations in deploying efficient, manageable and cost-effective solutions and processes that would address the wide ranging business and regulatory aspects of IT security. Daimon has deep experience in Payment Card Industry (PCI), HIPAA/Health Information Technology for Economic and Clinical Health (HITECH), FFIEC/Federal Deposit Insurance Corporation (FDIC), Federal Information Security Management Act (FISMA), NIST SP800 series, ISO 2700X, National Information Assurance Certification and Accreditation Process (NIACAP)/DoD Information Assurance Certification and Accreditation Process (DIACAP), American Electric Reliability Corporation(NERC)/Critical Infrastructure Protection (CIP), EU Data Privacy Directive, and various state security and privacy laws.

Professional Affiliations

- Information Systems and Controls Association (ISACA)
- International Information Systems Security Certification Consortium $(ISC)^2$
- FBI InfraGard, Michigan Chapter—Member, Presenter, Speaker Committee
- The SANS (SysAdmin, Audit, Networking, and Security) Institute
- The Ethical Hacker Network

Professional Certifications

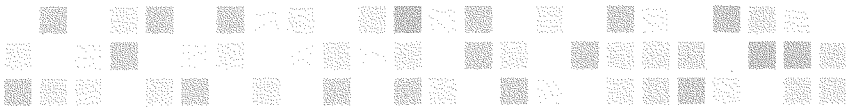
- Certified Information Systems Security Professional (CISSP)—$(ISC)^2$
- Certified Information Security Manager (CISM)—ISACA
- Certified Information Systems Auditor (CISA)—ISACA
- GIAC Certified Incident Handler (GCIH)—The SANS Institute
- GIAC Certified Reverse Engineer of Malware (GREM)—The SANS Institute
- Certified Ethical Hacker (CEH)— EC-Council

Education

- University of Michigan, Ann Arbor, Michigan, Master of Science in Computer Science
- United States Air Force Academy, Colorado Spring, Colorado, Bachelor of Science in Computer Science
- Numerous technical and industry courses and seminars

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

Legislative Hearing on H.R. 571, H.R. 593, H.R. 1015, H.R. 1016, H.R. 1017, H.R. 1128, and H.R. 1129



Statement of Daimon E. Geopfert

March 19, 2015

Summary

This testimony is meant to address the Department of Veterans' Affairs (VA) information security and privacy issues and the subsequent impact on veterans. Daimon Geopfert is a veteran of the United States Air Force, a former Department of Defense IT security contractor, and now serves as a security consultant within the public and private sectors. His testimony represents the feelings and expectations of veterans regarding the long-running challenges the VA has encountered in securing a wide variety of personal information, including known data breaches for unknown actors, years of documented audit failures, and thousands of vulnerable systems and applications. These reports stress that the VA's capabilities are immature, or lacking outright, in the expected areas of preventative, detective, and corrective controls. In comparison, similar systemic weaknesses in corporations of the same size and industry as the VA would not be tolerated. This situation results in an unacceptably high risk to veterans. These issues are already known to have exposed the data of millions of veterans, and they could arguably have exposed the information of millions more without the VA's knowledge due to limited capabilities to uncover such incidents. Such data breaches could lead to identity theft for vast numbers of veterans or even interruption of effective medical treatment. These are stressful events for anyone and especially for a population that is already under immense stress physically, mentally, emotionally, and often financially.

The men and women who have served our country, as well as their dependents, deserve and expect to have their welfare protected by organizations like the VA that play such a critical role in their lives. Targeted, appropriate legislation is needed to force compliance and provide veterans and their families with the security they deserve.

STATEMENT FOR THE RECORD BY
THE AMERICAN LEGION
BEFORE THE
OVERSIGHT AND INVESTIGATIONS SUBCOMMITTEE OF THE
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES
ON
PENDING LEGISLATION

MARCH 19, 2015

H.R. 571: The Veterans Affairs Retaliation Prevention Act of 2015

To amend title 38, United States Code, to improve the treatment of whistleblower complaints by the Secretary of Veterans Affairs, and for other purposes.

H.R. 1129: The Veterans Whistleblower and Patient Protection Act of 2015

To amend title 38, United States Code, to establish within the Department of Veterans Affairs an Office of Whistleblower and Patient Protection.

These bills would provide Department of Veterans Affairs (VA) whistleblowers with a means to solve problems at the lowest level possible, while offering them protection from reprisals and real accountability for those who reprise against them. It would establish a new system that employees could use to report retaliation claims, and supervisors would be required to report all retaliation claims to facility directors, eliminating the possibility for facility leaders to claim plausible deniability of such claims. The legislation would further codify prohibitions against negative personnel actions for employees who file whistleblower complaints or who cooperate with investigations by congressional, Government Accountability Office or authorities from the Office of the Inspector General, as well as establish mandatory disciplinary penalties for employees found to have engaged in retaliation against whistleblowers and create mandatory whistleblower protection training program for all VA employees.

In July of last year, The American Legion stated in testimony:

> When the problems of VA are viewed in total, several trends become clear. The guilty are not held accountable. Those who speak out against the system, be they employee or deeply concerned stakeholders, are vilified and shouted down. There is an institutional predilection against change and against responsibility.
>
> Whistleblowers will only be free from fears to come forward when they see consequences implemented against leaders who have harassed those who have already

spoken out. Acting Secretary Sloan Gibson has rightly stated that there is no place in VA for those who would harass whistleblowers.[1]

The American Legion supports the passage of these pieces of legislation.

H.R. 593: The Aurora Hospital Financing and Construction Reform Act of 2015

To extend the authorization for the construction of the Department of Veterans Affairs Medical Center in Aurora, Colorado, and to direct the Secretary of Veterans Affairs to enter into an agreement with the Army Corps of Engineers to manage such construction.

In April 2013, the Government Accountability Office (GAO) released a report on VA Construction: [2]*"Additional Actions Needed to Decrease Delays and Lower Costs of Major Medical Facility Projects"*. The purpose of the GAO report was to review the cost, schedule, and scope for new medical center projects, and for the VA to take actions for the purpose of improving their construction management practices and to improve their project management of projects. According to the report the Department of Veterans Affairs has been significantly over budget in all of the four major medical projects including: Las Vegas, Orlando, Denver, and New Orleans.

According to GAO, cost increases ranged from "59 percent to 144 percent representing a total cost of nearly $366 million per project with average schedule delays ranging from 14 to 74 months with an average delay of 35 months per VA major construction project."

In November 2013, the House Committee on Veterans' Affairs held a hearing examining the state of VA's major construction and lease programs and the VA's Office of Inspector General's Assistant Inspector General for Audits and Evaluations, Linda Halliday, claimed that reviews of VA's construction and leasing programs "have disclosed a pattern of poor oversight, ineffective planning and mismanagement of capital assets in VA."[3]

In April 2014, GAO released a follow-up report on VA Construction:[4]" *VA's Actions to Address Cost Increases and Schedule Delays at Denver and Other Major Medical Facility Projects*," in which GAO found that the costs associated with the VA medical center construction project in Denver have substantially increased, its schedule significantly delayed, and its scope modified.

In December 2014, construction on the Denver VA Medical Center was halted after Kiewit-Turner's workforce withdrew from the hospital work site when the U.S. Civilian Board of

---

[1] "Restoring the Trust: The View of the Acting Secretary and the Veterans Community" – July 23, 2014, House Committee on Veterans Affairs hearing

[2] *United States Government Accountability Office: April 2013 GAO-13-302 VA Construction: Additional actions Needed to Decrease Delays and Lower Costs of Major Medical-Facility Projects*

[3] Testimony of Linda Halliday, Assistant Inspector General for Audits and Evaluations, Office of the Inspector General – HVAC "Building VA's Future: Confronting Persistent Challenges in VA Major Construction and Lease Programs" November 20, 2013 http://veterans.house.gov/witness-testimony/ms-linda-halliday-2

[4] *United States Government Accountability Office: April 2014 GAO-14-548T VA Construction: VA's Actions to Address Cost Increases and Schedule Delays at Denver and Other Major Medical Facility Projects*

Contract Appeals (CBCA) ruled that VA breached its contract by failing to deliver a facility design that could be built for an approved budget of about $600 million.

On March 11, 2015, it has been reported that the Senate Veterans' Affairs Committee will visit the Denver VA Medical Facility in order to see, first-hand, the problems at the hospital, which is now "estimated to halt again around March 29 without Congressional approval for the appropriation of more funds.5

Dan Dellinger, Past National Commander of The American Legion, stated "*The failures in Florida, Louisiana, Colorado, and Nevada with major construction projects have made it clear that VA needs help. The Army Corps of Engineers has a proven track record of managing projects of this nature. Efforts to exhort the VA to pursue this path on their own have not proven successful. Maybe the VA should get out of the construction business, and do what they do best--take care of veterans.*"[6]

Ralph Bozella, Chairman of The American Legion's Veterans Affairs and Rehabilitation Commission testified that, *"The American Legion strongly believes there must be a serious look at how VA conducts their management of construction projects, and that the current state of affairs cannot be allowed to continue. With budgets drawn so tight in Washington, hundreds of millions of dollars of cost overruns on hospital projects hurt all veterans."*[7] During the hearing, The American Legion strongly urged VA to "clean up their own house, provide meaningful communication and transparency with the veterans' community, provide visible accountability for failures, and provide a clear roadmap to how the situation will improve."[8]

At The American Legion's Spring National Executive Committee, The American Legion passed a resolution that supported legislation and congressional oversight to improve future VA construction programs, as well as urged VA to consider all available options, both within the agency and externally, to include, but not limited to the Army Corps of Engineers, to ensure major construction programs are completed on time and within budget.

On January 21, 2015, The American Legion testified at a House Veterans Affairs Committee hearing regarding VA's construction issues and restated the resolution that calls on Congress and VA to "consider 'all available options' (including the Army Corps of Engineers) 'to ensure major construction programs are completed on time and within budget.'"9

The American Legion supports the passage of this legislation.

---

[5] "Senate Committee to Visit Aurora Hospital, Work Could Stop Again this Month" http://www.bizjournals.com/denver/blog/real_deals/2015/03/senate-veterans-affairs-committee-to-visit-aurora.html?page=all

[6] Joint Senate and House Veterans Affairs Committees hearing to receive the testimony of The American Legion, September 10, 2014

[7] "*Construction Conundrums: A Review of Continue Delays and Cost Overruns at the Replacement Aurora, Colorado VAMC.*" – House Committee on Veterans Affairs Subcommittee on Oversight and Investigation, April 22, 2014

[8] Ibid

[9] Testimony of Roscoe Butler, Deputy Director for Healthcare, The American Legion – HVAC "Building a Better VA: Assessing Ongoing Major Construction Management Problems Within the Department" January 21, 2015

H.R. 1015: The Protecting Business Opportunities for Veterans Act of 2015

To amend title 38, United States Code, to improve the oversight of contracts awarded by the Secretary of Veterans Affairs to small business concerns owned and controlled by veterans.

The American Legion believes that having small businesses certify to the VA that they comply with the relevant provisions of the Small Business Act is a good thing[10]. Holding small businesses accountable under the penalties of perjury would give the government the requisite authority to go after the bad actors in the small business community.

However, this is a measure that should be implemented agency-wide and not solely relegated to the veterans' small business community. The American Legion understands that HR 1015 would give existing legislation more teeth and give the courts more ammunition to go after the bad actors and we strongly support that aim, but we would also ask this Congress to consider expanding the legislation to hold all small businesses participating in government set-aside programs to this standard and not relegate this heightened threshold only to the veterans small business community. It would be wrong to think that only veteran owned small businesses were deserving of such scrutiny, and those businesses should not be unfairly thought of in that way.

The American Legion supports the passage of this legislation.

H.R. 1016: The Biological Implant Tracking and Veteran Safety Act of 2015

To amend title 38, United States Code, to direct the Secretary of Veterans Affairs to adopt and implement a standard identification protocol for use in the tracking and procurement of biological implants by the Department of Veterans Affairs, and for other purposes.

The American Legion previously raised concerns about the lack of a robust tracking system in the Veterans Health Administration (VHA). The Department of Veterans Affairs (VA) Office of the Inspector General (OIG) conducted an audit in 2012 and made recommendations regarding VA's management of their prosthetics supply inventory. In VHA's response, they indicated that they would work to develop a plan to replace the Prosthetic Inventory Package (PIP) and the Generic Inventory Package (GIP) with a more comprehensive system. The target completion date is March 30, 2015. In the interim, VHA indicated they were working on a VA OI&T patch (VistA Prosthetics patch 101), which was 95 percent completed.

While reaching this goal by 2015 is indeed laudable, 2015 is rapidly becoming a critical year for VA to meet strategic goals including the elimination of veteran homelessness and the disability claims backlog. The American Legion would like to see a more detailed timeline implementing these changes and improvements for veterans. Reports through System Worth Saving Task Force visits and contact with VHA employees indicate responsibility for entering serial numbers of implant devices is manual, not automated, and is inconsistently implemented.

---

[10] Resolution No. 349: "Support Verification Improvements for Veterans' Business within the Department of Veterans Affairs and Department of Defense" AUG 2014

Although VHA claims to work to a standard of "removing recalled products from inventory within 24 hours of a recall", there is still no clear policy on how veterans who have already received implants are tracked. It is not enough to cut off the problem at the source, attention must be paid to veterans who are already downstream in the process. Without consistent tracking of implants, including positive identification by serial number and other identifying factors, uncertainty remains as to how veterans are served in the case of recalls. The American Legion noted we would like to see a more comprehensive procedure and policy clearly delineated by Central Office to ensure consistency in all Veterans Integrated Service Networks (VISNs).

The analysis of the current inadequacy of the tracking system for bio-implants derives directly from The American Legion's System Worth Saving Task Force reports. The System Worth Saving Task Force was established to examine the State of VA Medical Facilities by resolution in 2004 . This annual report, provided to members of Congress and the veterans' community is a vital resource as the primary third party analysis of the quality of VA facilities.

The American Legion supports the passage of this legislation.

H.R. 1017: The Veterans Information Security Improvement Act

To improve the information security of the Department of Veterans Affairs by directing the Secretary of Veterans Affairs to carry out certain actions to improve the transparency and the governance of the information security program of the Department, and for other purposes.

H.R. 1128: The Department of Veterans Affairs Cyber Security Protection Act

To amend title 38, United States Code, to make certain improvements in the information security of the Department of Veterans Affairs, and for other purposes.

While protecting the information security of veterans' information on VA systems is important, The American Legion does not have a specific position or resolution on the best way to go about providing Information Technology security.

The American Legion has no position on these pieces of legislation.