CYBERSECURITY CHALLENGES AND CYBER RISK MANAGEMENT AT THE DEPARTMENT OF VETERANS AFFAIRS

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION

OF THE

COMMITTEE ON VETERANS' AFFAIRS

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

THURSDAY, NOVEMBER 14, 2019

Serial No. 116–45

Printed for the use of the Committee on Veterans' Affairs

Available via http://govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE

41–375 WASHINGTON : 2022

COMMITTEE ON VETERANS' AFFAIRS

MARK TAKANO, California, *Chairman*

JULIA BROWNLEY, California
KATHLEEN M. RICE, New York
CONOR LAMB, Pennsylvania, *Vice-Chairman*
MIKE LEVIN, California
MAX ROSE, New York
CHRIS PAPPAS, New Hampshire
ELAINE G. LURIA, Virginia
SUSIE LEE, Nevada
JOE CUNNINGHAM, South Carolina
GILBERT RAY CISNEROS, JR., California
COLLIN C. PETERSON, Minnesota
GREGORIO KILILI CAMACHO SABLAN, Northern Mariana Islands
COLIN Z. ALLRED, Texas
LAUREN UNDERWOOD, Illinois
ANTHONY BRINDISI, New York

DAVID P. ROE, Tennessee, *Ranking Member*
GUS M. BILIRAKIS, Florida
AUMUA AMATA COLEMAN RADEWAGEN, American Samoa
MIKE BOST, Illinois
NEAL P. DUNN, Florida
JACK BERGMAN, Michigan
JIM BANKS, Indiana
ANDY BARR, Kentucky
DANIEL MEUSER, Pennsylvania
STEVE WATKINS, Kansas
CHIP ROY, Texas
W. GREGORY STEUBE, Florida

RAY KELLEY, *Democratic Staff Director*
JON TOWERS, *Republican Staff Director*

SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION

SUSIE LEE, Nevada, *Chairwoman*

JULIA BROWNLEY, California
CONOR LAMB, Pennsylvania
JOE CUNNINGHAM, South Carolina

JIM BANKS, Indiana, *Ranking Member*
STEVE WATKINS, Kansas
CHIP ROY, Texas

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.

C O N T E N T S

THURSDAY, NOVEMBER 14, 2019

CYBERSECURITY CHALLENGES AND CYBER RISK MANAGEMENT AT THE DEPARTMENT OF VETERANS AFFAIRS

THURSDAY, NOVEMBER 14, 2019

U. S. HOUSE OF REPRESENTATIVES
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
COMMITTEE ON VETERANS' AFFAIRS
Washington, DC.

The subcommittee met, pursuant to notice, at 10:01 a.m., in room 210, House Visitors Center, Hon. Susie Lee [chairwoman of the subcommittee] presiding.

Present: Representatives Lee, Lamb, Cunningham, Banks, Watkins, and Roy.

OPENING STATEMENT OF SUSIE LEE, CHAIRWOMAN

Ms. LEE. Good morning. This hearing will now come to order. On behalf of Ranking Member Banks and myself and the subcommittee, thank you all for being here.

In searching this committee's history, we could not find any evidence that there has been a broad oversight hearing examining cybersecurity management challenges at the Department of Veterans Affairs. The Subcommittee on Technology Modernization is going to chart a new course today.

Cybersecurity is not a new challenge in the Federal Government. Each year, the Offices of Inspector General are mandated to audit compliance with the Federal cybersecurity framework that has been established to protect information, programs, and assets from threats. Those threats have become more complex and the potential for harm has only increased since the Federal Information Security Management Act, FISMA, was passed in 2002.

In the intervening years, we have also seen how big a target the health care sector has become for bad actors. Throughout the world, health care institutions have been breached and extorted, and data have been held hostage or stolen. Government health care institutions have not been immune from this either. Britain's national health service was a victim of one of the largest ransomware attacks in history. Almost daily, there are news reports or notifications by hospitals, insurance companies, and other entities that there has been a breach and that data may have been compromised. These attacks and breaches cost millions, and impact the health care and benefits delivery. They also cause Americans to lost trust in institutions' ability to protect some of the most sensitive there is.

At the same time, the reliance on electronic personal data, the electronic sharing of that data, and the modernization of systems to support health benefits and public service delivery is growing. As this reliance on technology increases, so does the risk. Therefore, it only makes that one of our country's largest providers of health care and benefits should be at the forefront of addressing these risks.

VA is in the process of modernizing numerous systems to adjudicate disability claims, provide educational benefits, and deliver health care. Information security management should be a key component of those efforts from the outset. However, my concern is that assessing risk and developing mitigation strategies does not have enough attention. Many Office of Inspector General (OIG) and Government Accountability Office (GAO) reports on security incidents cite management failures or lack of internal oversight as a reason behind the incidents. Too often, strong leadership on risk management and information security becomes an afterthought or a paperwork exercise done once a year for the Federal Information Security Modernization Act (FISMA) audit. Even worse, it only becomes an issue after the system has been compromised and sensitive data is put at risk.

Cybersecurity is a challenging and complex issue, and it requires an ever-changing response. The key is that the response needs to be a whole-of-government or a whole-of-agency effort. Every component of an agency needs to be involved, from the front-line staff employing good cyber hygiene, to acquisition professionals assessing the risk in the supply chain, to Information Technology (IT) professionals assessing the risks of new and legacy technology, and to leadership engaging in strategic assessments to understand the challenges and developing the plans to meet them.

The purpose of today's hearing is to hear from VA leadership about cybersecurity landscape, the challenges in the approach to risk management. We will hear from the Office of Inspector General about how the VA has faired in cyber risk management over the last several years and the outstanding concerns. We will also hear from the Government Accountability Office about responding to cybersecurity challenges and best practices for risk management.

I would like this hearing to serve as a foundation for other cybersecurity-related oversight that the subcommittee will engage in over the next year. The better we understand the challenges and the risks, the better we are able to assess whether we are making progress and what more needs to be done.

The protection of VA technology and data is not a hypothetical issue or something that occurs in a vacuum. These systems and data serve to support the care and the benefits our veterans have earned. I have heard from veterans loud and clear about privacy and data security concerns, and those concerns only become more amplified as more systems become electronic. We do not want to hold up progress that the VA is making on technology modernization—as we all know, it is sorely needed—but we do need to be mindful of the risks that we are taking as VA moves ahead.

Further, as we encourage veterans to use VA resources and, most especially, to find the support and care for the wounds, both visible and hidden, VA must show that it is secure; it can be trusted; and

that it has the tools, policies, and the leadership to protect veterans' health data and personal information. This is all a part of a sacred obligation we have made to those who have served our country.

I thank all the witnesses for being here today and I look forward to your testimony.

With that, I would now like to recognize my colleague Ranking Member Banks for 5 minutes to deliver any opening remarks he may have.

Mr. Banks.

OPENING STATEMENT OF JIM BANKS, RANKING MEMBER

Mr. BANKS. Thank you, Madam Chair.

There was a time when cyber attacks primarily threatened national security agencies and financial institutions; that time has long passed. Today, state-directed cyber attacks, cyber espionage, and cyber crimes are nearly daily occurrences, and they threaten every government agency and industry.

Cybersecurity has been a consistent priority across administrations throughout successive Congresses, and I am encouraged that cybersecurity policy is increasingly sound. However, implementation among Federal agencies seems to be continually uneven and fragmented, and the Federal Government still often struggles to defend itself.

Many of the technology modernization issues that we often discuss in other contexts also have major cybersecurity impacts. Legacy systems carry vulnerabilities, and scarce resources must be allocated to replacing them or hardening them. Competition for cybersecurity talent is fierce everywhere, but a one-size-fits-all personnel system hampers the Federal Government.

The VA must approach cybersecurity risk management not only as a government agency, but also as a health care system. The health care sector recognized the cybersecurity imperative somewhat later than other industries. The first major cyber attack on a hospital system was not until 2014 when Chinese hackers stole 4.5 million patients' non-medical data from Community Health Systems, Incorporated. It became apparent that many health care organizations had not sufficiently recognized or prioritized cyber threats, and they began to play catchup in their cybersecurity investments.

Health care faces an inherent challenge. Modern patient-centered care and evidence-based medicine require the real-time exchange of huge volumes of sensitive personal data. Patients demand this, but they also expect peace of mind that their data will not be mishandled or stolen.

The health care sector also contends with the increasing complexity and connectedness of medical devices. Medical devices were not always thought of as targets, but the Food and Drug Administration (FDA) and manufacturers have recognized that their cyber vulnerabilities are similar to those of industrial control systems.

Overall, VA's cybersecurity posture seems to be mixed. The Federal Information Security Modernization Act requires annual audits of each agency's cybersecurity practices. VA has been carrying a high number of unresolved recommendations for years, but this

is slowly trending in the right direction. Some of the weaknesses are also documented in the OIG's annual financial audits and they are unresolvable until VA replaces several outdated financial IT systems.

I am encouraged that Office of Information and Technology (OIT) has prioritized hiring cybersecurity talent and I am eager to see them demonstrate real progress in recruiting and retaining these personnel. I believe Veterans Health Administration (VHA) and OIT have only begun to seriously tackle the issue of vulnerabilities in medical devices. Thousands of these devices are running outdated operating systems and some are so obsolete that it is not even possible to update the software. This issue cannot be allowed to fall into a bureaucratic impasse. On the other hand, VA has demonstrated real leadership in developing its Technical Reference Model, which is a data base of IT equipment and software that is approved for use. This is a good step toward ensuring that VA is buying technologies that are safe.

Finally, I would like to address the issue of cybersecurity in the technology supply chain. Hackers can be virtually anyone, but when we talk about corrupting the supply chain, we are almost talking about China.

China is embedded in every aspect of the IT and communications equipment supply chain, and none of our other strategic adversaries come even close. China is the largest exporter of technology hardware globally, as well as a growing player in the mobile app marketplace, and nearly every U.S. hardware manufacturer's products contain multiple Chinese-made components. It is a frightening reality that some foreign companies are pre-loading malicious software into their products.

Healthcare Information and Management Systems Society (HIMSS) found in their 2019 cybersecurity survey that malware in commercial products accounted for 8 percent of significant cybersecurity incidents in health care systems.

It has been the U.S. Government's policy since the 1990's to buy commercial, off-the-shelf technology whenever possible, and this has been an overwhelming success in most respects. However, while Federal agencies tend to view themselves as independent entities, our cyber adversaries, especially State actors, see them as one big, interconnected target. Our adversaries coordinate all of their governmental, military, and corporate resources to hack our networks and compromise our supply chains, but we do nothing of the sort to defend ourselves; this has to change. We have to go far beyond a whole-of-government approach to cybersecurity.

I thank our witnesses for being here today. I look forward to discussing these issues.

With that, Madam Chair, I yield back.

Ms. LEE. Thank you, Mr. Banks.

I will now introduce the witnesses we have before the subcommittee today. Mr. Paul Cunningham is Deputy Assistant Secretary and Chief Information Security Officer for the Department of Veterans Affairs. Mr. Cunningham is also a Navy veteran.

Mr. Cunningham is accompanied by Mr. Gary Stevens, Deputy Chief Information Security Officer and Executive Director for Information Security Policy and Strategy. Mr. Andrew Centineo is Exec-

utive Director, Procurement and Logistics, Veterans Health Administration, and also an Army veteran. Thank you. Ms. Luwanda Jones, Deputy Chief Information Officer, Strategic Sourcing, in the Office of Information and Technology.

Mr. Nick Dahl, Deputy Assistant Inspector General for Audits and Evaluations, VA Office of Inspector General, who is accompanied by Mr. Michael Bowman, Director of Information Technology and Security Audits Division at the Office of Inspector General, and Mr. Gregory Wilshusen, Director of Information and Cybersecurity Team at the General Accountability Office.

We will now hear the prepared statements from our panel members. Your written statements in full will be included in the hearing record, without objection.

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

STATEMENT OF PAUL CUNNINGHAM

Mr. CUNNINGHAM. Good morning, Madam Chair Lee, Ranking Member Banks, and the distinguished members of the subcommittee. Thank you for the opportunity to speak about the Department of Veterans Affairs' cybersecurity strategy and its mission to protect the sensitive data of veterans and VA employees.

I am Paul Cunningham, VA's Chief Information Security Officer. I am here with Mr. Gary Stevens, VA's Deputy CISO; Mr. Andrew Centineo, the Executive Director of Procurement and Logistics under VHA; and Ms. Luwanda Jones, Deputy Chief Information Officer for Strategic Sourcing.

I want to begin by thanking Congress and the subcommittee for your continued support and shared commitment to the success of VA's efforts in delivery secure and effective services to our Nation's veterans. As a Navy veteran myself, I have seen firsthand the value and the real impact the VA has on the lives of so many of our veterans. As chief security professional, I understand the value that technology brings and how VA's mission is supported. I am also aware of the treasure trove of information that VA protects and the lengths our adversaries will go to gain access.

Secretary Robert Wilkie has committed VA to leveraging new technologies and best approaches to streamline the Department's services to our vets. However, new technologies and advancements bring additional risk to information systems, data management systems, and privacy.

In accordance with Federal Information Security Modernization Act of 2014, the Secretary has delegated the balancing of IT operations and cybersecurity to the Chief Information Officer, Assistant Secretary Jim Gfrerer. Likewise, the CIO has designated me as the Chief Information Security Officer to administer the cybersecurity program on behalf of the VA.

The Office of Information Security is charged to develop, implement, and maintain the VA's cybersecurity program and the risk strategy. The cybersecurity program deploys a centralized risk strategy that proactively aligns efforts with the National Institute of Standards and Technology, meets Federal requirements, and responds to today's threats while promoting VA's mission. Office of Information Security (OIS) administers the program through a holistic and robust set of strategies and policies that leverage direc-

tives, assessments, and proactive monitoring. OIS defines policies in handbooks that outline the roles and responsibilities of stakeholders, and defines the framework for implementation.

Based on the OIS guidance, system owners are required to develop security plans that define the purpose of their systems, identify the security requirements, and catalogs the appropriate controls based on the security level of those systems. OIS uses those security plans in our ongoing assessments to ensure sites and systems meet established standards are effective in safeguarding information. System owners and authorizing officials use assessment results and other security-related information in their determination if a system should have or should maintain access to VA's network and assessments.

OIS oversees a dedicated cybersecurity operational center that monitors and responds to malicious network activities. This talented team serves as VA's cybersecurity instant-response hub, and coordinates with the Department of Homeland Security in accordance with Federal requirements.

Any gap or vulnerability identified by OIS through assessments and monitoring are managed through an active plan of action and milestone, or Plan of Actions and Milestones) POA&M tracking system. The POA&Ms ensure remediation efforts are completed, assists in setting cybersecurity priorities, and provides analysis for policy and reporting.

However, VA's cybersecurity program is more than one cybersecurity office; it relies on all elements of the organization to establish local procedures to ensure policies, protocols, and agreements are followed properly. This includes limiting access to sensitive information, developing protocols for procuring third party vendors, and using technical assets in a secure manner. As we say in the Navy, it is an all-hands effort.

We do face challenges. New technologies, third party partnerships, and advancement in operational technology introduce new security risks, not just at VA, but across the Federal Government and private industry. VA understands the need to address the growing challenges in security while improving access and services to veterans. We are working closely with our Federal and our commercial partners to improve our ability to manage risk and maintain compliance with Federal mandates. We are confident that are cybersecurity program is positioned to proactively support VA's mission.

Madam Chair, Ranking Member, and members of the subcommittee, thank you again for this opportunity, and we are happy to answer any questions you may have.

[THE PREPARED STATEMENT OF PAUL CUNNINGHAM APPEARS IN THE APPENDIX]

Ms. LEE. Thank you, Mr. Cunningham.

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

STATEMENT OF NICK DAHL

Mr. DAHL. Madam Chair, Ranking Member Banks, and members of the subcommittee, thank you for the opportunity to discuss the Office of Inspector General's oversight of VA's Information Technology Security Program. My statement focuses on the security pro-

gram's purpose and the challenges in protecting the confidentiality, integrity, and availability of VA's systems and data.

IT systems and networks are critical to VA for carrying out its mission of providing medical care and a range of benefits and services to millions of veterans and their families. VA is responsible for storing, managing, and providing secure access to enormous amounts of sensitive data, including veterans' medical records, benefits determinations, financial disclosures, and education records. The OIG recognizes and appreciates that this is a complex undertaking.

To the extent that VA does not properly manage and secure their IT investments, they can become increasingly vulnerable to misuse and mishaps. Lack of proper safeguards renders these systems and networks vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other VA systems. Security failures also undermine the trust veterans put in VA to protect their sensitive information, which can affect their engagement with programs and services.

The Federal Information Security Management Act of 2002, known as FISMA, required that agencies develop, document, and implement an organization-wide security program for their systems and data. This act was amended in 2014 and became the Federal Information Security Modernization Act.

Annually, the OIG reports on the extent to which VA has IT safeguards in place consistent with FISMA requirements. Our most recent FISMA audit revealed that VA has made progress developing and distributing policies and procedures as part of its security program. However, VA continues to face significant challenges in complying with FISMA requirements, due in part to maintaining an aging and outdated IT security infrastructure. Our report contained multiple findings and 28 recommendations for improving VA's Information Security Program. Most of these recommendations are repeated from previous FISMA audits, as VA has yet to adequately address them.

Our findings and recommendations focused on the following areas: configuration management controls, which are designed to ensure critical systems have appropriate security controls and to ensure up-to-date vulnerability patches are implemented. In our vulnerability testing, we have found that critical security patches have not been consistently installed for various VA systems.

Identity management and access controls, which are meant to make certain that password standards are consistently implemented and to ensure user's access privileges are limited to only legitimate purposes. The OIG has seen many examples of default user names and passwords, or the use of easily guessed passwords, that provide increased opportunities for malicious users to gain unauthorized access to critical VA systems.

The agency-wide Security Management Program, which is intended to make sure that system security controls are effectively implemented and continuously monitored. This program is also designed to ensure that system security risks are effectively remediated through corrective action plans. VA has developed numerous plans of action and milestones to address identified system security risks; however, we continue to identify plans for which there is in-

adequate evidence of effective action to justify the closure of such plans.

Overall, the OIG's FISMA audit, in addition to a range of other reports on VA's IT security program, show that VA has considerable work to do in order to achieve better IT security outcomes.

VA's fundamental mission of providing benefits and services to veterans is dependent on deploying secure IT systems and networks. Until proven processes are in place to ensure adequate controls across the enterprise, VA's mission-critical systems and sensitive veterans' data will remain at risk. While VA has made recent improvements in some aspects of information management, there continue to be considerable challenges. We believe that VA's successful implementation of open recommendations from oversight reports is an important step in its efforts to address cybersecurity and risk management concerns.

Madam Chair, this concludes my statement. Mr. Bowman and I would be happy to answer any questions you or other members of the committee have.

[THE PREPARED STATEMENT OF NICK DAHL APPEARS IN THE APPENDIX]

Ms. LEE. Thank you, Mr. Dahl.

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

STATEMENT OF GREG WILSHUSEN

Mr. WILSHUSEN. Chair Lee, Ranking Member Banks, and members of the subcommittee, thank you for the opportunity to testify at today's hearing.

In providing health care and other benefits to veterans and their dependents, VA relies extensively on IT systems to receive, process, and store sensitive data, including veterans' medical records and other personally identifiable information. Accordingly, effective security controls are essential to ensure that VA's systems and information are protected from loss, misuse, unauthorized disclosure or modification, and are available when needed.

Today, as agreed, I will provide an overview of the status of information security across the Federal Government in general and at VA in particular. I will also discuss security challenges that VA faces as it modernizes and secures its systems. Before I do, if I may, I would like to recognize members of my team who were instrumental in developing my statement and the work underpinning it.

With me today are Assistant Director Jeff Knot and Analyst-in-Charge DiMond Spencer. Also contributing were Chris Businsky, Nancy Glover, Franklin Jackson, Daniel Swartz, Melina Asencio, Scott Pettis, and Zsaroq Powe. Thank you.

Chair Lee, Ranking Member Banks, Federal agencies, including VA, continue to have deficient information security programs. FISMA requires IGs to determine the effectiveness of their agency's security program. To do this, IGs use the five-level maturity model to assess the implementation of five core security functions defined by the National Institute of Standards and Technology (NIST) cybersecurity framework. Of the 24 Chief Fianacial Officer (CFO) Act agencies, VA was one of 18 agencies where the IG determined that

the agency-wide information security program was not effectively implemented during Fiscal Year 2018.

Additionally, most CFO Act agencies, including VA, had deficiencies in most general control categories for their financial systems in Fiscal Year 2018. For example, VA's IG reported weaknesses in security management, access control, configuration management, and contingency planning.

Auditors at 12 agencies designated information security as a significant deficiency in internal control over financial reporting for their agency, while IGs at VA and five other agencies designated the deficiencies as a material weakness, the most severe kind. Fiscal year 2018 was the 17th year in a row that VA had reported a material weakness in information security.

As VA secures and modernizes its information systems, it faces several key security challenges. These challenges pertain to implementing security controls over its information and information systems; mitigating known vulnerabilities in a timely and effective manner; establishing elements of a cybersecurity risk management program to identify, prioritize, and manage cyber risks; and categorizing the work roles of its IT and cyber-related workforce positions, a key step in identifying critical cybersecurity staffing needs.

Like other Federal agencies modernizing their IT systems, VA faces an additional challenge of managing IT supply chain risks. If unchecked and exploited, these risks could hamper VA's ability to serve our veterans.

In summary, similar to other Federal agencies, VA continues to be challenged in implementing an effective agency-wide program and controls for securing its information and information systems. As VA pursues efforts to modernize and secure its IT systems, it will need to successfully address multiple challenges in order to achieve effective outcomes.

Chair Lee, Ranking Member Banks, this concludes my written statement. I would be happy to answer your questions.

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

Ms. LEE. Thank you. I will now recognize myself for 5 minutes for questions, and I would like to start with you, Mr. Cunningham.

You have a rich history and career in the Federal information security space, including with the Department of Energy. When you arrived at the VA in January 2019, what if any observations did you make about where the VA stands with regards to its progress in adopting good practices and prioritizing cybersecurity?

Mr. CUNNINGHAM. Thank you, and thank you for the comments earlier about understanding the challenges that VA has in this area, as well as across the Federal Government.

It is true, risk and risk management and cybersecurity is a challenge in a lot of Federal agencies and how they approach it, obviously, we use NIST as our reference guide manuals; the risk publications under 1839 and 37 describe how to implement a cybersecurity program. What I have noticed when I arrived at VA was that we have an incredibly talented pool of people, especially in regards to how we monitor the network traffic and our ability to respond. I also saw a very strong relationship with Department of Homeland

Security (DHS), which was a very positive thing and where we could partner.

I did notice that there was some siloing or what I looked to see like remains of silos that may have been in the past, but I quickly realized that working with operations there was an open door, which a lot of times in Federal agencies there might be some conflicts between operations and cybersecurity, but that was not in place at VA, which was very reassuring. Also VA's approach to centralize cybersecurity, which is a little bit different than I have seen in other agencies, but promoted by NIST as well was a welcome change.

There are still some legacy issues that I have noted, especially around the FISMA reports in Fiscal Year 2018, or some of the AI findings from IG, but I also saw some really clever ideas that were being put in place to promote greater awareness through the senior leadership. For instance, they developed an Office of Quality Process and Risk, and they established a Risk Officer, which was an incredible feat, because a lot of organizations have difficulty getting the office set up and being staffed. That was remarkable and it is a great ally for cybersecurity as a whole to be able to have somebody that is equal pairing and unbiased feeding to the Chief Information Officer (CIO) and the Secretary information regarding cybersecurity risk.

I also saw—we also started looking at realignment to kind of the core values that we really look at, especially around FISMA 2014. We started looking at the pure NIST regulations and where those pockets and pools of money and activities are being placed. Then we also have a governance structure that is not siloed for cybersecurity, but I actually have an opportunity every week to talk with my peers both in operations and H.R. and Strategic Sourcing that talk about what issues I have, as well as listen to what issues they have, where we can be of better service to veterans.

Probably the most important part I noticed was the commitment from the CIO, as well as the Secretary and Deputy Secretary. They understand cybersecurity and they are a great ally.

Ms. LEE. Thank you. It sounds like you are making some progress, especially within the management level at the VA. Are there any program office changes that you are planning to make to ensure proper-level management for cybersecurity?

Mr. CUNNINGHAM. At this time, I think we have a three-level structure in the Office of Information Security, that gives us the ability to, one, be proactive in building strategy and policy, at the same time running operations and instant response. Any changes in there are pretty much cosmetic, because the activities will pretty much remain the same, maybe sequential amounts where we have better management and visibility of it.

With that, I do not see any other changes that I need at this time. Certainly, how we integrate with operations is effective. With that, I think we are good.

Ms. LEE. Thank you.

I am now yielding to Ranking Member Banks.

Mr. BANKS. Thank you, Madam Chair.

Mr. Wilshusen, the Federal cybersecurity policy seems to be increasingly well developed, but its implementation seems to be as

disjointed as ever. We are here today to talk about VA, but how should VA fit into a whole-of-government approach to cybersecurity?

Mr. WILSHUSEN. Well, I would certainly agree with you that policies and procedures that are being developed for Federal agencies are getting better, becoming more comprehensive, and you are absolutely correct in that the implementation and execution of those policies and procedures has been inconsistent across Federal agencies and I think that is something that will continue to occur. We will certainly keep looking at that as we conduct our government-wide work. But I think VA, certainly in its role as protecting the systems at that department, has some areas for improvement.

As the IG has consistently reported over the last several years, there are a number of particular areas where that department needs improvement, to include access controls, which are intended to help detect and limit access to agency systems, as well as assuring the proper management and configurations of its systems and the like. Indeed, VA certainly has a key role in approving the security over its systems and the networks that it operates and uses.

Mr. BANKS. All right. Mr. Cunningham, how does VA fit into a whole-of-government approach to cybersecurity?

Mr. CUNNINGHAM. I think we have—well, we have done a lot in the last 10 months I have been there. We have been working closely with the cyber—I am sorry, the Chief Information Security Officer (CISO) Council, the Federal CISO Council under Office of Management and Budget (OMB). We also look for partnering opportunities. For instance, we work with the Department of Energy, we have several activities that are out through one of their national labs, and in there we are partnering with the cybersecurity team to ensure that it is not just a drop-and-go, but a partnership.

Then we are also working with our internal and external partners around medical devices, and how we can be a better partner in establishing regulations and requirements.

Mr. BANKS. Okay. How much do we know about the threat actors targeting the VA? How many of them are nation State actors, as opposed to cyber criminals, and how many of them are foreign versus domestic?

Mr. CUNNINGHAM. While the Department does not have a dedicated intelligence community element, like some agencies do, and however we do have classified access to information and we share that information with—or we get shared information from DHS, as well as the intelligence community through high-side communications.

We do have active state-sponsored threat actors that are trying to get in, we recognize those where we can. A lot of times when we see an attack or we see some sort of attempt, we do not spend a lot of time doing attribution as much as blocking, because we leave that to DHS and the intelligence community.

Mr. BANKS. All right. Department of Defense (DOD) has what is called the Unified Capabilities Approved Product List and VA has its Technical Reference Model (TRM). They both contain lists of IT and communications equipment that is approved for purchase and believed to be free of malware and back doors. How is the TRM developed?

Mr. CUNNINGHAM. The TRM, I do not have the exact process, I believe it is worked through a group, but I will actually pass that to Ms. Jones.

Ms. JONES. Thank you, sir.

The TRM, we have a dedicated team in OI&T who assess the products that are being placed on the—in the TRM. We will be more than happy to at a later date come back and bring the appropriate people to do a deep dive into the products that are on that list, how we assess the products.

Mr. BANKS. Okay, that would be great.

The DOD OIG has discovered instances of items on the approved product list containing vulnerabilities, what is your level of confidence that the TRM does not contain compromised items?

Ms. JONES. Again, sir, we will bring the appropriate folks to answer that question, because I just do not want to just say something off the cuff. We will bring you that.

Mr. BANKS. Maybe not confident enough. I have many more questions, but my time has expired.

Ms. LEE. Thank you. I now recognize Mr. Roy for 5 minutes.

Mr. ROY. Thank you, Madam Chair. I apologize for being a few minutes late. We were down on the floor of the House of Representatives. As you know, we have to multi-task around here some, but I appreciate you all being here and I appreciate you all taking the time to address these important topics.

Mr. Cunningham, a question for you, if you do not mind. I am sure you are aware of the emerging Internet of Things, which is the interconnection of devices, machines, and objects equipped with network connectivity. The research firm Gardner predicts that by next year Internet of Things technology will be at 90 percent, as you know, I suspect, of new computer-enabled product designs, and it poses a significant cybersecurity challenge for VA as it procures and attempts to secure these devices.

A question for you is, do you believe that the VA is prepared for this new security challenge, and how do you intend to mitigate the new risk that the Internet of Things introduces.

Mr. CUNNINGHAM. It is a greater challenge, the Internet of Things. We can call them Supervisory Control and Data Acquisition (SCADA), we can call them—I call them operational technology, whether it is under medical or power, other sources. How they work and how they communicate with the cloud is very challenging from a cybersecurity perspective, but one of the things we do here at the Department is make sure that anything plugged in is protected, we also do that with our wireless communications.

Before anything can connect to our internal network or business networks, those have to go through a vetting process through procurement. They are also then identified and then mainly loaded into our network to be able to communicate.

Things that someone might bring in around a Fitbit watch or other Internet of Things (IOT)-purchased items, consumer-purchased items, will not be able to get into the dedicated networks. We do have guest networks that are monitored, but they are also architectured off, so they do not have access. They actually have to go out and come back in as if they were from home, so they are not a bigger threat.

Mr. ROY. Well, in that same vein, VA is attempting a multitude of systems modernization, we know that, across various platforms, while contending with a lot of the bureaucratic constraints that go along with that. The technology industry is obviously moving at breakneck speed, you know, I have got an iPhone in my pocket that 10 years ago, you know, was pretty much brand new. How are you all keeping your cybersecurity posture current in light of that and, you know, the issue you were just addressing before, is there—do you guys have like a sort of task force that focuses on this stuff and how to stay ahead of the curve, do you work with the private sector to do that? How are you keeping up?

Mr. CUNNINGHAM. We do not have a dedicated task force, but we do have—we have hired a lot of people from the outside that are very technically smart in this area, especially when it comes to getting access via smartphone to bring better services to veterans. Part of that is we have recently adopted the Developmental, Security and Operations (DevSecOps) model, which is very similar to what is out in industry, and that allows us to be more agile in development where we can actually bring capabilities, art capabilities early to the customer, and then continue refining to get the end result that we wanted.

This actually is very useful not only from an operational perspective, but from a cybersecurity perspective as well. We are able to embed ourselves in this development process as a requirement early and at the right phase, so as each new capability is being added we can redefine and reevaluate the security postures that we have in place. Each deliverable we are not waiting until the very end to try to bolt cybersecurity on. That is kind of one of the terms that we have talked about in the past where we do a lot of development, at the end we try to secure it; it costs a lot of money doing it that way. We try to bake it in or embed it in through the system life cycle of the product itself.

Mr. ROY. Well, thank you for that.

One quick question for you, Mr. Dahl, in the limited time I have got remaining. Earlier in your testimony you mentioned the two Veterans Benefits Administration (VBA) cybersecurity incidents, veterans' sensitive personal information was improperly placed in a shared drive at the Milwaukee benefits office, and the security risk level for the beneficiary/fiduciary field system was set too low. How would the cybersecurity initiatives VA has recently implemented, such as continuous monitoring in the operations center, have prevented these incidents?

Mr. DAHL. Well, this is a big challenge for VA. It is a large organization, as you know, and it is so decentralized. When you run into an incident like that in Milwaukee where it is really people putting information on a shared drive that they should not have, it is a challenge for Mr. Cunningham sitting in D.C. to prevent that. They have an action plan, they have made that read-only, those shared network drives, so that is a step in the right direction.

The Beneficiary Fiduciary Facilities System (BFFS) setting that at a moderate rather than a high level, I think they are in the process of reconsidering what the appropriate level is. I would hope that when they are implementing these new systems going forward that they take a harder look at the type of data that is going to

be available on those systems and the people that are going to be able to access that data, and err on the side of caution. You know, I know there is a concern about functionality and setting levels might impact functionality, but it really is important in this day and age, as you all know, to protect that sensitive data.

Mr. ROY. Thank you, Mr. Dahl.

I yield back the minute that I have gone over.

Ms. LEE. Thank you.

I now recognize Mr. Watkins for 5 minutes.

Mr. WATKINS. Thank you, Madam Chair. Thanks to the panel for being here.

Mr. Wilshusen, in your testimony you describe how the VA categorizes its information security incidents in terms of entry points and method of attack. Forty one are listed as other. Was this information not reported or is it unknown?

Mr. WILSHUSEN. It was reported to the United States Computer Emergency Readiness Team (US-CERT) as other, which could mean that it is unknown. Compared to other Federal agencies governmentwide, that category is typically around 27 percent of all incidents reported to US-CERT by other Federal agencies are reported as other. What can indicate particularly, since this is a relatively large percentage of the incidents, is that the VA's or the Department's capability to detect or to categorize and investigate these incidents is limited.

That is important to have a really good understanding of what type of incident occurred, how it occurred, and being able to report that up to DHS and US-CERT, because that information is then used to look at incidents across the Federal Government, and then being able to help look for opportunities to share information with other agency to address similar type of incidents. Not having that information is certainly detrimental.

Mr. WATKINS. Thanks.

Mr. Cunningham, do you have anything to add about the other security incidents?

Mr. CUNNINGHAM. Categorization is difficult. I appreciate the comments made about the high percentage and the importance of sharing that information with our partners. Certainly the CISOs, the Federal CISO Council was looking for ways to refine and put more fidelity in reporting, and we are on board with talking with DHS about that in the future to help refine our ability to categorize those and still meet the reporting requirements.

Mr. WATKINS. Also, your testimony discusses VA's Enterprise Cybersecurity and Privacy Strategy, which was updated this year to incorporate government and industry best practices. The government best practices seem to come primarily from the NIST, the National Institute of Standards and Technology. What are the industry best practices and where do they come from?

Mr. CUNNINGHAM. As the—it is a larger Federal Government, there is a committee that has—a privacy committee where they talk about best practices and we are able to share. Inside VA, some of the best practices that we are deploying is, one, we moved privacy under the Office of Information Security. This means that we are more aligned. I am actually the Chief Privacy Officer as well, this puts me in a unique position to be able to support privacy both

from a cybersecurity perspective, as well as an information protection perspective.

I am intimately familiar with the challenges of privacy. I brief with the privacy team at least once a week about the challenges that we have and ways that we can either, A, remediate, educate, or at least elevate the issues that we have in that arena.

Mr. WATKINS. Executive Order 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure which was issued last year is a significant step forward in Federal cybersecurity. You describe VA's implementation of the executive order as moving from reactive to proactive cyber risk management. Can you give me some concrete examples of how you are doing things differently now?

Mr. CUNNINGHAM. The risk management framework focuses strongly on systems and, if you look at the next level up around missions, you can see where the cybersecurity framework outlined in 13800 is of great value, it gives us the structure to be able to communicate with our operations team around the value of proactively identifying issues instead of responding reactively and then having to remediate.

I can tell you that we have done work in setting up our priority queue and stack, and the CFM (Construction and Facilities Management) is part of that alignment. Now when we have our budget plans it ties into—it takes 13800, FISMA, and IG recommendations as a priority queue and weights that, so we know we are spending our money with the biggest bang for the buck to improve our cybersecurity posture.

Mr. WATKINS. Ms. Jones, has the VA ever suspended or debarred a company for violating cybersecurity rules?

Ms. JONES. Sir, the VA uses various contract clauses to ensure that in our requirements documents that we are not getting vendors that have been debarred or suspended.

Mr. WATKINS. Do you believe the Buy American Act and the Trade Agreements Act as they are implemented in government contracting are effective in protecting the supply chain?

Ms. JONES. Yes.

Mr. WATKINS. Thank you.

I yield the balance of my time.

Ms. LEE. Thank you.

Ms. Jones or Mr. Centineo, does the VA—this is following up on Ranking Member Banks' question—does the VA have restrictions on the purchase of certain types of or manufacturers of off-the-shelf equipment?

Ms. JONES. Ma'am, this goes into the clauses that we use, which are basically there are two basic types: one clause is to basically State that we are prohibited from any unauthorized manufacturers or any unauthorized products and services that the government has basically stated that we will not use in the Federal, and we also refer in our contract requirements documents to our 6500, our various cybersecurity policies and procedures.

Ms. LEE. Is there a specific list for the VA, yes or no, or is this just the—like the general Federal Government list?

Ms. JONES. The question is not a yes or no, because it is based upon the clauses. We can bring the acquisition personnel to provide

a deep drive. To the best of my knowledge, there is—in the Federal Government there is a list or a process that the contracting officers have to use, and these clauses that we put in our contracts basically say that you cannot—if there are prohibited manufacturers or prohibited processes or products, you cannot bring them into the—we cannot purchase them.

Ms. LEE. There is not a specific VA list, you are using the Federal Government list?

Ms. JONES. Not to my knowledge.

Ms. LEE. Okay.

Mr. Centineo, what role does VHA play in supply chain management?

Mr. CENTINEO. Madam Chair, the VHA, from a procurement and logistics standpoint, plays into the bio-medical maintenance community for medical devices. The Office of Health Care Technology Management in VHA does a whole-of-agency, as was referenced earlier, approach to integrating medical devices with the Office of Information Technology, the local information security officers, it is also tied in with the procurement offices, a complete composite enterprise risk analysis for medical devices.

From a procurement standpoint, they have to be completely vetted through that process in order to ensure that as we go out to do procurements they have all been validated that they meet the cybersecurity requirements.

Ms. LEE. Okay. You know, now that it seems that we are moving into the world of applications and we had a security—a privacy roundtable a couple of weeks ago and there seemed to be some conflicting information about the security of them.

I just wanted to ask, once an app is allowed to connect or download or access veterans' health data, that data can be sold under expansive terms of use under these apps, used without permission or stolen by bad actors. The Washington Post recently reported that soldiers in an intelligent unit were told to download an app developed for the unit that could provide weather updates, training changes, and other logistics. However, that app could collect a trove of sensitive personal data, including photos, calendar, location, even email, other contacts.

Mr. Cunningham or Mr. Stevens, since the VA is promoting partnerships with app providers, including health apps, what steps is the VA taking to educate veterans on protecting their personal data.

Mr. CUNNINGHAM. I think you have captured the challenge of that fairly well. Once it leaves VA's space and how the veteran uses that information becomes a challenge, and education is our primary key. We have recognized this problem, we are looking with our trained department on how we can do it through flyers, it is certainly promoting videos. Currently, we have a video around National Cybersecurity Awareness month, that we play in our waiting rooms. Any chance we can give information to the veteran about protecting their own data as part of that is important.

Ms. LEE. Are you taking any steps to vet these apps that you promote?

Mr. CUNNINGHAM. No, that—the ones we do promote are vetted through our development teams. They have to go through an anal-

ysis based off what they are going to do with that information, they have to sign a release saying they are not going to sell that information, and we are looking at what type of information that they can download.

I will ask Mr. Stevens; do you have anything to add?

Mr. STEVENS. I would also add that, for those particular apps that are accessing the VA data, they have to comply with a set of design patterns that have been specified that articulate specifically what they can and cannot do. An app is restricted within that boundary to only do those things, and that is part of the rigorous review that would be conducted through that team.

Ms. LEE. If it is found that an app is improperly using data, what is the repercussion after your review, after——

Mr. STEVENS. If it is found that veteran data has been compromised in any instance, then there is a defined process per policy that clearly articulates how to handle that incident based upon the magnitude of the event to really distill, is it an event, yes or no, and then go through an iterative process. Then, depending upon the outcome, we will judge how we respond accordingly through either, you know, providing the veteran with particular services that they would need for credit monitoring or the like.

Ms. LEE. are there any repercussions on the app developer?

Mr. STEVENS. I would have to check on that; I do not have that specifically.

Ms. LEE. Okay, I would like to have some information. That is a major issue with veterans in terms of their trust on how their data is used.

Mr. STEVENS. Yes.

Ms. LEE. I am running out of my time. I will now recognize Ranking Member Banks.

Mr. BANKS. Thank you, Madam Chair.

Mr. Wilshusen, I want to contrast hacking government networks with compromising the supply chain. The pervasiveness of Chinese companies in the technology supply chain is well established, that includes state-controlled firms as well as those that pretend to be otherwise. It would never be feasible for the U.S. Government to turn away from commercial technology, so that is not a solution, but we need a more effective defense. The answer could be to centralize responsibility for cybersecurity up and down the Federal supply chain, and maybe even centralize the supply chain itself.

You audit cybersecurity throughout the Federal Government, how do we solve the supply chain vulnerability problem?

Mr. WILSHUSEN. Well, I think because with an IT supply chain, you know, it is important to remember that this occurs and the risk occurs throughout the entire life cycle of the assets that we use. I think, first and foremost, it is important for agencies to first make sure that they have robust and effective foundational practices for securing and acquiring their IT assets, and that includes making sure that the agencies appropriately identify those risks, determine what the threats and vulnerabilities are within their supply chains, and that includes, even after we have a system up and running at our organization and we are relying on other external service partners to provide these capabilities for us.

It is important to make sure that our fundamental things in terms of assessing risk, selecting the controls that are appropriate to meet those risks, assuring doing due diligence over our suppliers and our service providers, and also then making sure we have appropriate monitoring capabilities in place to assure that the appropriate controls are being implemented.

Also, importantly, it is required that we integrate the security requirements into our contractual vehicles and into the acquisition process. It cannot be two separate aspects or we have one group acquiring the IT assets and another group that is responsible for securing, they need to be joined so they have the ability to assure that security is being built and is being implemented and considered when acquiring our IT assets.

The other key thing, I believe, is also assuring that we have a robust software and hardware testing program. As we do identify and receive software that we test the code to make sure that there are not back doors hidden into those, into the software code, and making sure that it is performing the functions for which it is intended and we intend for that software to occur.

Mr. BANKS. Mr. Dahl, what is your perspective on that?

Mr. DAHL. I will let Mr. Bowman take that question.

Mr. BOWMAN. I definitely agree that there needs to be a very thorough vetting process when you are bringing on new applications and new hardware. Before connecting anything to the network, there needs to be a robust testing process just to make sure that the controls are in place, and you need to have an effective continuous monitoring process to make sure that your security posture does not change over time.

You know, with any security program, it is a cyclical process, but you have to continuously evaluate your risks, and you have to mitigate those risks and continually evaluate the controls just to make sure your posture remains intact.

Mr. BANKS. Mr. Cunningham, anything you would like to add?

Mr. CUNNINGHAM. When it comes to supply chain risk management, NIST talks about it being our high-impact systems, although in national security systems it is for low, moderate, and high-impact systems. That is one challenge that we have to be able to understand that, when we apply it, we have to also look downstream from moderate and lows and where do we come and make that risk-based approach, because it is very costly, and even NIST publication 800161 talks about that challenge.

Specifically what we are doing at the Department, I will pass to Mr. Gary Stevens about our process there.

Mr. STEVENS. Sir, whenever hardware or software gets added to the environment, it goes through a rigorous process consistent with the risk management framework, which is an assessment of those controls at varying degrees of veracity. That includes both scanning, using Nexus Tools and those types of things to understand those hardware vulnerabilities. Then also if code, for example, gets developed internally, we have internal software assessment processes that we follow, that we allow the developer to access and use that assessment tool to iteratively assess that code as it is in the process of being developed, so they can make corrective actions on an as-required basis.

The end result of that, either internally developed code or externally provided hardware/software is a risk perspective on that particular environment that gets rolled up in a comprehensive way for an authorizing official to sign off on that level of risk in whatever level they can, and then accept that risk.

Mr. BANKS. Thank you. My time has expired.

Ms. LEE. I now recognize Mr. Roy for 5 minutes.

Mr. ROY. Thank you, Madam Chair.

Picking up a little bit on this conversation that you are having on the supply chain issues, Mr. Centineo, if I might come to you for a minute, and then, Ms. Jones, I will go to you. Maybe we will go back and forth on this, but how do you work together to coordinate cybersecurity in the VHA supply chain? If you guys could talk about that a little bit, which, you know, you are responsible for, and then the IT supply chain, which, Ms. Jones, you are responsible for, if I understand it correctly. Can you give some specific examples on how you guys interact and how that works?

Mr. CENTINEO. Sir, the procurement aspects are IT is gone through the Office of Acquisition, Logistics, and Construction, which is the Technology Acquisition Center at the Department level, I have the responsibility at the procurement and logistics VHA side, particularly for medical devices, as was kind of briefed a few minutes ago.

There is a very iterative process within the agency that the Health Care Technology and Management Office within VHA has a prescriptive process for cybersecurity, to be able to identify the types of devices that need to be used, then it works its way into the Office of Information and Technology, the local-level Information Security Officers, and it is all managed to make sure that every device that is procured or is a requirement to be procured has a completed enterprise risk assessment or risk analysis done before we actually receive it in the procurement side of the house. We actually just act upon their output to be able to go procure the items.

The process is managed up through the Specialized Device Security Division of OIT, so it is collaborative to ensure that we have matched and worked within the OIT parameters of what the security requirements are. That is for the biomedical devices, but the IT side of the house Ms. Jones has for the Strategic Sourcing.

Mr. ROY. Okay. Anything you want to add, Ms. Jones, to that?

Ms. JONES. Yes, sir. From an IT perspective, you know, the CIO is responsible for implementing the Federal IT Information Technology Reform Act, FITARA, and so one of the things that we have put in place is Department-wide a FITARA process that, regardless of what you are purchasing, you have to go through the appropriate procedures from a FITARA-compliance perspective.

In addition to that, my office works hand-in-hand with our Office of Acquisition, Logistics, and Construction Office, who is really the contracting arm of VA, to ensure that we have the right the contract clauses, to make sure that we are not purchasing anything that is prohibited, and also that we have the right cybersecurity, once again, clauses in our contracts.

I see our office in OI&T as working hand-in-hand with the entire VA, whether it is VHA, VBA, National Cemetery Administration

(NCA), the whole Department, from an IT Federal Information Technology Acquisition Reform Act (FITARA) compliance.

Mr. ROY. A question for both of you again, whatever order you want to take it up. How do you all—how is cybersecurity in the supply chain handled differently between software services and hardware, can you just touch on that a little bit?

Ms. JONES. If I may, sir, I think that is a more appropriate question for Mr. Stevens to answer.

Mr. ROY. Okay.

Mr. STEVENS. Well, again, I would say that for cybersecurity as it relates to purchasing hardware/software either procured through a vendor or internally developed, regardless of how that procurement chain happens, it still has to go through the same process, and that is the process I described earlier, which is a rigorous review of the hardware and software environment, the technical controls associated with each aspect of those particular systems, and then that rolls up into the larger authorization boundary, and that boundary ultimately has a risk perspective rendered consistent with whatever the status is of those particular controls in compliance with the particular NIST requirements. That perspective gets signed off and the risk identified by the particular action officer—or, excuse me, authorizing official.

Mr. ROY. Thank you all.

I yield back.

Ms. LEE. Thank you. I would now like to turn to Mr. Wilshusen. In the GAO testimony at a previous hearing, it referenced a report that found that the VA had regressed in terms of leadership commitment, and, based on today's testimony, it seems that the VA still failed to take action on 42 of the 74 action items that the GAO identified in 2016. In the 6 months since that report was issued, has the VA corrected its course?

Mr. WILSHUSEN. We are still waiting—and indeed, actually we just this week received documentation from VA on a number of those open recommendations from 2016, and we are in the process of reviewing them. I will know better after we have a chance to analyze the evidence that was provided to us this week.

Ms. LEE. Okay, and we would love to have an update on that.

Mr. WILSHUSEN. I will be happy to give that.

Ms. LEE. What is the status of the VA to address the recommendations that the GAO made over the last 4 years?

Mr. WILSHUSEN. Well, one of the status is, as I mentioned, we just received the evidence related to many of those, but as you mentioned, 42 of the 74 recommendations we made back in 2016 are still open and not implemented, in our view.

One of the issues that we have identified in reviewing evidence that VA has provided to us over the years is that often it does not seem like it is validating the effectiveness of its corrective actions, because it has asserted, for example, that it had implemented 39 of the 42 recommendations that currently are open, but when we went in and looked at the evidence provided, it was not sufficient enough for us to confirm the implementation of that recommendation so we could close it.

That is one of the challenges I think it faces is just validating and verifying the effectiveness of its corrective actions. That is one aspect.

We have also made four recommendations to VA relative to a cybersecurity risk management program, which we issued a report earlier this year on that, it is a governmentwide review. VA concurred with each of those four recommendations and asserted that it is taking actions to implement them.

As it is in the recommendation we made relative to its categorization of the work roles of its IT and cybersecurity workforce positions, we noted that VA had not correctly categorized, I think it was like around 48, 45 percent of its IT positions. We made a recommendation for them to review that categorization in terms of what work roles those positions perform. It concurred with our recommendation and also asserted that it is taking corrective action. We have not yet received evidence of the completion of those actions as of today.

Ms. LEE. With respect to the validation of progress, are there any institutional changes that you recommend for VA leadership to help facilitate better results in that respect?

Mr. WILSHUSEN. Well, one is just to make sure that as the folks who are implementing the corrective actions is that it is properly reviewed and that those actions are confirmed perhaps by an independent party or another person or another group within the organization.

We had noted that at other agencies, Office of Personnel Management, as an example, had taken a similar approach where an independent party within the office had reviewed the actions taken by the operational folks in implementing our recommendations in resolving the underlying vulnerability.

Just having a secondary check to verify the effectiveness of those controls would be useful.

I might also add, in many of our recommendations they are limited to the scope of our review, but many of the vulnerabilities that we identify could apply to other similar systems. Typically, we only look at a few systems when we go in and examine information security controls, maybe 10, 15, but whatever vulnerabilities we identify on those systems could very likely also be in effect and affect other systems. Organizations would be wise to see if similar systems are also afflicted by the vulnerabilities that we identify during our examinations.

Ms. LEE. Okay, thank you.

I now recognize Mr. Banks.

Mr. BANKS. Thank you, Madam Chair.

Mr. Cunningham, there is no doubt in my mind that when a company infects its products with malware, or inserts back doors or engages in any kind of hacking, it must be immediately banned from doing business with the U.S. Government. I am going to ask you a series of questions about companies that have been proven to have done just that. I want you to tell me whether VA has ever purchased their products, either before or after bans were put in place.

Mr. Cunningham, as VA ever purchased equipment from Huawei Technologies?

Mr. CUNNINGHAM. I am going to have to take that back for the record.

Mr. BANKS. Okay. Mr. Cunningham, has VA ever purchased from ZTE Corporation?

Mr. CUNNINGHAM. I will have to take that back for the record.

Mr. BANKS. How about Hytera Communications Corporation?

Mr. CUNNINGHAM. I will have to take that back for the record.

Mr. BANKS. Same question, has VA ever purchased from Hangzhou Hikvision Digital Technology Company?

Mr. CUNNINGHAM. I will have to take that back for the record.

Mr. BANKS. How about Dahua Technology Company?

Mr. CUNNINGHAM. I will have to take that back for the record.

Mr. BANKS. The last one, has VA ever purchased software from Kaspersky Lab?

Mr. CUNNINGHAM. I will have to take that back for the record as well.

Mr. BANKS. All right, we will look forward to those questions being answered for the record.

Mr. Cunningham, as I said in my opening statement, it seems cybersecurity became a focus in the health care sector relatively late. The Community Health Systems (CHS) hack should have been a wake-up call, but cyber criminals may still see health care organizations as soft targets. VA is in somewhat of a unique position as a government agency and a health care system. How do you evaluate your cybersecurity risk and shape your strategy accordingly?

Mr. CUNNINGHAM. You are correct in assessing VA as also a health care provider. We are the largest networked health care provider in the United States, and we take that role seriously and we work with our partners on that. I can say that we share information with our partners and we share it with DHS, so to the greater good let our detection be their protection and likewise.

In the question I would say that we have that same struggle that all have when it comes to hospitals, very well-intentioned, very smart employees in providing the best service they can for their customers and, in our case, our veterans, will sometimes will look for opportunities to streamline the process to bring in new technology. Where we can and how we can through technical means and policies we put in place, we minimize that and, when we recognize it, we take appropriate action, whether it is through education of the individual or, if we see a malicious or known policy break, through administrative means.

Mr. BANKS. Okay. Madam Chair, that is all the questions I have, but I do ask for unanimous consent to enter the U.S.-China Economic and Security Review Commission's report entitled "Supply Chain Vulnerabilities from China and U.S. Federal Information and Communications Technology" into the record.

Ms. LEE. Without objection. Thank you.

Ms. LEE. I now recognize Mr. Lamb for 5 minutes.

Mr. LAMB. Good morning. Thank you all for coming.

For our GAO witnesses, would you mind elaborating a little bit on how VA compares to other Federal agencies? I saw in the report that they are one of 18, I think, of the 24 who have cybersecurity as a material weakness, are you able to say anything about, among those 18, sort of where VA sits?

Mr. WILSHUSEN. I would say based on a couple factors. Where they are with their information security program is consistent in many ways with many Federal agencies, but I also think in a couple various it may be a bit beneath the others, particularly when it comes to looking at the length of time that it has consistently reported a material weakness in the security controls over its financial systems, for financial reporting purposes. It has been going on 17 years in a row now. A few agencies, I believe, meet that longevity of that particular weakness.

In addition, the number of and percentage of its cybersecurity and IT-related personnel and the work roles that they perform, the high percentage of positions that were miscategorized based upon the work roles from the NIST cybersecurity workforce framework was rather startling in many respects.

In a couple areas I think it could do a much better job, but like most Federal agencies, particularly the larger ones, they have a number of significant challenges to overcome.

Mr. LAMB. Thanks.

Mr. Cunningham, I want to continue Mr. Banks' line about the supply chain issues a little bit, and if there is someone else who is better to answer it, you can let us know, but my questions are a little less specific.

It just seems like the concern about the supply chain is coming at a good time in some ways for VA, because I have only been sitting on this committee a little over a year and I have heard a lot about how we need to do infrastructure upgrades, we need to buy new computers, new systems, routers, networks, all this kind of stuff, especially looking down the road toward the records modernization that we are going to have and how that is going to really rely on having the bones of a modern system that can run it.

What is VA doing right now proactively, regardless of what has happened in the past, what are you doing proactively to ensure a safe supply chain for everything that is going to be purchased say for the next 4 or 5 years?

Mr. CUNNINGHAM. I would put in that VA is compliant with DHS's recommendations around binding operational directives when it identifies at-risk vendors or solutions, and we also support GSA in their efforts to identify where are the best sources to buy from that have been vetted.

In that regard, I would say that we are struggling like many other Federal agencies to understand where our department resides in either blacklisting a particular organization or company and not—that is not exactly in the VA's mission to determine whether a company is allowed to do work with the Federal Government or not, we will leave that to general counsel, and certainly to DHS and the intelligence community to tell us where we should not go or where we should not operate.

Mr. LAMB. Okay. In other words, is it safe to say you are sort of following the advice that is being issued across the Federal Government? You are not getting like specific—you are not getting input from these agencies that are specific to VA or to health care-type data or systems?

Mr. CUNNINGHAM. Correct. We are following the Federal regulation in that, if we feel that there is a vendor we prefer not to use

because of past experience, then it is certainly inside the roles of the procurement team, as well as the authorizing official and the system owner, to not acquire that equipment.

Mr. LAMB. Okay. Last, I saw in the news I think within the last week that veterans' health data is going to be available through Apple Health on iPhones now, do I have that right?

Mr. CUNNINGHAM. That is correct.

Mr. LAMB. Are there security implications of that? Does Apple sort of assume the role of the protector of that data at that point, or how have you thought through that?

Mr. CUNNINGHAM. We are looking at ways to protect that information, so it is ensured that it is tunneled all the way from the time it leaves VA's boundary until it arrives in the veteran's personal device. There are agreements with Apple on acceptable use of that data and protecting of that data.

Mr. LAMB. Thank you.

Madam Chairwoman, I yield back.

Ms. LEE. Thank you. I was concerned when I looked at the VA's budgetary submission for 2020. The 2019 budget contained $381 million for information security, while the 2020 budget is $362 million. Mr. Cunningham, could you tell me why there is a $19 million reduction?

Mr. CUNNINGHAM. Well, one, I think there are opportunities we have seen already where we can consolidate some of our activities to be more effective, definitely where we can partner or even ask for support from our other VA partners, as regards to especially if it is a specialized cybersecurity service that we are providing to a particular pillar inside the Department. We are looking at ways to be more effective identifying where the money is going and what activities are being tied to in that regard.

Ms. LEE. Great. We like saving money.

One question I have, why is security not listed as one of OIT's three strategic goals in this budgetary proposal?

Mr. CUNNINGHAM. I would have to ask the team that put together who is not here today.

Ms. LEE. Okay.

Mr. CUNNINGHAM. I will have to get it back for the record.

Ms. LEE. Thank you.

Mr. Cunningham or Stevens, this is in respect to the breaches in Milwaukee and Long Beach and the BFFS. Something that concerned me was that VA's internal assessments determined that these were not technically breaches and, therefore, did not require that veterans be notified of the incidents. Is the VA considering updating what it defines as a breach, so that veterans affected by these incidents can and will be notified?

Mr. CUNNINGHAM. From a privacy perspective, we had no evidence that the information was taken outside of VA's bounds or that personnel that were not read in or accountable through user agreements to protect that data had access. In that regards, we look at it that while we can notify individuals, that would be—you know, looking at it, do you show—if we show that it has not left the building, do we show that has been compromised? By definition, we look at it that it has not.

Where the benefit of notifying an individual that their information was looked upon by somebody who had authorization or signed agreements to protect the data we did not see as being reportable.

Ms. LEE. This is for the GAO. Is the VA's definition of breach that we just heard here, is that in accordance or is it consistent with the rest of the Federal Government?

Mr. WILSHUSEN. Usually, a breach is referred to as one where it is a violation of policy or practice that could put information and services at risk.

Ms. LEE. Okay. The policy that you have, do you think that that is in line with what veterans are expecting with respect to the security and the privacy of their data?

Mr. CUNNINGHAM. I think as it is presented, it has not left the VA, it has not been in possession by those that are bound to maintain the security of that information, I believe, as a veteran, I would understand that there are protocols that are broke and things do happen, but provided that the information was not leaked or lost, then I would understand that that is part of operations and I hope they would do better in the future to make sure that does not happen or occur.

Obviously, you put it closer to exploitation and that would trouble me, but also I understand that that is part of operations and if they are improving, as a veteran, I am satisfied with that.

Ms. LEE. Just to wrap up, in your assessment of your position in overseeing cybersecurity and understanding that what the definition of secure is, what do you identify, especially in light of the reports that we have and the recommendation, what is your assessment of what a win will be in terms—what is success in cybersecurity?

Mr. CUNNINGHAM. If you are asking—are you asking me——

Ms. LEE. Overall, in general, you have received recommendations from OIG and GAO, recognize many deficiencies, and so you—it seems like you are making progress, so what is success to you, is my question.

Mr. CUNNINGHAM. Certainly. Thank you for the clarification.

I look at it that, if we can look at the measures and metrics of how proactive we are in blocking, how proactive we are in identifying potential risks and then funding them, and then looking at over time what actually does occur to see if we predicted correctly. Certainly we cannot goldplate every system to the degree that I would be comfortable saying that we are 100-percent sure that it will not occur, but how can we make sure that we show due diligence in identifying those. That comes into the postmortem on how resilient we are and then identifying, when we do have a breach, what were the causal factors and were those things tied to what we already knew and, if we knew that, why did not we take that as a priority.

Ms. LEE. Okay. Thank you.

My time is up and I am going to—I think we are ready to adjourn.

I would like to thank all of the witnesses for your participation today. You know, as it comes to the VA providing care for our veterans, our men and women, especially with respect to data privacy—and this is the most sensitive personal data and, more im-

portantly, it is a trust relationship—in making sure that we are doing all we can to honor that our trust that our veterans give to us, especially with respect to this data.

This, as we do the electronic health record modernization and dealing with the legacy systems that present some serious challenges with that aging technology, as well as the standards that you have in place and making sure the protocol is being followed, certainly is a challenge. I thank you for being here and for your effort to address this, as well as OIG and GAO to keep us informed, and hopefully we can continue to work together in a cooperative spirit to make sure that we are protecting the data of our veterans, not just internally, but also, as we discussed today, with respect to applications as they become more and more widespread and used by our veterans.

Thank you. This is hopefully the beginning of a back-and-forth conversation and we will continue to work together, especially as we provide the oversight in the modernization efforts.

All members have 5 legislative days to revise and extend their remarks and include extraneous material.

This hearing is now adjourned. Thank you.

[Whereupon, at 11:31 a.m., the subcommittee was adjourned.]

A P P E N D I X

PREPARED STATEMENTS OF WITNESSES

Prepared Statement of Paul Cunningham

Good morning Madam Chair Lee, Ranking Member Banks, and distinguished Members of the Subcommittee. Thank you for the opportunity to testify today in support of the Department of Veterans Affairs (VA) cybersecurity initiatives to protect Veterans' and VA employees' sensitive data. I am accompanied today by Gary Stevens, Deputy Chief Information Security Officer, Executive Director for Information Security Policy and Strategy, Office of Information and Technology (OIT), Mr. Andrew Centineo, Executive Director, Procurement and Logistics, Veteran Health Administration (VHA) Procurement and Logistics Office, and Ms. Luwanda Jones, Deputy Chief Information Officer, Strategic Sourcing, OIT.

I want to begin by thanking Congress, and specifically this Subcommittee, for your continued support and shared commitment to the success of VA cybersecurity program. VA's mission of improving health care delivery to our Nation's Veterans and those who care for them while being responsible to safeguard their private information is conducted because of your unwavering support.

Introduction

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) has the great responsibility of safeguarding Veteran information and VA data, ensuring VA's networks and infrastructure are resilient to threats, and maintaining a secure operational environment that supports business needs and mission outcomes. OIT's Office of Information Security (OIS) is the primary office that carries out these responsibilities. OIS' mission is to protect the Personally Identifiable Information (PII) and Protected-Health Information (PHI) of Veterans, their families, and VA employees, as well as VA information systems and infrastructure. Security and privacy are integral to the Veteran experience. For this reason, VA believes that exceptional service to our Veterans can only be achieved in a secure digital environment. This belief guides a cybersecurity strategy that rises to meet the highest standards while focused on the protection of the Veteran.

VA has a complex cybersecurity environment, with over 1.6 million connected devices across approximately 2,500 facilities ranging from offices to data centers to VA hospitals, benefits regional offices, and beyond. Additionally, Secretary Robert Wilkie has outlined a Department-wide modernization strategy to transform and enhance how VA serves Veterans. VA is transforming the Veteran experience, providing them increased access to services and information. Migrating from legacy systems and allowing Veterans to access this information requires VA to further extend its digital footprint, introduce new technologies, and increase interoperability and data sharing. However, these improvements also introduce unique cybersecurity, privacy, and third-party risks. VA's cybersecurity strategy and posture aim to address these risks while enabling and improving business processes and shifting VA to a proactive stance in an ever-changing cyber landscape.

VA's cybersecurity posture consists of a holistic and robust set of strategies, programs, and capabilities. VA's 2019 Enterprise Cybersecurity and Privacy Strategy (ECPS), borne out of its Enterprise Cybersecurity and Privacy Program (ECSP), articulates the Department's current cybersecurity strategy and future cyber and privacy goals. These goals include enhanced risk management, secure interoperability, exceptional customer service, secure and resilient business processes, and a strong cyber and privacy workforce and culture. The Program, which was developed in 2015 and fully implemented in 2017, governs the Strategy and shifts VA to a proactive cybersecurity posture with programs and capabilities including the following:

- Supply Chain Risk Management (SCRM);
- Governance, Risk Management, and Compliance (GRC) tool;
- Information Security Continuous Monitoring (ISCM);

- Continuous Diagnostics and Mitigation (CDM); and
- Cybersecurity Operations Center (CSOC).

FY 2019 Enterprise Cybersecurity and Privacy Strategy (ECPS)

For Fiscal Year (FY) 2019, VA updated its ECPS to align with its Department-wide modernization strategy and to further mature its cybersecurity posture. The updated ECPS will adopt industry and Government best practices, account for changes in the cybersecurity landscape, and build a proactive and forward-looking cybersecurity posture. VA's updated ECPS consists of the following five goals: (1) Enhance enterprise cybersecurity and privacy risk management; (2) Ensure secure interoperability both within and outside VA; (3) Deliver exceptional customer service;(4) Enable secure and resilient business operations; and (5) Cultivate a VA cybersecurity and privacy workforce and culture. Together, they strengthen cybersecurity at VA while also improving business processes, and by extension, the service VA provides to Veterans.

(1) To enhance enterprise cybersecurity and privacy risk management, VA will emphasize cybersecurity and privacy in enterprise-wide risk management processes. VA has implemented the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) to manage the Department's cybersecurity risk at three organizational levels: information system, mission area/business process, and organization. The VA is leveraging cybersecurity best practices, from NIST, to address threats to medical devices, supply chain processes, financial services, and sources of protected Veteran information. Additionally, the framework drives VA decisions about cybersecurity and privacy investments.

(2) To ensure secure interoperability both within and outside the Department, VA must protect data regardless of location. Access methods must be secure and flexible, protecting data while enabling VA business processes. VA is leveraging shared security and privacy capabilities and collaborating with Federal and commercial partners and third-party providers to meet and enforce Federal security and privacy requirements. For Veterans, interoperability means streamlined access to data and services — but not at the expense of security and privacy.

(3) In pursuit of its permanent goal to deliver exceptional customer service, VA is integrating its cybersecurity policies and standards into business processes. With this integration approach, security and privacy are an enabler, not a barrier, to efficient business processes, facilitating Department-wide adoption of a rigorous cybersecurity posture.

(4) To enable secure and resilient business operations, VA is improving cyber hygiene across the Department. Good cyber hygiene limits threat exposure, accelerates adoption of protective cyber technologies, and enhances cross-organizational incident response processes.

(5) VA continually aims to cultivate a VA cybersecurity and privacy workforce and culture. VA is recruiting, training, and retaining a talented cyber and privacy workforce through its cyber retention pay and benefits, career progression tools, and training opportunities. VA is renaming Development Operations (DevOps) — a program office established this year to shift VA to an Agile development mindset — to Development Security Operations (DevSecOps). This change also reflects and embodies VA's security-first mindset as a cyber-conscious organization because protecting Veterans' information is not only a technical concern but a human and customer service issue.

VA plans to execute its updated ECPS by aligning the strategy with NIST RMF and Cybersecurity framework (CSF) policies and standards, as well as with internal stakeholder business processes. VA ensures enterprise-wide awareness and adoption of the strategy by aligning cyber policies and activities with business requirements and processes. With a robust cybersecurity posture baked into business processes, the Department can be sure that security and privacy are the baseline for every service provided to Veterans.

Enterprise Cybersecurity Program (ECSP)

VA's ECPS is governed by the ECSP, the Department's sanctioned cybersecurity program. VA established ECSP under the authority of an official memorandum issued in April 2018. The memorandum was issued in response to Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical In-

frastructure. The transition to ECSP marked a shift from reactive to proactive cyber risk management.

ECSP orients VA to adopt a more proactive approach to manage cyber risk by emphasizing cybersecurity projects that are aligned to the NIST CSF. ECSP incorporates leading practices and implements guidance from the NIST CSF to mature VA's cybersecurity posture, capabilities, and culture. ECSP also bolsters VA's proactive cybersecurity posture through the ECSP Prioritization Tool, which allows leadership to prioritize and address the highest-priority cybersecurity concerns. This allows the Department to make informed and defensible decisions about cybersecurity activities.

Finally, ECSP provides mechanisms to support external reporting requirements and maintain an acceptable level of overall cybersecurity risk compliance as required by the Federal Information Security Modernization Act (FISMA) of 2014.

VA's goal is for ECSP to become a sustainable, world-class cybersecurity program that protects VA information systems, and most importantly, Veterans' information. With a successful ECSP guiding VA's cybersecurity activity, Veterans can trust that ease of access does not mean compromised security and privacy.

Supply Chain Risk Management (SCRM)

VA must secure and manage risk related to its supply chain processes. Third party suppliers and external Federal and commercial partners must comply with VA's security and privacy policies to access VA data and information systems. OIT's Office of Strategic Sourcing (OSS), which modernizes VA's sourcing practices for IT products and services is collaborating with VA's contracting offices to ensure we are ordering from approved resellers of an OEMs products to avoid gray market equipment and we utilize Trade Agreement Act (TAA) compliancy in our contracts. We are also working with VA contracting offices to enforce prohibitive language is referenced in contracts templates preventing contractors and vendors from hiring or teaming with contractors and vendors that have been deemed suspended.

VA also requires that all users of its network meet security requirements specified in each contract. Access is strictly controlled by whether users have a 'need to know' information in the course of their duties. VA assesses cybersecurity risks associated with medical devices during the procurement process. Through OSS and OIS, VA continues to integrate cybersecurity and privacy with procurement, acquisition, and supply chain processes in conjunction with the Technology Acquisition Center (TAC) and other business partners across the Department.

Information Security Continuous Monitoring (ISCM)

VA established the ISCM program to provide Department-wide oversight and governance of ISCM activities according to Department of Homeland Security (DHS) requirements. ISCM consists of a combination of technological, operational, and management capabilities that consistently assess the security posture of VA information systems. These capabilities allow for data-driven risk management rather than compliance-driven risk management. VA is collaborating with DHS to remain in lockstep with Federal statutes, guidance, and updates to the program.

Continuous Diagnostics and Mitigation (CDM)

VA is implementing DHS' CDM program to better safeguard information technology (IT) assets. CDM allows the Department to better grasp its universe of assets, users, and network activity, which in turn allows VA to efficiently and effectively monitor for, identify, and mitigate potential risks.

The CDM program delivers capabilities in five distinct areas: (1) Facilitate continuous monitoring of assets, users, networks, and data through the CDM dashboards; (2) Identify assets on VA's network through Asset Management;(3) Identify and monitor users on the network through Identity and Access Management; (4) Identify what occurs on the network and how to protect it through Network Security Management; and (5) Manage and protect data on the network through Data Protection Management.

On November 1, 2019, the Department of Veterans Affairs (VA) achieved a major milestone by finishing the implementation of tools for hardware asset discovery giving VA visibility to assets connected to the network. This installation culminated a 4-year project that involved personnel from VA and the Department of Homeland Security (DHS) as part of the Continuous Diagnostics and Mitigation (CDM) program administered by DHS. As the VA continues to enhance its CDM capabilities, the Department begun a 30-month effort with DHS called the Request for Service (RFS) 15 which allows VA to enhance our Identity and Access Management (IAM)

tools and strategy, allowing VA to better manage users on our network, including those with special access to sensitive systems. Other efforts with DHS and internally at VA are addressing CDM capabilities in order to know what is happening on the network and protecting our data.

Cybersecurity Operations Center (CSOC)

VA's CSOC consistently monitors, reports, and responds to cyber threats and vulnerabilities. The CSOC conducts enterprise network security monitoring for the Department. The CSOC is divided into five sub-programs: Cyber Threat Intelligence, Cyber Technical Services, Cyber Incident Response, Cyber Security Analytics, and Cyber Business Intelligence. Coupled with an improved understanding of IT assets through CDM, consistent monitoring allows the Department to proactively detect, identify, and respond to suspicious activity, mitigating potential cyber risks, and protecting Veterans before their data is ever in danger.

Federal Information Security Modernization Act (FISMA)

FISMA, signed into law in December 2014, defines a framework to protect Government information, operations, and assets against threats. FISMA requires the VA to develop, document, and implement a Department-wide program to secure the information systems that support its unique operations and assets. The law requires annual reviews of information security programs to keep risk at or below specified acceptable levels.

VA submitted its Fiscal Year 2019 second quarter (Q2) CIO FISMA report to DHS and OMB on April 16, 2019. In the subsequent Risk Management Assessment, VA was evaluated as "Managing Risk" overall, with only the "Respond and Recover" category rated "at risk." Additionally, VA has met seven of the ten Cross Agency Priority (CAP) goals defined in the President's Management Agenda: Software Asset Management, Authorization Management, Mobile Device Management, Privileged Network Access Management, High Value Assets (HVA) System Access Management, and Data Protection. CDM will allow VA to meet the remaining three CAP goals.

Moving forward, VA continues to focus efforts on improving access control, governance, privacy and data protection, continuous monitoring, and configuration management processes and capabilities. VA also continues a shift from a reactive to proactive approach to its audit experience, reviewing previous audit findings to determine and enact appropriate remediation measures and improve audit scores in the future.

Department of Defense (DoD)/VA Collaboration

Seamless and secure interoperability is one of five imperatives under VA's modernization strategy. VA strives to streamline the Veteran experience by achieving seamless interoperability between VA and DoD, as well as other Federal and commercial partners. However, interoperability must also be secure; VA must augment standardized and secure designs, interfaces, and processes to promote secure access to authoritative data.

To this end, VA is collaborating with DoD to jointly deploy standards and controls based on NIST and Committee of National Security Systems (CNSS) guidelines. VA's GRC tool and Enterprise Mission Assurance Support Service (eMASS) join VA and DoD under a shared RMF to facilitate joint cybersecurity activities. Finally VA, in coordination with DoD, is building a capable cybersecurity monitoring team. In the future, VA plans to explore paths to mutually designating jointly shared systems as National Security Systems (NSS). VA and DoD are working shoulder-to-shoulder to strengthen privacy and security for Veterans.

Workforce Management

In response to a shortage of cyber and privacy personnel across the Federal Government, VA has emphasized the development of a world-class technology workforce as one of its six focus areas. VA has implemented special programs and incentives to attract, recruit, and retain talented cyber and privacy professionals, cyber retention pay and benefits, and other internal and external training and reskilling opportunities. Most importantly, VA has found that candidates and employees are attracted to and continually inspired by the Department's mission. Employees understand the impact they have on Veterans. As a cyber-conscious organization, VA will continue to emphasize the immeasurable impact of cybersecurity on Veterans. By

protecting Veteran data and VA information systems and ensuring secure services, cyber and privacy employees directly serve Veterans every day.

Quarterly Notice to Congress

On a quarterly basis, VA reports to Congress any breaches that occurred in the previous quarter, as mandated by Public Law 109–461 Veterans Benefits, Health Care, and Information Technology Act of 2006. For each data breach, the report identifies the Administration and facility responsible for processing or maintaining the sensitive personal information involved in the data breach and the status of any remedial or corrective action. The report is signed by the Secretary and transmitted to the Chair and Ranking Member of both Senate and House Committees on Veterans' Affairs. This continuous reporting promotes transparency and cooperation between the Department and Congress. Within VA, reporting improves situational awareness and leads to an improved data security posture. For Veterans, this means that their personal information becomes even safer.

Conclusion

The complex issues before VA represent an opportunity for the Department to renew its commitment to protecting Veteran and employee data. The Department is modernizing its cybersecurity strategy to meet new Federal guidance and to keep pace with today's ever-evolving technology landscape. While expanding access for Veterans, VA is concurrently strengthening access control between the Department and its external partners. VA has established programs to constantly and consistently monitor cyber activity and identify gaps and new opportunities to mature its posture. VA is working shoulder-to-shoulder with DoD and our Federal and commercial partners to ensure seamless and secure interoperability that maintains the privacy and security of our Nation's heroes and VA's employees. Recruiting, developing, and maintaining a talented cyber and privacy workforce remains a priority and motivates human capital management efforts. VA continues to maintain compliance with federally mandated requirements such as Binding Operational Directives, Executive Orders, and Office of Management and Budget (OMB) memoranda. VA understands the challenge of maturing its cybersecurity posture while also improving access and services that Veterans want and deserve. With the above strategies, policies, and programs, the Department has risen to that challenge, and continues in its mission to protect and secure the information of, and services for, our Veterans. Madam Chair, Ranking Member, and Members of the Subcommittee, thank you for the opportunity to testify before the Subcommittee today to discuss one of VA's top priorities. I am happy to respond to any questions that you have.

Prepared Statement of Nick Dahl

Madam Chair, Ranking Member Banks, and members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General's (OIG's) oversight of VA's information technology (IT) security program. I am accompanied today by Mr. Michael Bowman, Director of the OIG's Information Technology and Security Audits Division. My statement focuses on the security program's purpose and the challenges in protecting the confidentiality, integrity, and availability of VA systems and data. The OIG's conclusions expressed in this statement are based on recent oversight reports that touch on aspects of VA's development and management of information security and IT systems.

BACKGROUND

IT systems and networks are critical to VA for carrying out its mission of providing medical care and a range of benefits and services to millions of veterans and their families. VA is responsible for storing, managing, and providing secure access to enormous amounts of sensitive data, such as veterans' medical records, benefits determinations, financial disclosures, and education records. The OIG recognizes and appreciates that this is a complex undertaking. Ensuring the secure operation of the systems and networks that contain this sensitive data is essential, especially considering the wide availability and effectiveness of internet-based hacking tools. Lack of proper safeguards renders these systems and networks vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other VA systems. The OIG has a long history of reporting on security incidents at VA in which sensitive information, including personally identifiable information (PII), has been lost, stolen, or improperly secured,

potentially exposing countless veterans and their families to the loss of privacy, identity theft, and other financial crimes.[1]

For Fiscal Year (FY) 2020, VA requested a total IT investment of $4.3 billion, of which $362 million is to fund information security in connection with enterprise operations and maintenance.[2] Those investments must be carefully deployed and monitored. To the extent that VA does not properly manage and secure their IT investments, they can become increasingly vulnerable to misuse and mishaps. Security failures also undermine the trust veterans put in VA to protect their sensitive information, which can affect their engagement with programs and services.

MAJOR CYBERSECURITY CHALLENGES REPORTED BY OIG

In the OIG's 2019 Major Management Challenges, which will be released later this month, information management is highlighted. It is not a new problem; the OIG has identified information management as a major management challenge since 2000. The OIG specifically noted VA's challenges in ensuring effective information security program and system security controls. The OIG will continue to monitor VA's progress in addressing those challenges.

The OIG's independent contractors that perform the annual audit of VA's consolidated financial statements have reported that they will once again identify IT security controls as a material weakness in the findings also being released later this month.[3] VA relies extensively on IT system controls to initiate, authorize, record, process, summarize, and report financial transactions, which are then used for preparing its financial statements. Many of VA's legacy systems have been obsolete for several years.[4] Because of their obsolescence, legacy systems are more burdensome and costly to maintain, cumbersome to operate, and difficult to adapt to VA's continuously advancing operational and security requirements. Given the risks associated with using outdated systems, internal controls over these operations take on even greater importance to ensure the integrity, confidentiality, and reliability of critical data while reducing the risk of errors, fraud, and other illegal acts. The OIG has reported IT security controls as a material weakness for more than 10 consecutive years.

Additionally, the OIG has identified and reported on a myriad of significant deficiencies in IT security that are highlighted below. These reports help demonstrate the range of issues that VA has faced and the persistence of problems that can have serious consequences for veterans and the Department's programs and operations.

Federal Information Security Management Act Compliance

The Federal Information Security Management Act of 2002 (FISMA) requires that agencies and their affiliates (such as government contractors) develop, document, and implement an organization-wide security program for their systems and data.[5] For the 20th consecutive year, the OIG has reported on the extent to which VA has IT safeguards in place consistent with the Act's requirements. The Fiscal Year 2018 audit revealed that VA has made progress producing, documenting, and distributing policies and procedures as part of its security program. However, VA continues to face significant challenges in complying with FISMA requirements due in part to maintaining an aging and outdated IT security infrastructure. [6]

The Fiscal Year 2018 FISMA report, published by the OIG in March 2019, contained multiple findings and 28 recommendations to the Assistant Secretary for In-

---

[1] Review of Alleged Unsecured Patient Data base at the VA Long Beach Healthcare System, March 28, 2018; Review of Alleged Breach of Privacy and Confidentiality of Personally Identifiable Information at the Milwaukee VARO, September 15, 2016; Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans, July 11, 2006.

[2] Department of Veterans Affairs Fiscal Year 2020 Funding and Fiscal Year 2021 Advance Appropriations, Volume II: Medical Programs and Information Technology Programs

[3] A material weakness is a deficiency, or combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. The OIG's annual audit of VA's consolidated financial statements is pending publication and will be released in November 2019.

[4] For example, VA's core financial accounting system, FMS, is coded in Common Business Oriented Language (COBOL), which is a programming language developed in the late 1950's. VA's system employed at the medical centers—Veterans Health Information Systems and Technology Architecture (VistA)—was built in the late 1970's. Both systems are considered to be significantly outdated.

[5] Title III, The Federal Information Security Management Act of 2002, E-Government Act of 2002, P.L. 107–347 (December 17, 2002).

[6] Federal Information Security Modernization Act Audit for Fiscal Year 2018, March 12, 2019.

formation and Technology for improving VA's information security program. These findings and recommendations focused on the following areas:

- **Configuration Management Controls** are designed to ensure critical systems have appropriate security baseline controls and up-to-date vulnerability patches implemented. The OIG's findings included that VA systems and key data bases were not timely patched or securely configured to mitigate known and unknown information security vulnerabilities. Additionally, VA did not sufficiently monitor medical devices and ensure they were properly segregated from other networks.
- **Identity Management and Access Controls** are meant to make certain that password standards are consistently implemented across the enterprise and that user accounts are monitored to enforce the limitation of access privileges to those necessary for legitimate purposes and to eliminate conflicting user roles. The OIG's FISMA audit revealed that password standards were not consistently implemented and enforced across multiple VA systems, including the network domain, data bases, and mission-critical applications. In addition, multifactor authentication for remote access had not been fully implemented across the Department.[7] Further, inconsistent reviews of networks and application user access resulted in inappropriate access rights being granted, as well as numerous generic, system, and inactive user accounts not being removed or deactivated from the system.
- **The Agencywide Security Management Program** makes sure that system security controls are effectively and continuously monitored, and system security risks are effectively remediated through corrective action plans or compensating controls. The OIG's findings included that security management documentation, including the risk assessments and System Security Plans, were outdated and did not accurately reflect the current system environment or Federal standards. Also, background reinvestigations were not performed timely or tracked effectively, and personnel were not receiving the proper level of investigation for the sensitivity levels of their positions.
- **Contingency Planning Controls** ensure that mission-critical systems and business processes can be restored in the event of a disaster or emergency. The OIG determined that backup tapes were not encrypted prior to being sent to offsite storage at selected facilities and data centers. The OIG team also noted instances of unplanned outages or disruptions where services were not recovered within prescribed Recovery Time Objectives. Of addition concern, these instances did not prompt contingency plan reviews or updates in accordance with defined policy.

The Principal Deputy Assistant Secretary for Information and Technology concurred with 25 of 28 OIG recommendations and provided acceptable action plans for implementing open recommendations.[8] Overall, the OIG's FISMA audit shows that for VA to achieve better IT security outcomes, the Department must take actions that

- Address security-related issues contributing to the IT material weakness being reported again in the Fiscal Year 2019 audit of VA's Consolidated Financial Statements;
- Improve deployment of security patches, system upgrades, and system configurations that will mitigate significant vulnerabilities and enforce a consistent process across all field offices; and
- Enhance performance monitoring to ensure controls are operating as intended at all facilities and that identified security deficiencies are communicated to the appropriate personnel so they can take corrective actions to mitigate significant security risks.

Other VA IT Security Concerns

Other focused OIG reviews and audits, described below, also provide examples of the risks of ineffective or improper IT security.

---

[7] Multifactor authentication grants users access only after successfully presenting two or more pieces of evidence (or factors): knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is, such as fingerprint or eye-scanning biometrics).

[8] While the Principal Deputy Assistant Secretary did not concur with three recommendations, the OIG believes these recommendations warrant further attention from VA and will follow up on these issues during the Fiscal Year 2019 FISMA assessment.

Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives[9] The OIG conducted a review in response to a complaint from a Veterans Service Officer (VSO) working at the Milwaukee VA Regional Office (VARO) that veterans' sensitive personal information was stored on shared network drives and was likely accessible to other network users. Sensitive personal information—any information about an individual that is maintained by VA and can be linked to that individual—is protected by law and VA policy.[10] Without proper protection, veterans are at significant risk of unauthorized disclosure and misuse of their sensitive personal information. This has the potential to expose veterans to fraud and identity theft. Also, if a breach of sensitive personal information were to occur, VA would incur the expense of notifying and offering credit protection services to individuals whose information was involved. VA could also lose credibility with veterans who trust that their sensitive personal information is being appropriately secured.

The OIG team found that veterans' sensitive personal information was left unprotected on two shared network drives, where it was accessible to VSO officers who did not represent those veterans. Senior Office of Information and Technology (OIT) representatives told the team that other authenticated network users with access to the shared drives also could have accessed that information regardless of their business need. The OIG determined that mishandling this sensitive personal information was a national issue because the problem was not limited to the Milwaukee VARO. Authorized users, regardless of their location, who remotely connected to VA's network could have had access to the same shared network drives.

The reasons for the mishandling of sensitive personal information included the following:

- Certain users were knowingly or inadvertently negligent in their use of shared network drives to store veterans' sensitive data despite VA security policy prohibiting such activity.
- No technical controls were in place to prevent negligent users from storing sensitive personal information on the shared network drives.
- The lack of oversight by OIT and Veterans Benefits Administration (VBA) personnel resulted in failures to discover and remove any sensitive personal information stored on shared network drives.

The OIG recommended that the Assistant Secretary for Information and Technology and the Under Secretary for Benefits provide remedial training to users on the safe handling and storage of veterans' sensitive personal information on network drives. The OIG also recommended that OIT establish technical controls to ensure users cannot store veterans' sensitive personal information on shared network drives and implement improved oversight procedures, including facility-specific procedures, to ensure veterans' sensitive personal information is not being stored on shared network drives.

The Assistant Secretary for Information and Technology and the Under Secretary for Benefits concurred with all three recommendations and provided corrective action plans that are responsive to the recommendations. The OIG will monitor progress until all proposed actions are completed.

Security and Access Controls for the Beneficiary Fiduciary Field System Need Improvement[11] The OIG conducted an audit to determine if the Beneficiary Fiduciary Field System (BFFS) had the necessary controls to protect data integrity and safeguard protected, personal fiduciary and beneficiary information.[12] VBA deployed BFFS in May 2014 to replace the aging Fiduciary Beneficiary System and manage data on beneficiaries, including names, mailing addresses, social security numbers, medical record information, and financial information. BFFS also stores information on fiduciaries—individuals appointed to manage veterans' finances.[13]

---

[9] Mishandling of Veterans' Sensitive Personal Information on VA Shared Network Drives, October 17, 2019.

[10] Federal laws require appropriate administrative, physical, and technical safeguards to protect personal information and limit the uses and disclosures of that information without the individual's authorization. VA policy requires VA information system users who access sensitive personal information as part of their official duties to avoid its unauthorized disclosure and prohibits other users from accessing the information without a business need.

[11] Security and Access Controls for the Beneficiary Fiduciary Field System Need Improvement, September 12, 2019.

[12] BFFS is the information technology system used to manage the caseload for VA's Fiduciary Program. The Fiduciary Program manages payments for veterans and other beneficiaries who, due to injury, disease, or age, are unable to manage their financial affairs and are thus vulnerable to fraud or abuse.

[13] The fiduciary information stored includes credit and criminal histories.

The OIG audit assessed system controls related to security management, user access, and the separation of duties within the system.

The OIG team found that OIT inappropriately set the security risk level for BFFS at moderate instead of high. This happened because risk managers did not follow established standards and did not consider the existence of protected health information (PHI) and PII stored in the system's data base. The lower risk level reduced the system's security and access controls and potentially jeopardized the confidentiality, integrity, and availability of sensitive information related to beneficiaries and fiduciaries. The OIG team also found that some system users could access records not needed to perform their duties. More than 1,600 fiduciary hub personnel have nationwide access to BFFS data.[14] This is far beyond the number needed to address those limited instances in which information must be shared between hubs. Moreover, VBA does not have a process for reviewing these employees' access privileges. As a result, hub personnel can view records regardless of the physical location of beneficiaries and fiduciaries, which violates access requirements and increases the risk that beneficiary or fiduciary information could be misused. Additionally, VBA officials did not enable audit logs for all records and fields within BFFS out of concern that it would reduce the system's functionality. However, when combined with a user's ability to access records nationwide, this creates an unnecessary risk that unauthorized access to beneficiary PII, PHI, and other sensitive information will go undetected.

The OIG made four recommendations to improve the BFFS security and access controls to protect data integrity and safeguard protected, personal fiduciary and beneficiary information. Recommendations included reevaluating the risk determination for BFFS, improving controls over end users' access levels, fully enabling audit logs to ensure VBA can accurately and comprehensively track access to records within BFFS, and improving separation of duties for VA users. OIT and VBA concurred with the recommendations, and the OIG will monitor progress until all proposed actions are completed.

VA's Management of Mobile Devices Generally Met Information Security Standards[15] The OIG conducted an audit to determine whether OIT is implementing policies and procedures to mitigate information security weaknesses associated with mobile devices being used in VA's network infrastructure. OIT manages over 50,000 mobile devices that store, process, and transmit veterans' information, and therefore require protection at all times.

The OIG team found OIT's security practices for mobile devices generally mitigated security control weaknesses within VA's network infrastructure. However, the OIG team identified vulnerabilities associated with configuration management. Specifically, OIT did not enforce blacklisting, a process used to prevent the execution of malicious, vulnerable, or flawed applications. Because OIT has not implemented blacklisting, users can download applications that are not authorized on VA mobile devices, which increases the risk of lost VA data. Additionally, the OIG found that OIT did not validate adequate mobile device security training by users, effectively monitor installed applications, or control the automation of updates for its mobile devices.

The OIG made three recommendations to the Assistant Secretary for Information and Technology to mitigate information security weaknesses associated with mobile devices being used in VA's network infrastructure. Recommendations included enforcing blacklisting or formally assessing and documenting the approach of using training as the mitigating control, using configuration management tools to prevent premature or late updating, and validating that users are completing the required annual mobile device training. OIT concurred with all three recommendations and provided responsive corrective action plans, which OIG staff will monitor until successfully completed.

ONGOING OVERSIGHT INITIATIVES

By continuing to identify lapses, make recommendations, and monitor implementation of corrective action plans, the OIG's goal is to help VA strengthen areas of IT security that will more effectively safeguard veterans' personal information and secure their benefits. The OIG has planned and ongoing work that will provide additional oversight of VA's efforts.

The OIG is currently working on the Fiscal Year 2019 FISMA assessment to determine VA's compliance and expects to release the results in the Spring of 2020.

---

[14] The Fiduciary Program operates from six geographical hubs spread around the country.

[15] VA's Management of Mobile Devices Generally Met Information Security Standards, October 22, 2019.

This annual audit evaluates select management, technical, and operational controls supporting 49 major applications and general support systems hosted at 25 VA facilities, including VA's four major data centers. As previously discussed, the Fiscal Year 2018 FISMA audit showed that VA is making progress in some areas, however challenges remain in implementing components of its agencywide information security risk management program that will meet FISMA requirements.

OIG auditors are also conducting work to determine whether VA has implemented key elements of the Federal Information Technology Acquisition Reform Act (FITARA) regarding Chief Information Officer (CIO) Authority Enhancements (Section 831). FITARA was enacted by Congress in 2014 to modernize and strengthen Federal IT acquisitions and operations, significantly reduce wasteful spending, and improve project outcomes. Specifically, this audit evaluates the extent to which the CIO met requirements to (1) review and approve all IT asset and service acquisitions across the VA enterprise and (2) participate in VA's IT planning, programming, budgeting, and execution, including governance, oversight, and reporting.

Furthermore, the OIG is monitoring facets of VA's Electronic Health Record Modernization project, implementation of the MISSION Act, and other IT initiatives that will require substantial planning and resources to ensure they are properly protected and secured. As VA moves forward with these projects, the OIG will track the progress made and determine the most efficient and useful ways to oversee and report on VA's ongoing work.

CONCLUSION

VA's fundamental mission of providing benefits and services to veterans is dependent on deploying secure IT systems and networks. VA's information security program and its practices must protect the confidentiality, integrity, and availability of VA systems and data. The recurrence of IT security problems indicates the need for vigilance. Until proven processes are in place to ensure adequate controls across the enterprise, the IT material weakness will persist—putting VA's mission-critical systems and sensitive veterans' data at risk. While VA has made recent improvements in some aspects of information management, there continue to be considerable challenges. The OIG believes that VA's successful implementation of open recommendations from oversight reports is an important first step in its efforts to address ongoing and emerging issues.

Madam Chair, this concludes my statement. We would be happy to answer any questions you or other members of the Subcommittee may have.

Prepared Statement of Greg Wilshusen

United States Government Accountability Office

GAO

Before the Subcommittee on Technology Modernization, Committee on Veterans' Affairs, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Thursday, November 14, 2019

INFORMATION SECURITY

VA and Other Federal Agencies Need to Address Significant Challenges

Statement of Gregory C. Wilshusen,
Director, Information Security Issues

Chair Lee, Ranking Member Banks, and Members of the Subcommittee

Thank you for the opportunity to testify at today's hearing on cybersecurity challenges and cyber risk management at the Department of Veterans Affairs (VA). As you know, federal agencies, including VA, rely extensively on information technology (IT) to carry out their operations and deliver services to constituents.

Safeguarding federal computer systems has been a longstanding concern. This year marks the 22nd anniversary of GAO's first designation of information security as a government-wide high-risk area in 1997.[1] We expanded this high-risk area to include safeguarding the systems supporting our nation's critical infrastructure in 2003, protecting the privacy of personally identifiable information in 2015, and establishing a comprehensive cybersecurity strategy and performing effective oversight in 2018.[2] Most recently, we identified federal information security as a government-wide high-risk area in our March 2019 high-risk update.[3]

As we agreed, my statement provides an overview of the status of cybersecurity across the federal government in general and at VA in particular. This includes a discussion of the IT security challenges that the department faces as it modernizes and secures its information systems. In developing this testimony, we reviewed our prior reports,[4] as well as

[1]GAO, *High-Risk Series: An Overview*, GAO-HR-97-1 (Washington, D.C.: February 1997) and GAO, *High-Risk Series: Information Management and Technology*, GAO-HR-97-9 (Washington, D.C.: February 1997).

[2]GAO, *High-Risk Series: Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures*, GAO-03-121 (Washington, D.C.: January 2003); *High-Risk Series: An Update*, GAO-15-290 (Washington, D.C.: February 11, 2015); and *High-Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: September 6, 2018).

[3]GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP (Washington, D.C.: March 6, 2019).

[4]See, for example, GAO, *Federal Information Security: Agencies and OMB Need to Strengthen Policies and Practices*, GAO-19-545 (Washington, D.C.: July 26, 2019); *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384 (Washington, D.C.: July 25, 2019); *Cybersecurity Workforce: Agencies Need to Accurately Categorize Positions to Effectively Identify Critical Staffing Needs*, GAO-19-144 (Washington, D.C: March 12, 2019); *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T (Washington, D.C.: July 12, 2018); *Information Security: VA Needs to Improve Controls over Selected High-Impact Systems*, GAO-16-691SU (Washington, D.C.: September 30, 2016); and *Information Security: Agencies Need to Improve Controls over Selected High-Impact Systems*, GAO-16-501 (Washington, D.C.: May 18, 2016).

relevant Office of Management and Budget (OMB), inspector general (IG), and agency reports. A more detailed discussion of the objectives, scope, and methodology for this work is included in each of the reports that are cited throughout this statement.

The work on which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

VA's mission is to promote the health, welfare, and dignity of all veterans by ensuring that they receive medical care, benefits, social support, and lasting memorials. In providing health care and other benefits to veterans and their dependents, VA relies extensively on IT systems and networks to receive, process, and maintain sensitive data, including veterans' medical records and other personally identifiable information. Accordingly, effective information security controls based on federal guidance and requirements are essential to ensure that the department's systems and information are adequately protected from loss, unauthorized disclosure, inadvertent or deliberate misuse, or improper modification, and are available when needed.

Implementing an effective information security program and controls is particularly important for VA since it uses IT systems and electronic information to perform essential activities for veterans, such as providing primary and specialized health care services, medical research, disability compensation, educational opportunities, assistance with home ownership, and burial and memorial benefits. The corruption, denial, or delay of these services due to compromised IT systems and electronic information can create undue hardship for veterans and their dependents.

Federal Law and Policy Set Requirements for Securing Federal Systems and Information

The *Federal Information Security Modernization Act of 2014* (FISMA) requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of the information and information systems used by or on behalf of the agency. The act also requires federal agencies to develop, document, and implement an agency-wide information security program to provide security for the information and information systems supporting

their operations and assets by implementing policies and procedures intended to cost-effectively reduce risks to an acceptable level.[5]

In May 2017, the president signed Executive Order 13800 on strengthening the cybersecurity of federal networks and critical infrastructure.[6] The order sets policy for managing cybersecurity risk and directs each executive branch agency to use the National Institute of Standards and Technology's (NIST) cybersecurity framework to manage those risks.[7]

The NIST cybersecurity framework identifies specific activities and controls for achieving five core security functions:

- **Identify:** Develop an understanding of the organization's ability to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity incident.

According to NIST, these five functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

[5]The *Federal Information Security Modernization Act of 2014* (Pub. L. No. 113-283, Dec. 18, 2014) largely superseded the *Federal Information Security Management Act of 2002* (FISMA 2002), enacted as Title III, E-Government Act of 2002, Pub. L. No. 107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002). As used in this statement, FISMA refers to the new requirements in FISMA 2014, and to other relevant FISMA 2002 requirements that were unchanged by FISMA 2014 and continue in full force and effect.

[6]White House, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Executive Order 13800 (Washington, D.C.: May 11, 2017).

[7]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Gaithersburg, MD: Apr. 16, 2018).

The 23 Civilian CFO Act Agencies Have Spent Billions on Cybersecurity Activities

In fiscal year 2018, the 23 civilian agencies covered by the *Chief Financial Officers Act of 1990* (CFO Act),[8] including VA, reported spending over $6.5 billion on IT security- or cybersecurity-related activities. The 23 civilian agencies individually reported spending between $9 million and almost $1.9 billion on these activities.[9] Collectively, these 23 agencies spent on average about 14 percent of their total IT expenditures on cybersecurity-related activities. VA reported spending about $386 million on cybersecurity, which represented about 8 percent of its total IT expenditures.[10]

[8]The 23 civilian *Chief Financial Officers Act of 1990* (CFO Act) are the Departments of Agriculture, Commerce, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs; the Environmental Protection Agency; General Services Administration; National Aeronautics and Space Administration; National Science Foundation; Nuclear Regulation Commission; Office of Personnel Management; Small Business Administration; Social Security Administration; and the U.S. Agency for International Development. In addition to the 23 civilian CFO Act agencies, the Department of Defense is the 24th agency covered by the CFO Act.

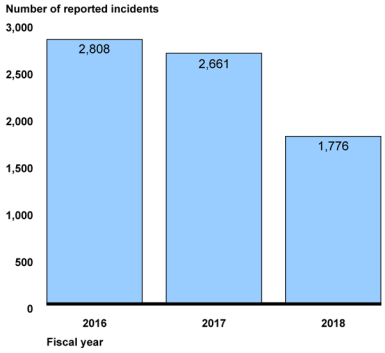
[9]According to the President's budget request for fiscal year 2020, the agency-reported cybersecurity spending may include cybersecurity-related spending that was not dedicated to the protection of their networks. Instead, the amounts reported may represent spending for the broader cybersecurity mission of the agency.

[10]See GAO-19-545.

Federal Agencies Continue to Report Large Numbers of Security Incidents, Although VA Has Reported Fewer Incidents In Recent Years

In fiscal year 2018, federal agencies continued to report large numbers of information security incidents. As we previously noted,[11] federal agencies reported over 30,000 security incidents during each of the last three fiscal years. Specifically, agencies reported a total of 30,899, 35,277, and 31,107 information security incidents in fiscal years 2016, 2017, and 2018, respectively. During those same periods of time, VA reported an average of 2,415 incidents annually, although the number of reported incidents steadily decreased from 2,808 to 1,776, as shown in figure 1.[12]

Figure 1: Information Security Incidents Reported by the Department of Veterans Affairs, Fiscal Years 2016 through 2018



Source: GAO analysis of Office of Management and Budget data. | GAO-20-256T

In fiscal year 2018, VA reported 1,776 incidents involving several threat vectors.[13] These threat vectors included web-based attacks, phishing

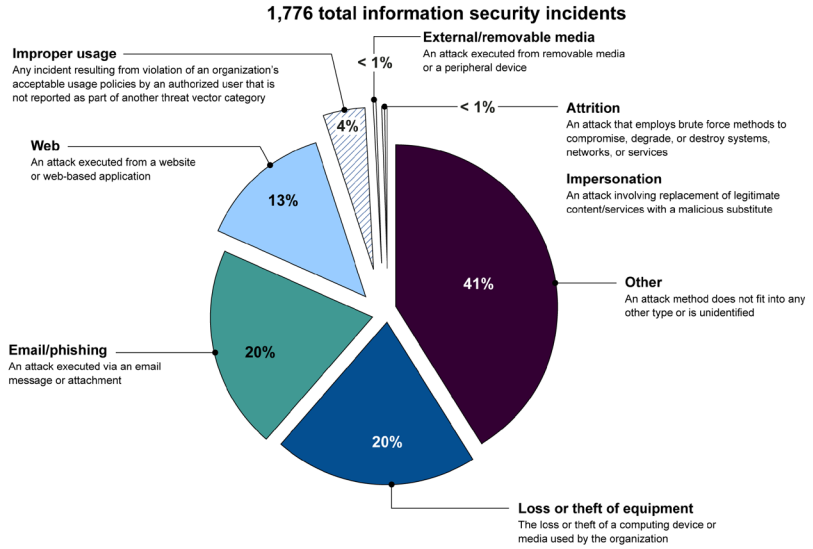
[11]GAO-19-545.

[12]Office of Management and Budget, *Federal Information Security Modernization Act of 2014 Annual Report to Congress* (Washington, D.C.: June 28, 2019).

[13]A threat vector (or avenue of attack) specifies the conduit or means used by the source or attacker to initiate a cyber attack or incident.

attacks,[14] and the loss or theft of computer equipment, among others. Figure 2 provides a breakdown of information security incidents, by threat vector, reported by VA in fiscal year 2018.

Figure 2: Department of Veterans Affairs Information Security Incidents by Threat Vector Category, Fiscal Year 2018



Source: GAO analysis of Office of Management and Budget data for fiscal year 2018. | GAO-20-256T

[14]Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information.

Perhaps most concerning of the incidents reported by VA is the relatively large percentage of incidents (41 percent) for which VA identified "Other" as the threat vector. Government-wide, agencies identified approximately 27 percent of their incidents in the "Other" category in fiscal year 2018. A large percentage of these incidents may indicate a lack of agency awareness and ability to investigate and catalog incidents.

Federal Agencies, Including VA, Continue to Have Deficient Information Security Programs

FISMA requires IGs to determine the effectiveness of their respective agency's information security programs. To do so, OMB instructed IGs to provide a maturity rating for agency information security policies, procedures, and practices related to the five core security functions—*identify, protect, detect, respond, and recover*—established in the NIST cybersecurity framework, as well as for the agency-wide information security program.

The ratings used to evaluate the effectiveness of agency information security programs are based on a five-level maturity model, as described in table 1.

Table 1: Inspector General Reporting Metrics Maturity Model

Maturity level	Description
Level 1: Ad hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented, but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess those policies procedures, and strategies, and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: GAO analysis of Fiscal Year 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, Version 1.0.1, May 24, 2018. | GAO-20-256T

According to this maturity model, Level 4 (managed and measurable) represents an effective level of security.[15] Therefore, if an IG rates the agency's information security program at Level 4 or Level 5, then that agency is considered to have an effective information security program.

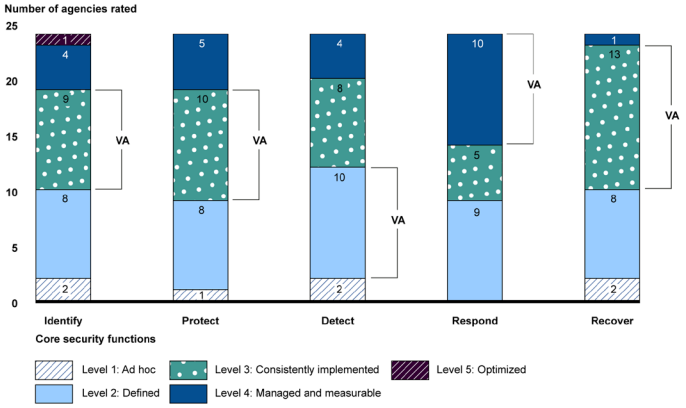
VA was one of 18 CFO Act agencies where the IG determined that the agency-wide information security program was not effectively implemented during fiscal year 2018. The VA IG also determined the department's maturity level for each of the five core security functions:

- Level 2 (defined) for the *Detect* function;
- Level 3 (consistently implemented) for the *Identify, Protect,* and *Recover* functions; and
- Level 4 (managed and measurable) for the *Respond* function.

As shown in figure 3, VA's ratings were generally consistent with the maturity level ratings of other CFO Act agencies.

[15]The National Institute of Standards and Technology defines security control effectiveness as the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements for the information system and are in compliance with established security policies.

Figure 3: Maturity Level Ratings for the Cybersecurity Framework Core Security Functions for 24 Major Agencies, including the Department of Veterans Affairs (VA), for Fiscal Year 2018



Source: GAO analysis of agency fiscal year 2018 *Federal Information Security Modernization Act of 2014* (FISMA) reports and the Office of Management and Budget's *Fiscal Year 2018 Annual FISMA Report to Congress.* | GAO-20-256T

Most CFO Act Agencies, Including VA, Had Significant Security Control Deficiencies over Their Financial Reporting

Agency IGs or independent auditors assess the effectiveness of information security controls as part of the annual audits of the agencies' financial statements. The reports resulting from these audits include a description of information security control deficiencies related to the five major general control categories defined by the *Federal Information System Controls Audit Manual* (FISCAM):[16]

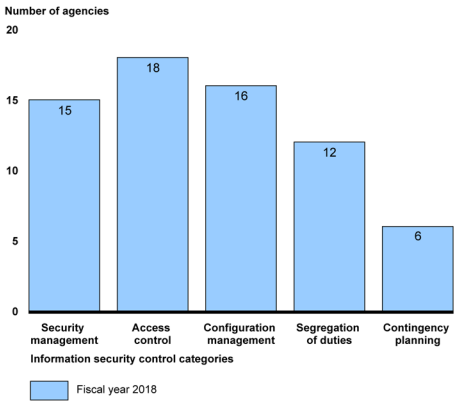
- **security management controls** that provide a framework for ensuring that risks are understood and that effective controls are selected, implemented, and operating as intended;

[16]FISCAM is GAO's audit methodology for performing information system control audits in accordance with generally accepted government auditing standards. See GAO, *Federal Information System Controls Audit Manual* (FISCAM), GAO-09-232G (Washington, D.C.: February 2009).

- **access controls** that limit or detect access to computer resources, thereby protecting them against unauthorized modification, loss, and disclosure;
- **configuration management controls** that prevent unauthorized changes to information system resources and assure that software is current and known vulnerabilities are patched;
- **segregation of duties controls** that prevent an individual from controlling all critical stages of a process by splitting responsibilities between two or more organizational groups; and
- **contingency planning controls** that help avoid significant disruptions in computer-dependent operations.

For fiscal year 2018, most of the 24 CFO Act agencies had deficiencies in most of the control categories, as illustrated in figure 4. VA's IG reported deficiencies in each of these categories for the department.

Figure 4: Number of 24 Chief Financial Officers Act of 1990 Agencies Reporting Deficiencies in Information Security Control Categories for Fiscal Year 2018



Source: GAO analysis of agency financial reports for fiscal year 2018. | GAO-20-256T

As a result of these deficiencies, the IGs at 18 of the 24 CFO Act agencies designated information security as either a material weakness (six agencies, including VA) or significant deficiency (12 agencies) in internal control over financial reporting for their agency.[17] For VA, fiscal year 2018 was the 17th year in a row that the department had reported a material weakness in information security. In addition, IGs at 21 of the 24 agencies, including VA, cited information security as a major management challenge for their agency for fiscal year 2018.

Most Civilian CFO Act Agencies, Including VA, Have Reported Meeting Many Cybersecurity Implementation Targets

The administration has developed key milestones and performance metrics for agency chief information officers (CIO) to use to assess their agency's progress toward achieving outcomes that strengthen federal cybersecurity. The milestones and metrics have specific implementation targets, most of which are expected to be met by the end of fiscal year 2020.

As of fiscal year 2018, most civilian CFO Act agencies, including VA, had reported meeting most of the implementation targets for that year.[18] VA reported meeting six of 10 targets. Table 2 shows the number of agencies meeting their targets as of fiscal year 2018, as well as VA's status in doing so.

[17]A material weakness is a deficiency, or combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of an entity's financial statement will not be prevented, or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those charged with governance. A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis.

[18]We did not include the Department of Defense because the data was not publicly available.

Table 2: Number of 23 Civilian Chief Financial Officers Act of 1990 Agencies Meeting Targets for 10 Key Milestones, along with the Department of Veterans Affairs' Status, for Fiscal Year 2018

Key milestone	Performance Metric & Target	Number of agencies reported meeting targets	VA status
Software asset management	95% of software assets are covered by a whitelisting capability.[a]	10	Not met
Hardware asset management	95% of hardware assets are covered by a capability to detect and alert upon the connection of an unauthorized hardware asset.	16	Not met
Authorization management	100% of high and moderate impact systems are covered by a valid security authorization to operate.	14	Not met
Mobile device management	95% of mobile devices are covered by a capability to remotely wipe contents if the device is lost or compromised.	19	Met
Privileged network access management	100% of privileged users are required to use a Personal Identity Verification (PIV) card[b] or Authenticator Assurance Level 3[c] (AAL3) multifactor authentication method to access the agency's network.	18	Met
High-value asset access management	90% of high-value assets require all users to authenticate using a PIV card or AAL3 multifactor authentication method.	14	Met
Automated access management	95% of users are covered by an automated, dynamic access management solution that centrally tracks access and privilege levels.	15	Not met
Intrusion detection and prevention	At least 4 of 6 intrusion prevention metrics have met an implementation target of at least 90% and 100% of email traffic is analyzed using email authentication protocols that prevent malicious actors from sending false emails claiming to originate from a legitimate source.	8	Met
Exfiltration and enhanced defenses	At least 3 of 4 exfiltration and enhanced defenses metrics have met an implementation target of at least 90%.	23	Met
Data protection	At least 4 of 6 data protection metrics have met an implementation target of at least 90%.	16	Met

Source: GAO analysis of Fiscal Year 2018 Chief Information Officer Federal Information Security Modernization Act of 2014 Reporting Metrics | GAO-20-256T

[a]Whitelisting is a process used to identify (1)software programs that are authorized to execute on an information system or (2) authorized websites.

[b]A Personal Identity Verification card is a physical artifact that contains stored identity credentials for the person it was issued to, so that the identity of the individual can be verified against the stored credentials by another person or an automated process.

[c]Authenticator Assurance Level 3 uses a hardware-based authenticator and an authenticator that provides verifier impersonation resistance.

VA Faces Key Security Challenges As It Modernizes and Secures Its Information Systems

In several reports issued since fiscal year 2016, we described deficiencies related to key challenges that VA has faced in safeguarding its information and information systems. The challenges we reported related to effectively implementing information security controls; mitigating known security deficiencies; establishing elements of its cybersecurity risk management program; and identifying critical cybersecurity staffing needs. Our work stresses the need for VA to address these challenges as well as manage IT supply chain risks as it modernizes and secures its information systems.

Effectively Implementing Information Security Controls

VA has been challenged to effectively implement security controls over its information and information systems. As previously mentioned in this statement, the VA IG reported that the department did not have an effective information security program and has had deficient information security controls over its financial systems. The weaknesses described by the IG are consistent with the control deficiencies we identified during an examination of VA's high-impact systems[19] that we reported on in 2016.[20] In those reports, we described deficiencies in VA's implementation of access controls, patch management, and contingency planning. These deficiencies existed, in part, because the department had not effectively implemented key elements of its information security program. Until VA rectifies reported shortcomings in its agency-wide information security program, it will continue to have limited assurance that its sensitive information and information systems are sufficiently safeguarded.

Adequately Mitigating Known Security Deficiencies

VA has not consistently mitigated known security deficiencies in a timely manner. As mentioned earlier, VA has reported a material weakness in information security for financial reporting purposes for 17 consecutive years. In fiscal year 2016, we recommended 74 actions for the department to take to improve its cybersecurity program and remedy

[19]High-impact systems are those systems where the loss of confidentiality, integrity, or availability of the systems or the information they contain can have a severe or catastrophic adverse effect on an organization's operations, assets, or individuals. Such an impact can result in loss or degradation of mission capability, severe harm to individuals, or major financial loss.

[20]GAO-16-501 and GAO-16-691SU.

known control deficiencies with selected high-impact systems.[21] However, as of October 2019, over 3 years later, VA had implemented only 32 (or 43 percent) of the 74 recommendations. One of the remaining unimplemented recommendations calls for the department to consistently and comprehensively perform security control assessments. This recommended activity is an important element of a cybersecurity program and helps to provide assurance that controls are operating as intended and to detect controls that are not functioning correctly.

VA has also been challenged in assuring that its actions to mitigate vulnerabilities and implement recommended improvements are effective. The department has asserted that it had implemented 39 of the 42 remaining open recommendations from our fiscal year 2016 reports. However, the evidence VA provided was insufficient to demonstrate that it had fully implemented the recommendations. The department subsequently provided additional evidence, which was also insufficient, indicating that its remedial action process was not validating the effectiveness of actions taken to resolve known deficiencies. Until VA adequately mitigates security control deficiencies, the sensitive data maintained on its systems will remain at increased risk of unauthorized modification and disclosure, and the systems will remain at risk of disruption.

Fully Establishing Elements of a Cybersecurity Risk Management Program

VA has been challenged in managing its cybersecurity risk. In July 2019, we reported that the department had fully met only one of the five foundational practices for establishing a cybersecurity risk management program.[22] Although VA established the role of a cybersecurity risk executive, the department had not fully:

- developed a cybersecurity risk management strategy that addressed key elements, such as risk tolerance and risk mitigation strategies;

[21]We issued five recommendations in the publicly available report, and an additional 69 recommendations in a separate report with limited distribution that we provided directly to VA. The accompanying report included recommendations to address weaknesses identified related to access control, patch management, and contingency planning. (GAO-16-501 and GAO-16-691SU respectively).

[22]GAO-19-384.

- documented risk-based policies that required the department to perform agency-wide risk assessments;
- conducted an agency-wide cybersecurity risk assessment to identify, assess, and manage potential enterprise risks; or
- established coordination between cybersecurity and enterprise risk management.

VA concurred with our four recommendations to address these deficiencies and asserted that it is acting to do so. Nevertheless, until VA fully establishes a cybersecurity risk management program, its ability to convey acceptable limits regarding the selection and implementation of controls within the established organizational risk tolerance will be diminished.

Identifying Critical Cybersecurity Staffing Needs

VA has been challenged to accurately identify the work roles of its workforce positions that perform IT, cybersecurity, or cyber-related functions—a key step in identifying its critical cybersecurity staffing needs. In March 2019, we reported that the department had likely miscategorized the work roles of many of these positions in its personnel system.[23] Specifically, VA had reported that 3,008 (or 45 percent) of its 6,636 positions in the 2210 IT management occupational series—positions that most likely performed IT, cybersecurity, and cyber-related functions—were not performing these functions.[24]

VA concurred with our recommendation to review the work roles for positions in the 2210 IT management occupational series and assign the appropriate work roles, and stated that it had begun to do so. Nevertheless, until VA completely and accurately categorizes the work roles of its workforce positions performing IT, cybersecurity, and cyber-related functions, the reliability of the information needed to improve workforce planning will be diminished and its ability to effectively identify critical staffing needs will be impaired.

[23]GAO-19-144.

[24]The 2210 IT management occupational series covers positions that manage, supervise, lead, administer, develop, deliver, and support information technology systems and services.

Managing IT Supply Chain Risks as Part of IT Modernization Programs

Assessing and managing supply chain risks are important considerations for agencies, including VA, when operating and modernizing IT systems. In July 2018, we reported that reliance on a global IT supply chain introduces risks to federal information systems.[25] We noted that supply chain threats are present during various phases of a system's development life cycle and we identified the following threats:

- Installation of malicious or intentionally harmful hardware or software;
- Installation of counterfeit hardware or software;
- Failure or disruption in the production or distribution of critical products;
- Reliance on a malicious or unqualified service provider; and
- Installation of hardware or software that contains unintentional vulnerabilities, such as defects in code that can be exploited.

These threats can have a range of impacts, including allowing adversaries to take control of systems or decreasing the availability of materials or services needed to develop systems.

Accordingly, agencies such as VA need to take appropriate measures to assess and manage IT supply chain risks as they operate and modernize their information systems. Failure to do so could result in data loss, modification, or exfiltration; loss of system availability; and a persistent negative impact on the agency's mission.

In summary, similar to other federal agencies, VA continues to be challenged in implementing an effective agency-wide program and controls for securing its information and information systems. As VA pursues efforts to modernize and secure its IT systems, it will need to successfully address multiple challenges in order to achieve effective outcomes.

[25]GAO-18-667T.

Chair Lee, Ranking Member Banks, and Members of the Subcommittee, this completes my written statement. I would be pleased to answer your questions.

GAO Contact and Staff Acknowledgments

If you or your staff members have any questions concerning this testimony, please contact me at (202) 512-6244 or wilshuseng@gao.gov.

Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this statement. Other individuals who made key contributions to this testimony include Jeffrey Knott (Assistant Director), Di'Mond Spencer (Analyst-in-Charge), Chris Businsky, Nancy Glover, Franklin Jackson, and Daniel Swartz. Also contributing were Melina Asencio, Scott Pettis, and Zsaroq Powe.

GAO's Mission	The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.
Obtaining Copies of GAO Reports and Testimony	The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.
Order by Phone	The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm. Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537. Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.
Connect with GAO	Connect with GAO on Facebook, Flickr, Twitter, and YouTube. Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts. Visit GAO on the web at https://www.gao.gov.
To Report Fraud, Waste, and Abuse in Federal Programs	Contact FraudNet: Website: https://www.gao.gov/fraudnet/fraudnet.htm Automated answering system: (800) 424-5454 or (202) 512-7700
Congressional Relations	Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548
Public Affairs	Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800 U.S. Government Accountability Office, 441 G Street NW, Room 7149 Washington, DC 20548
Strategic Planning and External Liaison	James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707 U.S. Government Accountability Office, 441 G Street NW, Room 7814, Washington, DC 20548