DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

STATEMENT OF BRENT ARRONTE
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDITS AND EVALUATIONS
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
COMMITTEE ON VETERANS' AFFAIRS
UNITED STATES HOUSE OF REPRESENTATIVES
HEARING ON
MAPPING THE CHALLENGES AND PROGRESS OF THE
OFFICE OF INFORMATION AND TECHNOLOGY
APRIL 2, 2019

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 Office of Information and Technology (OIT). Our statement will focus on the effectiveness of VA's information security program, the progress made, and challenges VA continues to face in developing the information technology (IT) systems needed to effectively carry out their mission. We base our conclusions on OIG reports on VA's information security program and our ongoing oversight of IT systems development and management. I am accompanied by Mr. Michael Bowman, Director of the OIG's Information Technology and Security Audits Division.

BACKGROUND

Since 2000, the OIG has identified information management as a major management challenge because VA has a history of not properly planning and managing its critical IT investments. [1]

For fiscal year (FY) 2020, VA requested a total IT investment of $4.3 billion to fund information system security, system development initiatives, and system operations and maintenance.

IT systems and networks are critical to VA in carrying out its mission of providing medical care and a range of benefits and services to veterans and their families. Ensuring the secure operation of these systems and networks is essential given 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

[1] *Office of Inspector General 2018 Major Management Challenges,* November 2018.

operations, or launch attacks against other VA systems. VA has previously reported security incidents in which sensitive information, including personally identifiable information, has been lost or stolen, potentially exposing millions of veterans and their families to the loss of privacy, identity theft, and other financial crimes.[2]

MAJOR CHALLENGES FACING OIT

OIG audits have consistently shown that IT systems development is a challenge for VA. Projects are susceptible to cost overruns, schedule slippages, performance problems, and in some cases, complete failure. The OIG has identified significant control deficiencies in the IT areas of security, project management, and system development that are discussed in more detail below. By continuing to identify deficiencies, make recommendations, and oversee implementation plans, the OIG's goal is to help VA:

- Strengthen areas of IT security weakness to effectively safeguard veterans' personal information and benefits.
- Properly plan and manage IT projects to deliver a timely and cost-effective product that adequately satisfies the needs of VA staff.

IT Security

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 be designed to protect the confidentiality, integrity, and availability of VA systems and data.

Federal Information Security Management Act of 2002 Audit. 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. In FY 2018, the OIG's contractors completed audits to review the extent to which VA had appropriate IT safeguards in place. [3] The audit concluded that VA has made progress producing, documenting, and distributing policies and procedures as part of its program. However, VA continues to face hurdles implementing components of its agencywide information security risk management program to meet FISMA requirements.

Significant deficiencies persist related to system access controls, system configuration management controls, system hardware and software change management controls, as well as system disaster recovery practices designed to protect mission-critical systems from unauthorized access, alteration, or destruction. To address these deficiencies, VA must prioritize remediation of these security weaknesses, as ongoing delays in implementing effective corrective actions may contribute to the continued reporting of an information technology material

[2] *Review of Issues Related to the Loss of VA Information Involving the Identity of Millions of Veterans*, July 11, 2006.
[3] *Federal Information Security Modernization Act Audit for Fiscal Year 2018*, March 12, 2019.

weakness in VA’s financial statements. The FY 2018 FISMA report contained 28 recommendations to the Assistant Secretary for Information and Technology for improving VA’s information security program. These recommendations focused on improving the following security domains:

- System access controls to include password standards and user account reviews
- System configuration management controls to include timely system security updates
- Information security management controls such as consistently updating Plans of Action and Milestones and System Security Plans
- System disaster recovery practices for critical systems

The Principal Deputy Assistant Secretary for Information and Technology concurred with 25 of 28 recommendations and provided acceptable action plans. 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 FY 2019 FISMA audit.

Use of Unauthorized Databases. The OIG conducted a review in response to anonymously reported allegations that the VA Long Beach Healthcare System (the system) in California was maintaining an unauthorized Microsoft Access database, the unauthorized database hosted Sensitive Personal Information (SPI), and all of the Veterans Health Administration’s 24 Spinal Cord Injury Centers had access to the database through a Microsoft SharePoint intranet portal.[4] The complaint also stated that unsecured veteran SPI was stored on a server outside of VA’s protected network environment. The OIG substantiated the allegation related to the unauthorized database at the system. Consistent with the allegation, the OIG found multiple instances of databases that hosted SPI in violation of VA policy. The OIG also substantiated that veteran SPI was hosted on an external server, located at the University of Southern California, without a formal Data Use Agreement authorizing such activity. In addition, the review team noted this server could be accessed from the internet using default logon credentials. The OIG recommended the Under Secretary for Health ensure that the Spinal Cord Injury and Disorders program staff comply with VA’s Privacy Program and information security requirements for all sensitive veteran data collected, the Executive Director for the National Spinal Cord Injury Program Office discontinue storing SPI in unauthorized Microsoft Access databases, and the Acting Assistant Secretary for Information and Technology ensure that Field Security Services and VA’s Privacy Service implement improved procedures to identify unauthorized uses of SPI and take appropriate corrective actions. The three responsible offices concurred with the recommendations. VA provided corrective action plans that were responsive to the recommendations. Based upon our review of VA’s corrective actions, the OIG has closed all report recommendations.

[4] *Review of Alleged Unsecured Patient Database at the VA Long Beach Healthcare System*, March 28, 2018.

IT Project Management and System Development

VA must continue to invest in and improve IT project management and system development so that future initiatives and major projects can experience more efficient and seamless rollouts. To the extent that VA does not properly plan and manage these IT investments, they risk overrunning projected costs and delivering products that do not consistently align with user requirements.

Real Time Location System Review. The OIG conducted a review based on concerns of contract mismanagement involving the development and implementation of the Real Time Location System (RTLS), a product that uses multiple technologies for locating and tracking medical equipment.[5] At the time of the review, VA was in the process of deploying RTLS at all medical facilities nationwide. The team determined that management failed to comply with VA policy and guidance when it deployed RTLS assets without appropriate project oversight. Specifically, the OIG concluded the RTLS Project Management Office (PMO) did not follow guidance to use an incremental project management approach during the acquisition and deployment of RTLS assets to compensate for numerous known project management risks. Consequently, the RTLS PMO did not ensure the vendor could meet contracted functionality requirements on the initial $7.5 million task order, such as accurate asset tracking, before ultimately committing a total of $431 million to the same vendor for further RTLS deployments. The OIG reported that management failed to provide effective oversight of the RTLS project from acquisition through development and implementation to ensure the product was successfully deployed.

The OIG also reported that VA deployed RTLS assets without meeting VA's information security requirements. Specifically, RTLS assets were deployed without the appropriate system authorizations needed to connect such devices to VA's network. This inadequate oversight of RTLS risk management activities left VA mission-critical systems and data susceptible to unauthorized access, loss, or disclosure. Consequently, VA's internal network faced unnecessary risks resulting from untested RTLS system security controls. In response to the OIG's findings, the Acting Assistant Secretary reported that OIT will conduct risk assessments prior to future deployments and will enforce the use of incremental project management to ensure an adequate return on investment. VA provided corrective action plans that were responsive to the OIG's recommendations. Based upon its review of VA's corrective actions, the OIG has closed all report recommendations.

Data Center Consolidation. The OIG conducted an audit to determine whether VA met the data center requirements of the *Federal Information Technology Acquisition Reform Act* (FITARA).[6] Specifically, the OIG assessed whether VA accurately identified and reported data center inventories, achieved cost savings, and met the Office of Management and Budget's Data Center

[5] *Review of Alleged Mismanagement of VA's Real Time Location System Project*, December 19, 2017.
[6] *Lost Opportunities for Efficiencies and Savings During Data Center Consolidation*, January 30, 2019.

Optimization Initiative (DCOI) targets for data centers at existing VA facilities. The OIG found that VA faced several challenges in identifying data centers VA-wide, establishing a sufficient plan to achieve cost savings and avoidance targets, and meeting optimization metrics and closures. The OIG determined that all VA data centers were not accurately reported to OMB and VA's strategic plan was inconsistent with DCOI requirements due to missing and incomplete information. Without an accurate inventory of data centers or a credible plan to increase operational efficiency and achieve cost savings, VA will continue to operate in an IT environment that is at greater risk for duplication and waste. The OIG made five recommendations, and the Principal Deputy Assistant Secretary for IT concurred and has provided an acceptable action plan for four of the five recommendations.

Veterans Benefits Management System. A key part of the Veterans Benefits Administration's (VBA's) modernization efforts involved replacing its paper-based claims process with an automated solution that integrates commercial and government off-the-shelf web-based technology and improved business practices. VBA and OIT jointly developed the Veterans Benefits Management System (VBMS).

- In 2015, the OIG reviewed how effectively VA was managing the cost, performance, and schedule of VBMS development.[7] While the OIG found that VA stayed on schedule in deploying planned VBMS functionality to all VA regional offices, VBMS costs increased significantly, more than doubling from about $579.2 million to approximately $1.3 billion from 2009 to 2015. The increases were due to inadequate cost control, unplanned changes in system and business requirements, and inefficient contracting practices. As a result, VA could not ensure an effective return on its investment and total actual system development costs remained unknown. The OIG recommended the Executive in Charge for OIT, in conjunction with the Under Secretary for Benefits, define and stabilize system and business requirements, address system performance problems, deploy required functionality to process claims end-to-end, and institute metrics needed to identify and ensure progress toward meeting stated goals. While this report is from 2015, it highlights issues with IT project management that VBA continues to face.

In recent OIG reports on the processing of disability claims, the OIG found that VBMS functionality issues have contributed to concerns related to the processing of benefits.

- In a review of whether VBA staff assigned correct effective dates on claims for compensation benefits with an intent to file, the OIG determined that inaccurate dates for these claims partially occurred because VBMS lacked the needed functionality to assist rating personnel when assigning effective dates for benefits based on intent to file claims.[8] The intent to file allows claimants the opportunity to provide minimal information related to the benefit sought and gives them up to one year to submit a complete claim. The OIG

[7] *Follow-up Review of VA's Veterans Benefits Management System*, September 14, 2015.

[8] *Processing Inaccuracies Involving Veterans' Intent to File Submissions for Benefits*, August 21, 2018.

found that VBA assigned incorrect effective dates for approximately 17 percent of compensation benefits with receipt of the intent to file from claimants. VBA concurred with the OIG's recommendation related to functionality and indicated a correction is due in late 2019.

- In a review to determine whether VBA employees required disabled veterans to submit to unwarranted medical reexaminations, the OIG also found VBMS functionality issues.[9] The OIG determined that many unwarranted medical reexaminations occurred because VBMS did not have the functionality to prevent the scheduling of reexaminations in cases that met the exemption criteria. While reexaminations are important in certain situations to ensure taxpayer dollars are appropriately spent, unwarranted reexaminations cause undue hardship for veterans. They also generate excessive work, resulting in significant costs and the diversion of VA personnel from veteran care and services. VBA concurred with the OIG's recommendation and stated that VBA and OIT are in the process of developing automated examination request requirements and anticipate full functionality in FY 2019, pending prioritization and approval of new development efforts.

Forever GI Bill. In March 2019, the OIG released an issue statement in response to allegations that VA planned to withhold retroactive payments for missed or underpaid monthly housing stipends that it failed to pay students under the *Harry W. Colmery Veterans Education Assistance Act*, also known as the Forever GI Bill.[10] Given the impact of delayed or incorrect payments on veterans and congressional concerns, the OIG examined VA's timeline of early implementation actions and the impediments to meeting Forever GI Bill mandates. The OIG found that VBA failed to modify their electronic systems, such as the Long-Term Solution application, by the required implementation date to make accurate housing allowance payments under sections 107 and 501 of the law. VA also lacked an accountable official to oversee the project during most of the effort. Ineffective program management resulted in unclear communication of implementation progress and inadequately defined expectations, roles, and responsibilities of the various VA business lines and contractors involved. [11] The OIG also found that approximately 10 months passed from the time Congress enacted the Forever GI Bill until VA received the initial software development release and began testing the system modifications to VA's Long-Term Solution application in order to address sections 107 and 501 of the law.

ONGOING OVERSIGHT INITIATIVES

OIG engagements that are planned or underway will provide additional oversight of VA's IT management and IT security programs.

[9] *Unwarranted Medical Reexaminations for Disability Benefits*, July 17, 2018.
[10] *Forever GI Bill: Early Implementation Challenges*, March 20, 2019.
[11] The VA business lines and contractors involved include OIT, VBA Education Service, VBA Office of Business Process Integration, Booz Allen Hamilton, and VA leaders.

The FY 2019 FISMA audit will determine the extent to which VA's information security program and practices comply with FISMA requirements. This annual audit will evaluate selected management, technical, and operational controls supporting 49 selected major applications and general support systems hosted at 25 VA facilities, including VA's four major data centers. As previously discussed, in 2018 the OIG reported that VA has made progress developing, documenting, and distributing policies and procedures as part of its program. However, VA still faces challenges implementing components of its agency-wide information security risk management program to meet FISMA requirements. The OIG's 2019 audit will determine whether VA's improvement efforts are adequate to remove the IT material weakness from the OIG's report on VA's financial statements.

The OIG is also conducting an audit to determine whether VA has implemented key elements of FITARA Section 831, Chief Information Officer Authority Enhancements. Specifically, this audit will evaluate the extent to which the Chief Information Officer 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.

The OIG is monitoring many facets of VA's Electronic Health Record Modernization project, implementation of the MISSION Act, and other IT initiatives. As VA moves forward with these projects, the OIG will track the progress made and determine the most efficient and useful ways to provide oversight of VA's ongoing work.

CONCLUSION

Advances in IT enable VA to more effectively deliver benefits and services to our nation's veterans and their families. It is imperative that VA maintain secure systems and properly develop new systems. Until a proven process is in place to ensure control across the enterprise, the IT material weakness will remain and VA's mission-critical systems and sensitive veterans' data will be at risk of attack or compromise. While VA has made recent improvements in information management, more work remains to be done and VA must continue to address OIG recommendations related to the security and development of IT systems. The OIG will continue to conduct oversight of OIT initiatives and major projects to ensure they are secured, developed, and managed appropriately.

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