BRENT ARRONTE
DEPUTY ASSISTANT INSPECTOR GENERAL FOR
AUDITS AND EVALUATIONS
OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
SUBCOMMITTEE ON INFORMATION TECHNOLOGYCOMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
UNITED STATES HOUSE OF REPRESENTATIVES
HEARING ON
"VA INFORMATION TECHNOLOGY AND CYBERSECURITY OVERSIGHT"
MARCH 16, 2016

Mr. Chairman and Members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General's (OIG) work regarding the VA's management of information technology and information security. Our statement will focus on the effectiveness of VA's information security program and progress made and challenges VA continues to face in developing the systems it needs to care out is missions and program. We base our conclusions on OIG reports on VA's information security program and our oversight of information technology (IT) systems development activities. I am accompanied by Mr. Michael Bowman, Director, OIG's Information Technology and Security Audits Division.

BACKGROUND

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. Ensuring the secure operation of these systems and networks is essential, given the wide availability of hacking tools on the internet and the advances in the effectiveness of attack technology. Lacking proper safeguards, the systems and networks are vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other systems. VA 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.

For fiscal year (FY) 2016, VA estimates a total IT investment of about $4.1 billion to fund information system security, system development initiatives, and system operations and maintenance. To the extent that VA does not properly plan and manage these IT investments, they can become costly, risky, and counterproductive. In addition, although IT investments may be managed by the Office of Information Technology (OIT), it is imperative to include input from VA business owners and other stakeholders throughout the incremental system development process.

Our audits in recent years also show that IT system development at VA is a longstanding high-risk challenge, susceptible to cost overruns, schedule slippages, performance problems, and in some cases, complete project failures. Also in 2015, the

Government Accountability Office identified VA's management of IT acquisitions and operations as "high risk" and in their report they cited some significant failed VA IT investment projects totaling approximately $735 million.[1] In addition, the Government Accountability Office identified Security of Federal Information Systems as "high risk" and stated that Cybersecurity incidents to systems supporting the federal government and national critical infrastructures have significantly increased over the past eight years.

INFORMATION SECURITY

In November 2015, for the 16th consecutive year, the OIG's independent contractors that perform the annual audit of VA's consolidated financial statements have identified IT security controls as a material weakness. This work supports our requirements to perform annual Federal Information Security Modernization Act (FISMA) assessments. FISMA requires agencies to develop, document, and implement agency-wide information security risk management programs and prepare annual reports. FISMA also requires that each year, the OIG assess the extent to which VA complies with FISMA's information security requirements, information security standards developed by the National Institute of Standards and Technology (NIST), and the annual reporting requirements from the Office of Management and Budget.

In March 2012, VA instituted the Continuous Readiness in Information Security Program (CRISP) to ensure continuous monitoring year-round and establish a team responsible for resolving the IT material weakness. In our report, *Federal Information Security Management Act Audit for Fiscal Year 2015* (March 15, 2016), we discussed more focused VA efforts to implement standardized information security controls across the enterprise. For example, we reported that:

- VA had updated its policy which establishes a foundation for VA's comprehensive information security and privacy program and its practices based on applicable NIST Special Publications.
- VA's Chief Information Officer formed an Enterprise Cybersecurity Strategy team that was charged with delivering an enterprise cybersecurity strategic plan designed to help achieve greater transparency and accountability while securing veteran information.
- VA continued to implement an IT Governance, Risk, and Compliance tool to improve the process for assessing, authorizing, and monitoring the security posture of the agency.
- VA improved implementation of security awareness training for all employees and individuals with outdated background investigations had been reduced.
- Data center web application security had been improved.

[1] The Department of Veterans Affairs' (VA) Financial and Logistics Integrated Technology Enterprise program, which was intended to be delivered by 2014 at a total estimated cost of $609 million, but was terminated in October 2011 due to challenges in managing the program and the VA Scheduling Replacement Project, which was terminated in September 2009 after spending an estimated $127 million over 9 years.

However, these improvements require time to be fully implemented and show evidence of their effectiveness. Despite progress made, the CRISP initiative was not fully effective in addressing systemic weaknesses and eliminating the material weakness. We continue to see repeat information security deficiencies in type and risk level to our reported findings in prior years and an overall inconsistent implementation of the security program. Communication between the CRISP team and VA site managers also needs improvement. Our FY 2015 FISMA audit report discussed control deficiencies in four key areas: configuration management controls, access controls, security management, and contingency planning controls.

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

- Systems including key databases supporting various applications were not timely patched or securely configured to mitigate known and unknown information security vulnerabilities.
- The financial management system uses outdated technology that hinders mitigation of certain vulnerabilities.
- VA needs to strengthen its methodologies for monitoring medical devices and ensuring they are properly segregated from other networks.
- Baseline configurations, including implementation of the Federal Desktop Core Configuration, were not consistently implemented to mitigate significant system security risks and vulnerabilities across the facilities.
- Change control policy and procedures for authorizing, testing, and approval of system changes were not consistently implemented for the networks and mission critical system hardware and software changes.
- Several VA organizations shared the same local network at some medical centers and data centers; however, the systems were not under the common control of the local site. Some organizational systems often had critical or high-level vulnerabilities that weakened the overall security posture of the VA sites.
- Formal processes were lacking to prevent installation of or remove unauthorized application software on VA systems.

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

- Password standards were not consistently implemented and enforced across multiple VA systems, including the network domain, databases, and mission critical applications. In addition, multi-factor authentication for remote access had not been fully implemented across the agency.
- Inconsistent reviews of networks and application user access resulted in numerous generic, system, and inactive user accounts that were not removed or deactivated from the system, and users with access rights that were not appropriate.

- Proper completion of user access requests was not consistently performed to eliminate conflicting roles and enforce principles of least system privilege.
- Monitoring of access was lacking in the production environment for individuals with elevated application privileges for a major application.
- Identification, notification, and remediation of security incidents were not consistently implemented to ensure incidents were resolved timely. In addition, network security event logs were not consistently maintained or reviewed across all facilities.

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

- Security management documentation, including the risk assessments and System Security Plans, were outdated and did not accurately reflect the current system environment or Federal standards.
- Background reinvestigations were not performed timely or tracked effectively. In addition, personnel were not receiving the proper level of investigation for the sensitivity levels of their positions.
- Plans of Action and Milestones (POA&Ms) were not completed by their milestone dates and were not updated to reflect changes to milestones. POA&M closures were not supported with adequate documentation. VA had approximately 9,500 open POA&Ms in FY 2015 compared with 9,000 in FY 2014. POA&Ms identify which actions must be taken to remediate system security risks and improve VA's overall information security posture.
- VA did not effectively manage and monitor its systems hosted at a cloud service provider.

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

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

Further, we continued to identify significant technical weaknesses in databases, servers, and network devices that support transmitting sensitive information among VA Medical Centers, Data Centers, and VA Central Office. Within our annual FISMA report, we discuss security deficiencies where control activities were not appropriately designed or operating effectively. Inconsistent application of vendor patches to address such weaknesses jeopardized the data integrity and confidentiality of VA's financial and sensitive information.

Moving forward, VA needs to complete implementation of an enterprise-wide information security program and improve its monitoring process to ensure controls are operating as intended at all facilities. The dispersed locations, the continued reorganization of VA business units, and the diversity in applications adversely affected facilities and management's ability to consistently remediate IT security deficiencies agency-wide. For example, VA's dispersed financial system architecture resulted in a lack of common system security controls and inconsistent maintenance of IT mission-critical systems. Consequently, VA continues to be challenged by a lack of consistent enforcement of established policies and procedures throughout its geographically dispersed portfolio of legacy applications and newly implemented systems. In addition, VA lacked an effective and consistent corrective action process for identifying, coordinating, correcting, and monitoring known internal security vulnerabilities on databases, web applications, and networks infrastructures. Effective communication between VA management and the individual field offices is critically needed to notify the appropriate personnel of identified security deficiencies so that they can timely implement corrective actions.

Our FY 2015 FISMA report included 31 recommendations to the Assistant Secretary for Information and Technology for improving VA's information security program. The report also highlighted 4 unresolved recommendations from prior years' assessments for a total of 35 outstanding recommendations. Overall, we recommended that VA:

- Address security-related issues that contributed to the IT material weakness reported in the FY 2015 audit of the Department's consolidated financial statements.
- Remediate high-risk system security issues within its POA&Ms.
- Establish effective processes for evaluating information security controls via continuous monitoring and vulnerability assessments.
- Implement effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and Web application servers.
- Institute procedures to oversee contractor management of cloud-based systems, ensure OIG access to those systems, and ensure information security controls are adequate to protect sensitive VA systems and data.
- Conduct periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and excessive or unauthorized accounts.

We are evaluating VA's progress during our current work on the FY 2016 FISMA audit and acknowledge increased VA efforts to improve information security. This fall, upon completion of our FY 2016 FISMA testing and related work at 24 of sites nationwide, including VA's four major data centers, we will make a determination as to whether VA's improvement efforts are successful in eliminating the IT material weakness.

OTHER INFORMATION TECHNOLOGY CONCERNS AT VA

VA faces the added challenge of overcoming several information security concerns not highlighted in previous years, such as the reorganization of OI&T's regional structure and new leadership of the CRISP program without institutional knowledge as a result of turnover of senior leadership. Where appropriate, we are pursuing these issues as a part of our ongoing FISMA audit work. Otherwise, we are conducting separate reviews or pursuing other means to address the issues noted below.

Limited Reporting of Security Incidents to the OIG

VA continues to experience security breaches of its enterprise as a result of employee and contractor actions, malware, or "focused operations actors" activity. However, the reporting of these incidents to OIG has been relatively low and limited. In accordance with FISMA, VA must provide the OIG with timely notifications of network intrusions and system compromises so we can properly execute our oversight function.

The following are examples of security incidents not properly reported to the OIG:

- Since December 2010, we have noted six incidents involving compromises of VA contractor owned computers or user credentials resulting in unauthorized access into VA networks. The two most recent contractor computer compromises occurred in February 2015 and May 2015; however only the latter security incident was ever reported to the OIG.
- Since November 2014, the Network Security and Operations Center (NSOC) has identified two incidents of keystroke logging software data on devices with one containing logged Veterans Health Information Systems and Technology Architecture (VistA) user credentials. Despite Federal requirements, neither of these incidents were reported to the OIG. Keystroke loggers are typically used to capture user credentials so malicious users can gain unauthorized access onto computer systems.
- In June 2015, the NSOC identified network traffic associated with certain software used to enable anonymous communication across the Internet and to conceal users' identity and location. The resulting analysis identified a VA domain administrator using a computer and security device that prevented the NSOC from evaluating the machine for compliance with VA security requirements. The NSOC initially reported this issue to the OIG as "cracked" Corel Draw software. However, the NSOC did not disclose any information to us regarding the use of anonymizing software or the security implications of using a security device to prevent compliance checks.
- In light of recent Office of Personnel Management data breach, the NSOC has evaluated enterprise activity for "Indicators of Compromise" and identified 7 potentially compromised hosts. While VA's Forensic Investigation Service is currently analyzing these computers for security compromises, the OIG was never notified of these security issues. We proactively discovered this information when reviewing VA's Remedy System.

As a result, we are not satisfied with the inconsistent reporting of security incidents to the OIG.

Veterans Health Information Systems and Technology Architecture

We have evaluated certain key controls within VistA as part of our FISMA audit. Specifically, we have reviewed VistA controls supporting financial transactions that are reported in VA's consolidated financial statements each year. However, we have not evaluated VistA's on-going evolution and its interoperability with Department of Defense's electronic health record (EHR) application. Recently, we reported that certain audit controls within VistA were not enabled, which limited our oversight work in order to determine whether any malicious manipulation of scheduling data or unauthorized access to VistA records occurred at several VA Medical Centers noted below. Additionally, we discovered during a recent investigation at the Washington DC VA Medical Center that VistA email was purged without sufficient backups, resulting in an unknown quantity of email that is unrecoverable.

In February 2015, the OIG's Office of Healthcare Inspections conducted a review of the care a patient received at the Atlanta VA Medical Center, in Decatur, Georgia, and evaluated an improper disclosure of protected information outside VA.[2] We confirmed that an individual with access to a patient's VistA EHR improperly disclosed protected health information outside VA. The patient's record was designated as "non-sensitive" at the time of the disclosure. As a result of this designation, the Veterans Health Administration (VHA) lacked the ability to audit access to VistA "non-sensitive" records. More importantly, managers do not have the necessary tools to identify wrongdoers and therefore cannot consistently enforce some rules and statutes. To date, OIG investigators were unable to determine who accessed the patient's EHR or who was responsible for the improper disclosure. VA's Interim Under Secretary for Health concurred with our recommendations and agreed to evaluate the feasibility of enabling system audit logging for all patient records.

In February 2015, the OIG's Office of Healthcare Inspections conducted another inspection to assess the merit of allegations of poor and delayed care of a patient in the Urgent Care Clinic at the Tomah VA Medical Center in Tomah, Wisconsin.[3] One specific allegation stated that unauthorized parties accessed or disseminated a patient's electronic health record information inappropriately. The complainant provided several Internet news article "comments" that were potentially indicative of sensitive VistA EHR information having been accessed and used in an inappropriate manner. After reviewing these comments, we did not identify any protected information that could only have been obtained from the patient's VistA EHR or other VA privacy protected documents. However, we found that it was possible that the patient's VistA EHR was accessed inappropriately since the record was designated as "non-sensitive" and was not monitored. When a record is designated as "non-sensitive," an electronic audit trail is not created when the EHR is accessed. The patient's record was not designated "Sensitive" until February 25, 2015. VA's Interim Under Secretary for Health concurred with our recommendations and agreed to evaluate the feasibility of enabling system audit logging for all patient records.

[2] *Evaluation of a Patient Care and Disclosure of Protected Information, Atlanta VA Medical Center, Decatur Georgia* (June 23, 2015).

[3] *Care of an Urgent Care Clinic Patient, Tomah VA Medical Center, Tomah Wisconsin* (June 18, 2015).

In August 2014, we reported that certain audit controls within VistA were not enabled, which hurt our ability to determine whether any malicious manipulation of the VistA scheduling data occurred at the Phoenix VA Health Care System, in Phoenix, Arizona.[4] Consequently, we requested that OIT leadership enable all audit trails within the scheduling system. We also requested that OIT discontinue deleting VistA accounts for former employees and instead place these accounts in a disabled state so that we can evaluate system use and scheduling data as part of our review. OIT complied with these requests. The OIG is committed to performing additional scrutiny of the functionality and data integrity of this system as part of ongoing and future reviews.

Improper Access to the VA Network by VA Contractors from Foreign Countries

In April 2015, an OIG administrative investigation found that certain OIT employees failed to follow VA information security policy and contract security requirements when they improperly approved VA contractor employees to work remotely and access VA's network from China and India, respectively.[5] We noted that one contractor accessed VA's network from China using personally-owned equipment that he took to and left in China, and the other accessed VA's network from India using personally-owned equipment that he took with him to India and then brought back to the United States. Further, we found that a VA employee and other VA contractor employees improperly connected to VA's network from foreign locations. We further noted that VA information security officials and the Executive in Charge for OIT failed to quickly and effectively respond to determine if there was a compromise as a result of VA contractor employees accessing VA's network internationally.

Improper Use of Web-based Collaboration Technology

In August 2015, we reported that VA employees improperly used Yammer.com, a Web-based collaboration technology that was not approved or monitored as required by VA policy.[6] Further, we found the application had vulnerable security features, recurring website malfunctions, and users were engaged in a misuse of time and resources. Although One VA Technical Reference Model approved the installation of Yammer's "Notifier" desktop application, the use of the Yammer social network was not approved for VA employee use. Furthermore, we noted that the Internet based application was used and showcased by the Executive in Charge of Information Technology and Chief Information Officer, for an open chat forum, as well as in a CIO Message reminding employees to comply with VA Directive 6515 when using Yammer. This direction gave the false impression that VA had approved employees' use of Yammer.com. As of July 14, 2015, Yammer.com reflected there were 24,864 VA email addresses registered with active members and another 25,252 VA email addresses registered which were not yet activated.

[4] *Review of Alleged Patient Deaths, Patient Wait Times, and Scheduling Practices at the Phoenix VA Health Care System* (August 26, 2014).

[5] *Administrative Investigation – Improper Access to the VA Network by VA Contractors from Foreign Countries Office of Information and Technology Austin, TX (April 13, 2015).*

[6] *Administrative Investigation – Improper Use of Web-based Collaboration Technology Office of Information and Technology* (August 17, 2015).

We also found that Yammer users violated VA policy when they downloaded and shared files, videos, and images, risking malware or viruses spreading quickly from the site. We further noted that Yammer regularly spammed and excessively emailed users, as well as VA employees who had no interest in joining the site. In addition, users were unable to remove the "Online Now" instant messaging feature, resulting in every user violating VA policy simply by logging onto the site. We found numerous user posts that were non-VA related, unprofessional, or had disparaging content that reflected a broad misuse of time and resources. Moreover, the continuous data streams, instant messaging, video, audio, large attachment files, and other uploaded non-VA content to the site can cause disruption of service and degrade the performance of VA's network. OIT's lack of control over the Yammer website has made VA vulnerable to users uploading personally identifiable information, protected health information, or VA sensitive information, of which any current or former employee active on the site would have access.

Data Sharing Violations at the Palo Alto VA Medical Facility

In October 2014, we received an allegation that the VA Palo Alto Health Care System (PAHCS), in Palo Alto, California, Chief of Informatics entered into an illegal agreement with Kyron, a health technology company, to allow data sharing of sensitive VA patient information. This allegation involved veterans' personally identifiable information, protected health information, and other sensitive information that was transmitted outside of VA's firewall. The complainant also alleged Kyron personnel received access to VA patient information through VA systems and networks without appropriate background investigations.

In September 2015, we did not substantiate the allegations that the Chief of Informatics formed an illegal agreement with Kyron or that sensitive patient information was transmitted outside of VA's firewall. However, we reported that Kyron personnel received access to VA patient information without appropriate background investigations.[7] Further, the Information Security Officers (ISOs) failed to execute their required responsibilities in accordance with VA Handbook 6500, Information Security Program, by not providing PAHCS management and staff guidance on information security matters. The lack of coordination between facility program proponents and ISOs resulted in Kyron having access to VA information systems without appropriate background investigations and Kyron's software being used on a VA server without formal approval. VA's Assistant Secretary for Information and Technology concurred with our findings and recommendations and provided an acceptable corrective action plan.

Cloud Computing

In February 2013, we communicated concerns to VA regarding its intent to migrate its e-mail systems to a cloud service provider. Specifically, VA had moved 15,000 email user accounts to a cloud-based system as part of a pilot study and planned to migrate the remaining 600,000 email user accounts to the virtual cloud environment thereafter. As

[7] *Review of Alleged Data Sharing Violations at VA's Palo Alto Health Care System* (September 28, 2015).

a result, all VA email messages were planned to be hosted on a contractor-owned and operated system.

Upon OIG review of the underlying contract, we noted the contract did not require the cloud service provider to provide OIG access to VA systems and data stored at the contractor facilities. Consequently, the OIG would not have legal access to VA systems and data needed for investigative and oversight purposes. Further, the contract terms would potentially compromise our efforts to ensure that annual FISMA requirements are met. Additionally, the contract lacked requirements for the cloud service provider to segregate VA sensitive data from other customer data, potentially impeding OIG investigations and creating new information security weaknesses involving VA electronic data. VA planned to adopt a policy to delete cloud-hosted emails greater than 90 days old in an effort to save costs with the cloud-based contract. Email is integral to the manner in which VA conducts day-to-day business. As such, retention of emails is critical to support VA work, OIG investigations and oversight reviews, and to defend VA actions in the administrative and judicial appellate systems.

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

Enterprise Archiving System

The OIG has communicated major concerns to VA’s senior leadership regarding retrieval of Enterprise Archive System emails prior to June 2013. Currently, VA stores archived emails on a “Digital Safe” device which VA uses to support email collections pursuant to our oversight work. In June 2015, we were notified that VA’s “Digital Safe” was not working properly and all email content prior to June 2013 was not readily available to support OIG investigations or VA legal discovery requests. OIT originally stated that the "Digital Safe" problem would be resolved in September 2015, but the targeted resolution date has moved to May 2016.

While VA has been able to provide email prior to June 2013, due to the "Digital Safe" not working properly, the process is extremely labor intensive and time consuming, resulting at times in delays that impair the OIG’s and VA’s Office of General Counsel’s ability to satisfy its oversight and legal responsibilities, respectively. The lack of a viable solution to provide timely “Digital Safe” data negatively impacts the OIG’s internal operations by delaying receipt of archived emails associated with multiple OIG investigations and inspections. The lack of timely access to this data also adversely affects both the VA's and the OIG's obligation to comply with legal discovery requirements from the Department of Justice, other administrative bodies as well as requests for information from Congress. Accordingly, we are concerned that VA lacks sufficient resources, processes and data to support operational transparency and accountability.

Personally Identifiable Information Transmission Over Unsecure Internet Connections

In March 2013, we reported that VA was transmitting sensitive data, including personally identifiable information and internal network routing information, over an unencrypted telecommunications carrier network.[8] VA disclosed that personnel typically transfer unencrypted sensitive data, such as electronic health records and internal internet protocol addresses, among certain VA Medical Centers and Community-Based Outpatient Clinics using an unencrypted telecommunications carrier network. OIT acknowledged this practice and formally accepted the security risk of potentially losing or misusing the sensitive information exchanged.

These risks continue to exist across the VA enterprise. Despite concurring with our report findings and recommendations, VA has not fully implemented the technical configuration controls needed to ensure encryption of sensitive data in accordance with VA and Federal information security requirements. Without controls to encrypt the sensitive VA data transmitted, veterans' information may be vulnerable to interception and misuse by malicious users as it traverses unencrypted telecommunications carrier networks. Further, malicious users could obtain VA router information to identify and disrupt mission-critical systems essential to providing health care services to veterans.

INFORMATION TECHNOLOGY SYSTEMS DEVELOPMENT

VA remains challenged in developing the IT systems it needs to support VA's mission goals. Recent OIG reports disclose that some progress has been made in timely deploying system functionality because of the Agile system development methodology. This methodology allows subject matter experts to validate requirements and functionality in increments of 6 months or fewer, while technology is developed and updated to meet user needs. Despite these advances, VA continues to struggle with cost overruns and performance shortfalls in its efforts to develop several major mission-critical systems. VA's mechanism for overseeing IT program management has improved but has not been fully effective in controlling these IT investments. Inadequate IT human capital management plays a notable role in these system development outcomes.

Veterans Benefits Management System

In February 2013, we issued a report, *Review of VBA's Transition to a Paperless Claims Processing Environment,* evaluating whether VA had performed sufficient testing of the Veterans Benefits Management System (VBMS) and assessing whether VA was positioned to meet its goal of eliminating the disability claims backlog and increasing the accuracy rate of processing claims to 98 percent by 2015.[9]

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

[9] *Review of Transition to a Paperless Claim Processing Environment* (February 4, 2013).

As of September 2012, VBMS was still in the early stages of development. We found that due to the use of VA's Agile incremental development approach, the system had not been fully developed to the extent that its capability to process claims from initial application through review, rating, award, to benefits delivery could be sufficiently tested. While we did not evaluate the quality of system testing, we determined the partial VBMS capability deployed as of that date had experienced system performance issues. At the time of that audit work, VA senior officials stated they had taken recent actions to improve in the areas identified. However, given the incremental system development approach used and the complexity of the automation initiative, we concluded VA would continue to face challenges in meeting its goal of eliminating the backlog of disability claims processing by 2015. Because the system was in an early stage of development, we could not examine whether VBMS was improving VBA's ability to process claims with 98 percent accuracy. The then-Under Secretary for Benefits and the then-Assistant Secretary for Information and Technology concurred with our report recommendations that VA establish a plan with milestones for resolving system issues and develop a detailed approach to scanning and digitizing claims so that transformation efforts do not adversely affect claims processing and add to the claims backlog.

In September 2015, we issued a follow-up review to determine whether VA has improved its schedule, cost, and performance in VBMS development to better position VA to meet its claims processing accuracy and backlog elimination goals.[10] We reported that VA deployed certain planned VBMS functionality to all VA Regional Offices in 2013, largely due to the incremental Agile development approach. With the deployments, VA has expanded automated claims processing functionality, supported improved data exchange, and standardized business practices that VA reports have helped reduce the claims processing backlog. However, total estimated VBMS costs increased significantly from about $579 million initially in September 2009 to about $1.3 billion in January 2015. Further, we found VBMS still did not fully provide the capability to process claims from initial application through review, rating, award, to benefits delivery. The system continues to experience performance issues, including service disruptions and slowness. VBMS cost overruns and performance shortfalls were chiefly due to unplanned changes in system and business requirements and a lack of performance metrics. Until these issues are addressed, VA will remain unable to ensure effective return on its VBMS investment. Further, until a fully functioning system is in place, VA will be challenged to meet its 98 percent claims processing accuracy and backlog elimination goals. VA's Executive in Charge for the Office of Information and Technology, in conjunction with Veterans Benefits Administration (VBA), generally agreed with our findings and recommendations.

We are currently reviewing allegations related to VBA failing to integrate suitable audit logs into VBMS. We will report out on this work in late Spring.

[10] *Follow-up Review of the Veterans Benefits Management System* (September 14, 2015)

Pharmacy Reengineering

In December 2013, we reported on OIT's management of the Pharmacy Reengineering (PRE) project.[11] OIT restarted PRE in October 2009 under the Project Management Accountability System (PMAS). PRE is critically needed to help address patient safety issues associated with adverse drug events. Although some progress had been made, OIT had not been effective in keeping the PRE project on target in terms of schedule and cost, as well as the functionality delivered. Deployed PRE functionality had improved patient safety. However, project managers have struggled to deploy PRE increments in a timely manner. Project managers were also unable to provide reliable costs at the increment level. OIT restarted PRE at a time when PMAS had not evolved sufficiently to provide the oversight needed to ensure project success.

As such, PRE management was challenged in keeping the project on track. Consequently, OIT was at an increased risk of not completing PRE on time and within budget. Moreover, the future of Pharmacy Reengineering was uncertain due to potential plans to transfer funding and remaining development to the Integrated Electronic Health Record (iEHR) project in FY 2014. Stronger accountability over cost, schedule, and scope for the remaining development is needed prior to such a transfer so that iEHR is not compromised by the same challenges.

VA's Executive in Charge and Chief Information Officer agreed with our recommendations to ensure all of the time used, including the time on the initial operating capability phase, to complete each remaining PRE increment is reported and monitored; ensure adequate oversight and controls, including the planning guidance, staffing, and cost and schedule tracking needed to deliver functionality on time and within budget; and establish a plan for future funding of PRE until iEHR is decided. OIT now requires paused projects to pass a review that serves as a critical checkpoint before they can advance to an active development state. OIT implemented controls to ensure all projects maintain adequate staffing. Further, OIT has provided adequate funding for PRE to move forward with continued development.

Program Management Accountability System

VA launched PMAS in June 2009 to improve its ability to deliver successful IT projects. At the request of VA's Chief Information Officer, we conducted an audit in 2011 to evaluate the effectiveness of PMAS planning and implementation. We reported that a great deal of work remains before PMAS can be considered completely established and fully operational.[12] For example, OIT created and instituted the PMAS concept without a roadmap, adequate leadership, and staff to effectively implement and manage the new methodology. If such foundational elements are not fully implemented, the discipline and accountability needed for effective management and oversight of IT development projects will not be instilled. VA's Chief Information Officer concurred with our findings and recommendation and provided an acceptable corrective action plan.

[11] *Audit of VA's Pharmacy Reengineering Software Development Project* (December 23, 2013).

[12] *Audit of the Project Management Accountability System Implementation* (August 29, 2011).

In 2014, we performed a follow-up audit to evaluate whether OIT took effective actions to address recommendations that we made in our prior audit report on PMAS. In our report, we noted that OIT had taken steps to improve PMAS.[13] For instance, OIT had defined PMAS roles and responsibilities, developed guidance for re-planning paused projects, and established controls to ensure essential staff is assigned to manage the projects. However, at the time of that report, OIT needed to take additional actions to improve IT project accountability and oversight and the PMAS Business Office still lacked sufficient leadership and staff. We reported that the PMAS Dashboard retained an incomplete audit trail of baseline data and project managers continued to struggle with capturing and reporting costs. These issues occurred because OIT did not appropriately address our prior report recommendations. Project managers also did not report costs for enhancements to existing systems on the PMAS Dashboard due to unclear PMAS guidance. As a result, OIT and therefore VA leaders lack reasonable assurance these IT investment projects are delivering functionality on time and within budget. We also identified potentially $6.4 million in cost savings OIT could achieve by hiring Federal employees to replace contract employees currently augmenting PMAS Business Office staff. VA's Executive in Charge concurred with most of our recommendations and provided acceptable corrective action plans.

CONCLUSION

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

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

[13] *Follow-Up Audit of the Information Technology Project Management Accountability System* (January 22, 2015).