DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

STATEMENT OF NICK DAHL
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
CYBERSECURITY CHALLENGES AND CYBER RISK MANAGEMENT AT
THE DEPARTMENT OF VETERANS AFFAIRS
NOVEMBER 14, 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 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

[1] *Review of Alleged Unsecured Patient Database 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 FY 2020 Funding and FY 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 1950s. VA's system employed at the medical centers —Veterans Health Information Systems and Technology Architecture (VistA)—was built in the late 1970s. Both systems are considered to be significantly outdated.

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 FY 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 FY 2018 FISMA report, published by the OIG in March 2019, contained multiple findings and 28 recommendations to the Assistant Secretary for Information 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 databases 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, databases, and mission-critical applications. In addition, multifactor authentication for remote access had not been fully implemented

[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.

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 FY 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.

[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 FY 2019 FISMA assessment.

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.

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.

[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.

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] 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 database. 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

[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.

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

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

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

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 FY 2019 FISMA assessment to determine VA's compliance and expects to release the results in the Spring of 2020. 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 FY 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.