STATEMENT OF MICHAEL BOWMAN
OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS
DIRECTOR OF IT AND SECURITY AUDITS DIVISION
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
U.S. HOUSE OF REPRESENTATIVES COMMITTEE ON VETERANS' AFFAIRS
HEARING ON
CYBERSECURITY AND RISK MANAGEMENT AT VA:
ADDRESSING ONGOING CHALLENGES AND MOVING FORWARD
MAY 20, 2021

Chairman Mrvan, Ranking Member Rosendale, 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. Our statement discusses the security program's purpose and the many challenges VA faces in protecting the confidentiality, integrity, and availability of VA systems and data.

The Federal Information Security Modernization Act of 2014 (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.[1] FISMA also requires an agency's Inspector General to provide an annual assessment of the agency's security program and practices. On April 29, 2021, the OIG released its FISMA audit of VA for fiscal year (FY) 2020.[2] This is the 21st consecutive year that the OIG has reported on the extent to which VA has IT safeguards in place consistent with the Act's requirements. Our audit evaluated select management, technical, and operational controls supporting 48 major applications and general support systems hosted at 24 VA facilities, including VA's four major data centers.

The OIG's conclusions in the FY 2020 FISMA audit are not new or revelatory—rather, they repeat many of the same concerns with VA's IT security that the OIG has found for many years. We recognize, however, that VA is operating in a very challenging environment, with an extremely large decentralized organization and many outdated systems that are constantly being upgraded or replaced. These long-standing problems will not be quickly resolved. We have noted

[1] The Federal Information Security Modernization Act of 2014 amended and updated existing requirements set forth in the Federal Information Security Modernization Act of 2002.

[2] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, April 29, 2021.

some progress in certain areas of VA's security program. These can best be characterized as incremental improvements in addressing the deficiencies the audit team has repeatedly identified.

In 2019 the OIG testified before this subcommittee on VA's cybersecurity challenges and reviewed the 28 recommendations in our FY 2018 FISMA audit. Our recently released FY 2020 FISMA audit included 26 recommendations (some new and some repeated), which reflects VA's limited progress. Of the 26 recommendations, 21 have been included in every FISMA audit dating back to at least 2017. An appendix to our statement provides information on which of these recommendations were also made to VA in our three most recent FISMA audits. The number of persistent problems identified underscores VA's inability to make major improvements and impactful change in their security program.

My statement will focus on the most pressing issues identified in our recently released FISMA audit, discuss possible corrective actions that VA could take to achieve meaningful change, and highlight additional ongoing OIG initiatives that are meant to assist VA in improving IT security.

BACKGROUND

IT systems and networks are critical to VA for carrying out its mission of providing medical care, 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 tremendously 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. Without proper safeguards, these systems and networks are vulnerable to intrusions by groups seeking to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other VA systems.

Developing and maintaining adequate safeguards is made more complex because many of VA's legacy systems have been obsolete for several years. These antiquated systems are 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 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 criminal acts. It is vital that VA's IT investments are carefully deployed and monitored.[3] To the extent that VA does not properly manage and secure their IT investments, they can become

[3] For FY 2021, VA requested a total IT investment of $4.9 billion, of which $342 million is to fund information security in connection with enterprise operations and maintenance.

increasingly vulnerable to misuse and mishaps. Security failures also undermine the trust veterans put in VA to protect their sensitive information and can affect their engagement with programs and services.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT COMPLIANCE

The FY 2020 FISMA 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.

As mentioned earlier, the FY 2020 FISMA report contained multiple findings and 26 recommendations to the Acting 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. Security deficiencies could allow any system and database user to gain unauthorized access to critical system information. The OIG concluded that VA systems and key databases were not patched timely 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. Consequently, the audit identified numerous critical and high-risk vulnerabilities, such as users having unnecessary system permissions and missing security patches on systems that support medical devices that were connected to VA's general network.
- **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. The use of weak passwords is a well-known security vulnerability that allows malicious users to easily gain unauthorized access to mission-critical systems. 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. 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. Periodic reviews are critical to restrict legitimate users to specific systems and to prevent unauthorized access by both internal and external users. Moreover, unauthorized access to critical systems can leave sensitive data vulnerable to inappropriate modification or destruction.

- **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. Inadequate security documentation may result in insufficient awareness and management of system risks and deficiencies as well as ineffective continuous monitoring of security controls. The OIG's findings included that security management documentation, such as system security plans, were outdated and did not accurately reflect the current system environment or federal standards. Also, periodic 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. Without accurate and reliable investigation reporting, VA is at risk of allowing unnecessary or unauthorized access to sensitive systems and data.
- **Contingency Planning Controls** ensure that mission-critical systems and business processes can be restored in the event of a disaster or emergency. Mission-critical systems at VA include the systems that support the day-to-day operations at over 1,000 healthcare facilities nationwide and those that provide recurring benefits payments to eligible veterans. The OIG team noted instances of unplanned outages or disruptions from which services were not recovered within prescribed Recovery Time Objectives. Of additional concern, the OIG team concluded that plans were not consistently tested in accordance with VA policy requirements. If critical business functions are not recovered within agreed upon timeframes, VA is at risk of not effectively providing mission-critical services.

The Acting Assistant Secretary for Information and Technology concurred with the 26 OIG recommendations and provided acceptable action plans for implementing open recommendations. Overall, the OIG's FISMA audit shows that for VA to achieve better IT security outcomes, the Department must take the following actions:

- Address security-related issues contributing to the IT material weakness being reported again in the FY 2020 audit of VA's Consolidated Financial Statements;[4]
- 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

[4] A material weakness is "a deficiency, or combination of deficiencies, in internal controls 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." *Audit of VA's Financial Statements for Fiscal Years 2020 and 2019*, November 24, 2020. 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. The OIG's most recent audit of VA's consolidated financial statements once again identified IT security controls as a material weakness.

- 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.

The OIG will continue to monitor progress and review status updates from VA on open recommendations until all proposed actions are successfully completed.

ONGOING OVERSIGHT INITIATIVES

In addition to working on the FY 2021 FISMA assessment, the OIG has multiple ongoing projects that will provide additional oversight of VA's IT security efforts.

In February 2020, the OIG launched an IT security inspection program to review sites not evaluated under the annual FISMA audits, or facilities that did not perform well in prior FISMA audits. These reviews are not intended to duplicate OIG FISMA audits but to provide more oversight and ensure VA focuses on IT security at all levels—local, regional, and national. The OIG plans to publish its first of a series of IT inspection reports in June 2021.

The OIG is also conducting a review to determine if the Office of Information Technology ensured that all cloud-based software it deployed met federal authorization requirements. Cloud-based services are applications or software that are available remotely and hosted on a VA or vendor's server on behalf of VA, and allow users access to software applications that run on shared computing resources (for example, processing power, memory, and disk storage). These services pose potential risks of VA data being exposed or its systems being improperly accessed if VA policy and Federal Risk and Authorization Management Program policies are not followed and if the vendors do not meet federal authorization requirements.

Furthermore, the OIG is monitoring facets of VA's Electronic Health Record Modernization program and other IT initiatives that will require substantial planning and resources to ensure they are properly protected and secured. The OIG will continue to pursue the most efficient and useful ways to oversee and report on VA's progress.

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, and VA's incremental improvements are not enough to effect meaningful change. Until proven processes are in place to ensure adequate controls across the enterprise, VA's mission-critical systems and sensitive veterans' data remain 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 the recommendations from our FISMA audit is vital to its efforts to address ongoing and emerging issues.

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

APPENDIX A: REPEAT RECOMMENDATIONS IN RECENT VA OIG FISMA AUDITS

FISMA Audit Recommendation for FY 2020	Recommendation included in FISMA FY 2017	2018	2019
1. We recommended the Assistant Secretary for Information and Technology (ASIT) consistently implement an improved continuous monitoring program in accordance with the National Institute of Standards and Technology Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions.			X
2. We recommended the ASIT implement improved mechanisms to ensure system stewards and information system security officers follow procedures for establishing, tracking, and updating Plans of Action and Milestones for all known risks and weaknesses including those identified during security control assessments.	X	X	X
3. We recommended the ASIT implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing plans of action and milestones.	X	X	X
4. We recommended the ASIT develop mechanisms to ensure system security plans reflect current operational environments, include an accurate status of the implementation of system security controls, and all applicable security controls are properly evaluated.	X	X	X
5. We recommended the ASIT implement improved processes for reviewing and updating key security documents such as security plans, risk assessments, and interconnection agreements on an annual basis and ensure the information accurately reflects the current environment.	X	X	X
6. We recommended the ASIT implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices.	X	X	X
7. We recommended the ASIT implement periodic reviews to minimize access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts.	X	X	X
8. We recommended the ASIT enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.	X	X	X
9. We recommended the Office of Personnel Security strengthen processes to ensure appropriate levels of background investigations are completed for	X	X	X

FISMA Audit Recommendation for FY 2020	Recommendation included in FISMA FY 2017	2018	2019
applicable VA employees and contractors and applicable investigation data are accurately tracked within the authoritative system of record.			
10. We recommended the Office of Personnel Security formalize the position descriptions and methodology used within the Human Resource business processes to ensure that employees with similar positions are required to have the same level of background investigation.[5]			
11. We recommended the ASIT implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.	X	X	X
12. We recommended the ASIT implement a more effective patch and vulnerability management program to address security deficiencies identified during our assessments of VA's web applications, database platforms, network infrastructure, and workstations.	X	X	X
13. We recommended the ASIT maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately implemented for compliance with established VA security standards.	X	X	X
14. We recommended the ASIT implement improved network access controls that restrict medical devices from systems hosted on the general network.	X	X	X
15. We recommended the ASIT consolidate the security responsibilities for networks not managed by the Office of Information and Technology under a common control for each site and ensure vulnerabilities are remediated in a timely manner.	X	X	X
16. We recommended the ASIT implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.	X	X	X
17. We recommended the ASIT implement improved procedures to enforce standardized system development and change control processes that integrates information security throughout the life cycle of each system.	X	X	X
18. We recommended the ASIT review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives are met.			X

[5] The deficiency addressed in this recommendation has been communicated to VA in previous years, however this is the first year it was included in the report narrative. Therefore, while it is technically a new recommendation it is not a new issue.

FISMA Audit Recommendation for FY 2020	Recommendation included in FISMA FY 2017	2018	2019
19. We recommended the ASIT ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements.[6]			
20. We recommended the ASIT implement more effective agency-wide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards.	X	X	X
21. We recommended the ASIT ensure that VA's Cybersecurity Operations Center has full access to all security incident data to facilitate an agency-wide awareness of information security events.	X	X	X
22. We recommended the ASIT implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.	X	X	X
23. We recommended the ASIT implement improved measures to ensure that all security controls are assessed in accordance with VA policy and that identified issues or weaknesses are adequately documented and tracked within plans of action and milestones.		X	X
24. We recommended the ASIT fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to prevent the use of prohibited software on agency devices.	X	X	X
25. We recommended the ASIT develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.	X	X	X
26. We recommended the ASIT implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.	X	X	X

[6] Similar to Recommendation 10, the deficiency addressed in this recommendation has been communicated to VA in previous years, however this is the first year it was included in the report narrative. Therefore, while it is technically a new recommendation it is not a new issue.