STATEMENT OF MICHAEL BOWMAN
OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS
DIRECTOR OF INFORMATION TECHNOLOGY AND SECURITY AUDITS DIVISION
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION
COMMITTEE ON VETERANS' AFFAIRS, U.S. HOUSE OF REPRESENTATIVES
HEARING ON
CYBERSECURITY AND RISK MANAGEMENT AT VA:
ADDRESSING ONGOING CHALLENGES AND MOVING FORWARD
JUNE 7, 2022

Chairman Mrvan, Ranking Member Rosendale, and members of the Subcommittee, thank you for the opportunity to discuss the Office of Inspector General's (OIG) oversight of the Department of Veterans Affairs' (VA) information technology (IT) security program. Our statement discusses the many challenges VA faces and the limited progress it has made in ensuring the confidentiality, integrity, and availability of VA systems and data.

VA CYBERSECURITY CHALLENGES

As the second largest federal agency, VA relies on IT systems and networks to advance nearly every aspect of its mission. These IT systems are critical to the provision of 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 tremendously complex undertaking. Safeguarding the secure operation of the systems and networks that contain this sensitive data is essential, especially with the wide availability and effectiveness of internet-based hacking tools. Without proper measures, 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 by VA's obsolete legacy systems. These antiquated 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 Given the risks associated with using outdated systems, internal controls over operations take on even greater importance to sustain the integrity, confidentiality, and reliability of critical data while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. To the extent that VA does not properly manage and secure its 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.

This statement focuses on the most pressing issues identified in the recently released audit required by the Federal Information Security Modernization Act of 2014 (FISMA). It also discusses possible corrective actions that VA could take to achieve meaningful change, and highlights ongoing OIG initiatives that are meant to assist VA in improving IT security.

IT SECURITY OVERSIGHT

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 13, 2022, the OIG released its FISMA audit of VA for fiscal year (FY) 2021.[2] This is the 22nd consecutive year that the OIG has reported on the extent to which VA has IT safeguards in place consistent with the Act's requirements. The audit evaluated select management, technical, and operational controls supporting 50 major applications and general support systems hosted at 24 VA facilities, including VA's four major data centers.

In 2021, the OIG testified before this Subcommittee on VA's cybersecurity challenges and reviewed the 26 recommendations in the FY 2020 FISMA audit. The recently released FY 2021 FISMA audit included the same 26 recommendations, which reflects VA's limited progress. Of the 26 recommendations, 23 have been included in every FISMA audit dating back to at least 2018. An appendix to this statement provides information on which of these recommendations were also made to VA in the three most recent FISMA audits. The number of persistent problems identified underscores VA's slow progress in making major improvements and impactful change in their security program.

The FISMA audit can be considered a scorecard of an agency's IT security program. The OIG is consistent in its approach to the annual audit in order to track VA's progress over time in addressing the identified security concerns. While VA has made some progress in certain areas of their security program, these can best be characterized as incremental improvements in addressing the deficiencies the audit team has repeatedly identified. The OIG recognizes that VA is operating in a very challenging environment, with a large, decentralized organization and

[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 2021*, April 13, 2022.

many outdated systems that are being upgraded or replaced. These challenges continue to impede VA's progress in addressing their security program deficiencies.

The OIG has increased its oversight of IT security projects and products in recent years, including the launch of an IT security inspection program. That program focuses on reviewing sites not evaluated, or that underperformed, in the annual FISMA audit. The goal is to broaden oversight of VA's IT security enterprise by identifying persistent issues and trends at these sites, with the expectation that enacting changes at the local level can spur progress in addressing system-wide deficiencies.

FEDERAL INFORMATION SECURITY MODERNIZATION ACT COMPLIANCE

The FY 2021 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.

The related report's multiple repeat findings and 26 recommendations relate to deficiencies in the following areas:

- **Configuration Management Controls** are designed to ensure critical systems have appropriate security baseline controls and up-to-date vulnerability patches. 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 timely patched or securely configured to mitigate known and unknown information security vulnerabilities. Testing identified security control deficiencies related to unsecure web application servers, excessive permissions on database platforms, and vulnerable and unsupported third-party applications and operating system software. 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. The OIG made six recommendations related to configuration management controls.
- **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 domains, databases, and

mission-critical applications. For example, the audit team noted weak passwords on major databases, applications, and networking devices at many VA facilities. Specifically, numerous service accounts were identified that were not needed or had passwords that were not changed in over three years. Further, inconsistent reviews of networks and application user access resulted in inappropriate access rights being granted, as well as numerous generic (not tied to a specific user), 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 OIG made five recommendations related to access management.

- **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 of their positions. Without accurate and reliable investigation reporting, VA is at risk of allowing unnecessary or unauthorized access to sensitive systems and data. The OIG made five recommendations to address deficiencies in VA's security management program.
- **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 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 established timeframes, VA is at risk of not effectively providing mission-critical services to veterans and their families. Two report recommendations address the OIG's findings in contingency management controls.

The Assistant Secretary for Information and Technology generally concurred with the OIG recommendations and provided acceptable action plans for making significant progress on 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 reported in the FY 2021 audit of VA's Consolidated Financial Statements.[3]
- Improve deployments of security patches, system upgrades, and system configurations that will mitigate significant vulnerabilities and enforce a consistent process across all field offices.
- 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 minimize significant security risks.

The OIG will continue to monitor progress by reevaluating these issues in the next FISMA audit.

OTHER OVERSIGHT INITIATIVES

In addition to working on the FY 2022 FISMA assessment, the OIG has conducted further oversight work given the importance of VA's IT security efforts.

IT Security Inspection Program

As previously mentioned, the OIG launched an IT security inspection program in FY 2021 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 additional oversight and ensure VA focuses on IT security at all levels—local, regional, and national. The inspections focus on the same four areas as the FISMA audit, but at the facility level. They provide a framework of issues and recommended fixes that can be applied by the chief information officer or local IT leaders across VA. When persistent issues and themes are identified in IT security inspections, the expectation is that leaders at similar VA facilities will review the relevant reports and consider the applicability of findings to their own locations without waiting for an OIG inspection to occur. If local leaders are proactive in this regard, VA

[3] "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." VA OIG, *Audit of VA's Financial Statements for Fiscal Years 2021 and 2020*, November 15, 2021, Page i. 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.

is likely to make faster and more meaningful progress in addressing the deficiencies in their security program.

To date, four IT security inspections reports have been published.[4] These inspections reviewed compliance with federal security requirements at the VA Consolidated Mail Outpatient Pharmacies (CMOPs) located in Dallas, Texas, and Tucson, Arizona, a VA Outpatient Clinic in Austin, Texas, and the VA Financial Services Center also located in Austin. The inspection teams found numerous critical and high vulnerabilities in host systems at facilities that were not remediated within timeframes required by OIT policy. The teams also found inventories for networked devices that were not accurate and media that was not processed for sanitization, which increases the risk of unauthorized disclosure of veteran personal health information or personally identifiable information.

It is noteworthy that of the 24 recommendations made in these four reports, 12 have been successfully closed. This shows that these inspections can quickly identify issues that need remediation, and that VA has the capability to act quickly to make the necessary improvements. IT leaders at other VA facilities can and should review these findings and recommendations and make the needed changes now to ensure their IT security programs are adequate.

There are two IT security inspections of VA medical centers scheduled to publish before the end of this fiscal year, and additional inspections planned in FY 2023.

Veterans Data Integration and Federation Enterprise Platform Lacks Sufficient Security Controls

Last week, the OIG published a report reviewing security controls in VA's Veterans Data Integration and Federation Enterprise Platform (VDIF).[5] VDIF allows VA to share sensitive health information, such as medical chart notes and laboratory results, with the Department of Defense and participating community care providers through data-sharing networks. Exchanging health information across electronic platforms is essential to improving care for our nation's veterans. It also enables VA and community providers to develop comprehensive care plans, improve continuity of care, reduce duplicative tests, and avoid clinical errors when patients see different providers. The OIG audited whether OIT developed and implemented VDIF's security controls to ensure confidentiality, data integrity, and the safeguarding of sensitive health

---

[4] VA OIG, *Inspection of IT Security at the VA Outpatient Clinic in Austin, Texas*, June 22, 2021; *Inspection of IT Security at the VA Financial Services Center*, March 31, 2022; *Inspection of IT Security at the Consolidated Mail Outpatient Pharmacy in Dallas, Texas*, June 1, 2022; *Inspection of IT Security at the Consolidated Mail Outpatient Pharmacy in Tucson, Arizona*, June 1, 2022.

[5] VA OIG, *Veterans Data Integration and Federation Enterprise Platform Lacks Sufficient Security Controls*, June 1, 2022.

information according to federal standards. The review found OIT inappropriately categorized some security objectives for VDIF and did not adequately determine whether the implemented controls were correctly applied. Because of insufficient oversight, VDIF became operational with inadequate security controls, heightening the risk to personal health information of more than 10 million veterans.

The OIG made three recommendations, with the first two designed to ensure the VDIF system is categorized and assessed at the high-risk level, and that VA implement appropriate security controls. The assistant secretary for OIT and chief information officer requested the OIG close recommendations 1 and 2 and did not concur with them. The OIG maintains the system should be set at the high-risk level to protect veterans' sensitive information, which is the basis for recommendations 1 and 2. In fact, setting the system at a high-risk level is in line with OIT's own prior assessment. Further, VA clearly recognized the need for additional protection mechanisms and security controls for VDIF, as it applied a privacy overlay in the Enterprise Mission Assurance Support Service (eMASS) tool.[6] While the overlay added 71 additional controls in eMASS at the moderate level, it still did not address the controls needed at the high level. The OIG encourages VA to reconsider its nonconcurrence with these recommendations in order to more fully mitigate the potential risk of data breaches and privacy violations. The assistant secretary concurred with recommendation 3 and provided an acceptable action plan to conduct effective monitoring and oversight of security controls for IT systems.

VA Applications Lacked Federal Authorizations, and Interfaces Did Not Meet Security Requirements

In December 2021, the OIG published a report that reviewed whether OIT ensured that all cloud-based software it deployed met federal authorization requirements.[7] 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 (FedRAMP) policies are not followed and if the vendors do not meet federal authorization requirements. The OIG found that OIT granted security authorizations for applications that were not authorized by FedRAMP or VA. OIT also did not follow VA security requirements in developing interfaces that allow third parties to "plug into" VA systems and applications to send and retrieve data. Failure to comply

[6] eMASS is VA's governance, risk, and compliance tool through which they can implement additional security controls.
[7] VA OIG, *VA Applications Lacked Federal Authorizations and Interfaces Did Not Meet Security Requirements*, December 2, 2021.

with FedRAMP and VA security standards increases the risk that VA and veterans' data could be compromised. The report included four recommendations directed at OIT to address and remediate the security concerns identified. VA concurred with all four recommendations and provided acceptable action plans, and all report recommendations are currently open.

Ongoing IT Oversight

In addition to the planned IT security inspections, the OIG has other projects in progress that focus on IT security issues, including these three:

First, the OIG is conducting a review of the Mission Accountability Support Tracker (MAST), a system that helps quantify the work that Veterans Benefits Administration's support services staff perform in response to employee requests for facility, equipment, and vehicle management; reasonable accommodation; and identification card issuance and renewal. Because staff use personally identifiable information in their work, the information could be compromised in an unauthorized, unsecured application. The review team is currently evaluating the merits of a complaint to the OIG hotline alleging that staff disregarded privacy procedures to more quickly use a workload tracking system without receiving the appropriate security authorization. The findings will be included in a report planned for release this summer.

Second, a review team is examining whether VA is effectively governing its Identity, Credential, and Access Management (ICAM) program, as required by the Office of Management and Budget (OMB). ICAM is a set of tools, policies, and systems that an agency uses to ensure the right individual has access to the right resource, at the right time, for the right reason in support of federal business objectives. Agencies use ICAM to unify IT services and improve physical access control, information security, and decision-making. The OIG is assessing allegations from another hotline complaint concerning VA's governance of its ICAM program. The allegations suggest there has been a lack of agreement within VA regarding roles and responsibilities for the ICAM program. The OIG is reviewing whether there has been a lack of cooperation among VA's governing entities and whether that has affected compliance with OMB's ICAM policy.

The third and most expansive oversight efforts continue to monitor facets of VA's Electronic Health Record Modernization program and other large-scale IT initiatives that will require improvements in planning and tremendous investments in resources and staffing to ensure they are properly protected and secured. The OIG will continue to pursue the most efficient and effective strategies to report on VA's progress and identify areas for advancement and corrective action.

CONCLUSION

While VA has made recent improvements in some aspects of information management and IT security, there remain considerable challenges. The OIG believes that VA's successful

implementation of open recommendations from oversight reports is vital to its efforts to address ongoing and emerging issues. The additional oversight OIG is providing through local-level IT security inspections and reviews of VA systems such as VDIF, MAST, and ICAM can help spur progress, especially if IT leaders across the enterprise proactively review and implement OIG recommendations that are relevant to the facilities and systems they manage.

Secure IT systems and networks are essential to VA's fundamental mission of providing eligible veterans and their families with benefits and services. VA's information security program and its practices must protect the confidentiality, integrity, and access to VA systems and data. The recurrence of IT security concerns 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.

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 2021	Audit Recommendation by Fiscal Year		
	2018	2019	2020
1. We recommended the Assistant Secretary for Information and Technology (ASIT) consistently implement an improved continuous monitoring program in accordance with the NIST Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions.		X	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 applicable VA employees and contractors and applicable investigation data are accurately tracked within the authoritative system of record.	X	X	X

FISMA Audit Recommendation for FY 2021	Audit Recommendation by Fiscal Year 2018	2019	2020
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.	X	X	X
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	X
19. We recommended the ASIT ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements.		X	X
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

FISMA Audit Recommendation for FY 2021	Audit Recommendation by Fiscal Year		
	2018	2019	2020
21. We recommended the ASIT ensure that VA's Cybersecurity Operations Center has full access to all security incident data to facilitate an agencywide 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	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