STATEMENT OF MICHAEL BOWMAN
DIRECTOR OF THE INFORMATION TECHNOLOGY SECURITY DIVISION
FOR THE OFFICE OF AUDITS AND EVALUATIONS,
OFFICE OF INSPECTOR GENERAL, DEPARTMENT OF VETERANS AFFAIRS
BEFORE THE
SUBCOMMITTEE ON TECHNOLOGY MODERNIZATION,
COMMITTEE ON VETERANS' AFFAIRS
US HOUSE OF REPRESENTATIVES
HEARING ON
"VA CYBERSECURITY: PROTECTING VETERAN DATA FROM EVOLVING THREATS"
NOVEMBER 20, 2024

Chairman Rosendale, Ranking Member Cherfilus-McCormick, and members of the Subcommittee, the Office of Inspector General (OIG) appreciates your focus on our oversight of VA's information technology (IT) security program. As the second largest federal agency, VA has a vast amount of veterans' sensitive personal information and data of other beneficiaries, patients, personnel, and contractors. Strict controls are needed to uphold the related requirements and responsibilities for protecting this information. Yet the inadequacy and overall ineffectiveness of VA's information security controls highlighted in this statement are not new. The concerns related to VA's cybersecurity programs have been the subject of several OIG congressional testimonies in 2019, 2021, and 2022.[1] This statement underscores the need to continue efforts to address the many persistent challenges VA faces and its incremental progress in ensuring the confidentiality, integrity, and availability of VA systems and data.

VA is not alone. Secure information storage and management are high-risk endeavors across the government.[2] Federal IT leaders are continually challenged to protect individuals' privacy and sensitive data. The OIG recognizes the success of many of those efforts, while acknowledging that it is a constant battle to keep pace with new and unrelenting threats. Various data breaches—

[1] VA OIG, *Statement of Nick Dahl, Deputy Assistant Inspector General for Audits and Evaluations, before the House Committee on Veterans' Affairs, Subcommittee on Technology Modernization*, November 14, 2019; VA OIG, *Statement of Michael Bowman, Director of IT Security Division, before the House Committee on Veterans' Affairs, Subcommittee on Technology Modernization*, May 20, 2021; VA OIG, *Statement of Michael Bowman, Director of IT Security Division, before the House Committee on Veterans' Affairs, Subcommittee on Technology Modernization*, June 7, 2022.

[2] Government Accountability Office, *High-Risk Series: Federal Government Needs to Urgently Pursue Critical Actions to Address Major Cybersecurity Challenges*, March 24, 2021.

within federal agencies and the private sector—have affected millions of individuals and have fueled ongoing concerns that personally identifiable information is not always being adequately protected. Due to advances in technology, hackers can more easily glean information about individuals from various data breaches and track someone's activities to further malicious or criminal schemes. Congress passed the Federal Information Security Modernization Act of 2014 (FISMA) in part to strengthen federal programs and practices.[3] FISMA provides a comprehensive framework to help ensure the effectiveness of information security controls that support federal operations and assets. It requires that each federal agency (including VA) develop, document, and implement an agencywide information security and risk management program, and that the respective OIG provide an annual evaluation of the agency's program and practices.

The FISMA audit can be considered a scorecard of an agency's IT security program. Therefore, the OIG is consistent in its approach to the annual audit to facilitate tracking VA's efforts over time in addressing 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's conclusions in the fiscal year (FY) 2023 FISMA audit that were published in May 2024 are not new or revelatory—rather, they repeat many of the same concerns the OIG has found for years.[4] In fact, all 25 OIG recommendations made in the FY 2023 FISMA audit are repeat recommendations from the prior annual report.[5] One of the 26 recommendations from the FY 2022 audit was closed as implemented because VA has made significant improvements in the timely notification and resolution of computer security incidents.

This statement focuses on cybersecurity challenges, the major issues identified in the most recent FISMA audit (FY 2023) and persistent concerns, possible corrective actions that VA could take to achieve meaningful change, and additional ongoing OIG initiatives that are meant to assist VA in improving IT security.

VA'S CYBERSECURITY CHALLENGES

The OIG recognizes and appreciates that managing VA cybersecurity is an immensely difficult task. The sheer size and complexity of VA's IT systems present a monumental data protection challenge. VA's IT systems are critical to the provision of medical care and a range of benefits

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

[4] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, May 14, 2024.

[5] The OIG's FISMA engagement audits VA's information security program each year and reevaluates the status of prior year recommendations. Therefore, the FY 2024 audit will be released in FY 2025.

and services to millions of veterans, their families, survivors, and caregivers. These missions require VA to store, manage, and provide secure access to enormous amounts of sensitive data, such as veterans' medical records, benefits determinations, financial disclosures, and education records. VA's ever-growing list of applications and data repositories, whether on premises or in service provider clouds, includes high-impact targets for cybercriminals. IT staff must protect massive amounts of data and large legacy systems, alongside newer IT services and applications that are specific to VA's administrations and other program office locations.

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. Security failures can also undermine the trust of those whose information VA is charged with protecting and potentially affect their level of engagement with programs and services.

VA HAS NOT ADEQUATELY ADDRESSED THE OIG'S REPEAT FISMA FINDINGS AND RECOMMENDATIONS

For the most recently completed FISMA audit, the OIG assessed VA's IT security program through personnel inquiries, observations, and tests of selected controls supporting 45 major applications and general support systems at 23 VA facilities and the VA Enterprise Cloud.[6] The FY 2023 audit found VA has made some progress developing, documenting, and distributing significant policies and procedures. However, VA still faces challenges implementing components of its agencywide information security risk management program to meet FISMA requirements. The FY 2023 audit identified ongoing significant deficiencies related to the controls for configuration and change management, access, as well as insufficient service continuity practices. Collectively, these controls and practices are designed to protect mission-critical systems from unauthorized access, alteration, destruction, and interruptions to services and operations.

VA Has Made Limited Progress, but Significant Challenges Remain

In FY 2023, VA's Chief Information Officer continued an Enterprise Cybersecurity Strategy Program (ECSP) to implement VA's new *Cybersecurity Strategy* launched in 2022.[7] However, the OIG found issues remain with the consistent application of the security program and practices across VA's portfolio of systems. VA needs to ensure adequate controls and risk management procedures are applied to all systems and applications in order to fully address

[6] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, May 14, 2024.

[7] VA, *Cybersecurity Strategy*, October 13, 2021. The Chief Information Officer is also the Assistant Secretary for the Office of Information Technology. For consistency in this statement, they will only be referred to as the Chief Information Officer.

previously identified weaknesses. The ECSP team has launched several high-level action plans to address previously identified security failings and the IT "material weakness" reported as part of the Consolidated Financial Statement Audit.[8] As part of the ongoing ECSP efforts, the OIG noted improvements related to recommended actions to achieve these outcomes:

- Increased visibility of infrastructure platforms and host-based protection solutions.
- Continued maturation of processes related to developing and maintaining assessment and authorization documentation within VA's Governance, Risk, and Compliance tool.
- Enhanced identification, notification, and remediation of security incidents.
- Improved data quality related to personnel background investigations and more consistent risk designations for positions across the organization.

However, these actions and related controls require time to mature and demonstrate their effectiveness. Additionally, the OIG determined that VA needs to apply controls in a comprehensive manner across its information systems to be considered consistent and fully effective. Accordingly, OIG auditors have repeatedly seen information system security deficiencies similar in type and risk level to prior years' findings and an overall inconsistent implementation and enforcement of the security program. Although VA has continued to develop its enterprise-wide risk and security management processes, the OIG is still identifying deficiencies related to overall governance. These include risk management processes, control assessments, Plans of Action and Milestones, Authority to Operate processes, and system security plans. The risk-mitigation strategies discussed in the following sections are essential for protecting VA's mission-critical systems.

Highlights of the OIG's FY 2023 FISMA Audit Findings

As mentioned earlier, the FY 2023 FISMA report contained multiple findings and 25 recommendations—all repeated from the previous year—for improving VA's information security program that focus on these areas:

- **Configuration Management Controls** are designed to ensure critical systems have appropriate security baseline restrictions and up-to-date vulnerability patches implemented. Yet the OIG continues to identify insufficient configuration management controls, which are also used for accurate system and software inventories, as well as

[8] "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 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. VA, *FY 2024 Agency Financial Report*, November 15, 2024, pp. 115–149.

system configurations. VA has instituted high-level policy guidelines for mandatory configuration settings for information technology hardware, software, and firmware. However, OIG testing identified security control deficiencies related to unsecured web application servers, excessive permissions on database platforms, vulnerable and unsupported third-party applications and operating system software, and a lack of common platform security standards and monitoring across the enterprise. Security deficiencies could allow any system and database user to gain unauthorized access to critical system information.

- **Identity Management and Access Controls** help make certain that password standards are consistently implemented across the enterprise and that user accounts are monitored to enforce access privileging limitations 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, VA's 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 ensure only legitimate users have access to specific systems and to prevent access by both internal and external unauthorized users who seek to improperly modify or destroy sensitive data.
- **Agencywide Security Management Program Controls** make sure that system security controls are effectively and continuously monitored, and risks are effectively remediated through corrective action plans or compensating 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. Inadequate security documentation may result in insufficient awareness and management of system risks and deficiencies as well as ineffective continuous monitoring of security controls.

  Also, periodic personnel background reinvestigations were not performed on a timely basis or effectively tracked, and personnel were not being investigated at the level appropriate to their positions.

  Overall, the OIG found that VA had not consistently implemented components of its agencywide information security risk management program to meet FISMA requirements, despite having established an enterprise risk management program. The program's policies, procedures, and documentation were not routinely applied or carried out across all VA systems. For example, system security risks previously identified by VA were not always

documented in corresponding remediation plans or considered in risk management decisions. Without accurate and reliable reporting, VA is at risk of allowing unnecessary or unauthorized access to sensitive systems and data.

- **Contingency Planning Controls** help ensure the continuity of mission-critical systems and business processes or their restoration in the event of a disaster or emergency. Mission-critical systems at VA include those that support the day-to-day operations at over 1,000 healthcare facilities nationwide and provide recurring benefit 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 audit team concluded that plans were not consistently tested in accordance with VA policy requirements. If critical business functions are not recovered within the set time frames, VA is at increased risk of not effectively providing essential services.

Corrective Actions VA Could Take for Meaningful Change

The Chief Information Officer concurred with 15 of the OIG's recommendations and provided acceptable action plans for implementation. VA did not concur with the remaining 10 recommendations, despite having done so with similar recommendations in previous years. For most of these nonconcurrences, VA argued that their compliance percentage was adequate, stating they achieved above 95 percent. However, VA was unable to provide the OIG with evidence to support their claims. When these same areas were tested by the OIG, the team identified numerous examples of critical and high-risk vulnerabilities, such as not applying security updates to financial management systems, as well as inconsistent implementation of information security policy across the enterprise. Accordingly, the OIG stands by its findings and recommendations and encourages VA to commit to improving remediation processes and ensuring that all significant security vulnerabilities are effectively mitigated across critical systems and platforms.

Based on its overall audit work, the OIG contends 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 2024 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

- 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 track VA's work and review these same areas in the ongoing FY 2025 and future FISMA audits until all proposed actions are successfully implemented.

THE OIG'S INFORMATION SECURITY INSPECTION PROGRAM OVERSIGHT

In addition to working on the FY 2024 FISMA audit, the OIG has been developing and expanding its Information Security Inspection Program (ISIP) to review VA sites not evaluated under the annual FISMA audits or facilities that underperformed in prior audits. These inspections provide additional oversight opportunities and underscore the need for VA to focus on IT security at all levels—local, regional, and national. The ISIP focuses on the same four areas as the FISMA audit, but at the facility level rather than at the regional or enterprise levels. The inspections provide a framework for assessing a consistent list of issues and for recommending fixes that can be applied by a Chief Information Officer or local facility IT leader. ISIP reports are written not just for the site at issue. All VA facility leaders and personnel at similar types of facilities can proactively address the identified failings and related themes in the ISIP reports by considering their applicability to their own locations without waiting for an OIG inspection to occur. Doing so would position VA to make faster and more meaningful advances in addressing deficiencies in their security program.

To date, 18 information security inspection reports have been published under ISIP.[9] These inspections reviewed compliance with federal security requirements at a variety of VA locations, including medical centers and healthcare systems; Consolidated Mail Outpatient Pharmacies; the VA Financial Services Center in Austin, Texas; the Health Eligibility Center in Atlanta, Georgia; a VA outpatient clinic; and a rehabilitation clinic. The inspection teams found numerous critical and high-risk vulnerabilities in host systems at facilities that were not remediated within the time frames required by VA policy. The teams also found inventories for networked devices that were inaccurate and IT media that were not processed for sanitization. These security issues increase the risk of unauthorized disclosure of veterans' personal health information or personally identifiable information.

It is noteworthy that of the 131 recommendations made in these 18 reports, 92 (about 70 percent) have been successfully closed to date. This shows that these inspections can quickly identify issues that need remediation, and that VA has the capability to act promptly to make the necessary improvements. There are two additional ISIP inspections in various stages of

[9] All ISIP reports can be found on the OIG website.

completion as of November 18, 2024. The OIG is encouraged by the VA facilities' responsiveness to ISIP recommendations and will continue to refine the program to make it as effective and impactful as possible.

CONCLUSION

VA's fundamental mission of providing timely and effective benefits and services to veterans is dependent on deploying secure IT systems and networks. VA's information security program must also protect the confidentiality, integrity, and availability of its systems and data. The recurrence of OIG's IT security findings indicates the need for vigilance and investments that will speed VA's incremental improvements to effect more meaningful change. The OIG's annual FISMA audit has never detected improper access or successful malicious incursions into VA's systems. However, until proven processes are in place to ensure adequate controls across the enterprise, VA's mission-critical systems and sensitive data remain at risk. While VA has worked to implement initiatives and has made some progress in aspects of information management, there continue to be considerable challenges. VA still has a long way to go to appropriately secure sensitive information and major systems. Many pervasive IT security weaknesses remain, leaving VA with unacceptable risks.

The additional oversight OIG is providing through local-level information security inspections can help spur improvements, especially if local IT leaders across the enterprise proactively review and carry out OIG recommendations that are relevant to the facilities and systems they manage. The OIG believes that VA's successful implementation of the FISMA audit recommendations is vital to efforts to address ongoing and emerging issues. And finally, VA should continue to work with oversight personnel at the OIG, Congress, and Government Accountability Office to ensure that appropriate risk-based and cost-effective IT security programs, policies, and procedures are in place to secure VA's information, operations, and assets.

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