US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the Health Eligibility Center in Atlanta, Georgia

Information Security Inspection	24-01232-02	November 13, 2024

BE A
VOICE FOR
VETERANS

REPORT WRONGDOING

vaoig.gov/hotline | 800.488.8244

OUR MISSION

To serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

CONNECT WITH US

Subscribe to receive updates on reports, press releases, congressional testimony, and more. Follow us at @VetAffairsOIG.

PRIVACY NOTICE

In addition to general privacy laws that govern release of medical information, disclosure of certain veteran health or other private information may be prohibited by various federal statutes including, but not limited to, 38 U.S.C. §§ 5701, 5705, and 7332, absent an exemption or other specified circumstances. As mandated by law, the OIG adheres to privacy and confidentiality laws and regulations protecting veteran health or other private information in this report.

Visit our website to view more publications.
vaoig.gov

Executive Summary

Information security controls protect VA systems and data from unauthorized access, use, modification, and destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm to conduct an annual audit of VA's information security program and practices.[1] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget and the National Institute of Standards and Technology (NIST).

The fiscal year (FY) 2023 FISMA audit indicated that VA continues to face significant challenges meeting the law's requirements. The audit made 25 recommendations to VA, including repeat recommendations included addressing deficiencies in configuration management, contingency planning, security management, and access controls.[2] Appendix A details these recommendations.

In 2020, the OIG started an information security inspection program. These inspections assess whether VA facilities are meeting federal security requirements related to four control areas the OIG determined to be at highest risk. Typically, facilities selected for these inspections either were not included in the annual audit sample or had previously performed poorly. Appendix B presents background information on federal information security requirements.

For this inspection, the OIG selected the Health Eligibility Center (HEC) in Atlanta, Georgia, because it had performed poorly during the fiscal year 2022 FISMA audit.[3] The HEC was one of 23 locations selected for the FISMA audit and the FISMA report made general recommendations to the agency with no specific recommendations to the HEC. This inspection's scope and methodology are detailed in appendix C.

The inspections focused on four security control areas:

1. **Configuration management controls** identify and manage security features for all hardware and software components of an information system.[4]
2. **Contingency planning** controls provide reasonable assurance that information resources are protected from unplanned interruption, minimize risk, and provide for

[1] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No 23-01105-69, May 14, 2024.

[2] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*.

[3] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023.

[4] GAO, *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G, February 2009.

recovery of critical operations should interruptions occur.[5] Contingency planning also includes physical and environmental controls, such as fire protection, water damage protection, and emergency power and lighting.

3. **Security management controls** "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[6]
4. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. Access includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal.[7]

Although the findings and recommendations in this report are specific to the HEC, other VA facilities could benefit from reviewing this information and considering these recommendations.

What the Inspection Found

The OIG identified deficiencies in three of the four areas: configuration management, security management, and access controls. Contingency planning had no deficiencies.

Configuration Management Controls Had Three Deficiencies

The HEC had deficiencies in three configuration management controls:

- **Vulnerability remediation.** Analysis of the Office of Information and Technology (OIT) vulnerability scan results and plans of action and milestones indicated that the facility did not create plans of action and milestones for vulnerabilities persisting past the VA deadlines of 30 days for critical vulnerabilities and 60 days for high vulnerabilities.
- **System life-cycle management.** The OIG team found that HEC's network devices were running outdated software, including software not securely configured.
- **Unauthorized software.** The HEC was not remediating unauthorized software on the network.

Contingency Planning Controls Had No Deficiencies

To assess contingency planning controls, the inspection team interviewed the area manager, the information system security officer, members of OIT's Office of Development, Security and

[5] GAO, *FISCAM*.

[6] GAO, *FISCAM*.

[7] GAO, *FISCAM*.

Operations, and facility management. The team also reviewed local policies and procedures. The OIG found that encrypted backups of the Workload Reporting and Productivity Assessing (WRAP) application file server and data were stored at a secure offsite location.[8] Accordingly, the OIG did not make any recommendations for improvement.

Security Management Controls Had One Deficiency

A facility's "security management program should establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures."[9] The OIG identified approximately 3.3 million veterans' records containing sensitive personal information that were not encrypted on the WRAP application file server. VA security policy requires the encryption of sensitive information hosted on computer systems.[10] NIST also allows agencies "the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields."[11] HEC representatives stated that the WRAP application went live in February 2016, which they thought was before VA's requirement for implementing encryption controls became effective. However, the VA and NIST requirement for encrypting data was established in 2010.[12] A compromise of this server could result in a data breach of veteran sensitive personal information, potential financial loss, and reputational loss to VA.

Access Controls Had Two Deficiencies

Access controls provide reasonable assurance that computer resources are restricted to authorized individuals.[13] At the HEC, the inspection team reviewed access and environmental control elements over the computer room, communication closets, and a file room that contained sensitive records. The inspection team found deficiencies with access controls in the inventory of facility keys, and in logging administrative actions, log retention and log reviews for the WRAP application file server.

[8] The WRAP application is a tool that tracks Health Eligibility Center (HEC) Enrollment Eligibility Department (EED) and Income Verification Department (IVD) employees' workload and performance.

[9] GAO, *FISCAM*.

[10] VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program,* February 2021.

[11] NIST Special Publication 800-53.

[12] VA Handbook 6500 and NIST Special Publication 800-53.

[13] NIST Special Publication 800-53.

What the OIG Recommended

The OIG made the following recommendations to the assistant secretary for information and technology and chief information officer:

1. Improve vulnerability management processes to ensure all vulnerabilities are identified and that plans of action and milestones are created for vulnerabilities that cannot be mitigated by VA deadlines.
2. Implement a more effective system life-cycle process to ensure network devices are running authorized software and operating systems that are configured to approved baselines and free of vulnerabilities.
3. Ensure all file systems holding veteran information are encrypted in accordance with NIST and VA policy requirements.

The OIG made two recommendations to the VA HEC director in conjunction with the assistant secretary for information and technology:

4. Maintain an accurate inventory of personnel with key access to the facility.
5. Enable improved audit logging capability to monitor administrator access to sensitive information hosted on the Workload Reporting and Productivity Assessing file server.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 through 5 and requested recommendation 4 be closed due to corrective actions he said were completed.[14] To support the closure request, the assistant secretary provided sufficient evidence showing that the actions were taken to address recommendation 4. Therefore, the OIG considers recommendation 4 closed. For the other recommendations, the OIG will monitor implementation of the planned actions and will close the remaining recommendations when VA provides evidence demonstrating progress in addressing the identified issues.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations.

[14] The full text of the assistant secretary's response is included in appendix D.

Contents

Abbreviations

FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAO	Government Accountability Office
HEC	Health Eligibility Center
IT	information technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information and Technology
OMB	Office of Management and Budget
WRAP	Workload Reporting and Productivity Assessing

Introduction

Information security controls protect VA systems and data from unauthorized access, use, modification, or destruction. To determine compliance with the Federal Information Security Modernization Act of 2014 (FISMA), the VA Office of Inspector General (OIG) contracts with an independent public accounting firm that conducts an annual audit of VA's information security program and practices.[15] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST). Appendix A details the fiscal year (FY) 2023 FISMA audit's recommendations.

In 2020, the OIG started an information security inspection program. These inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[16] Appendix B presents information about FISMA and other federal criteria and standards discussed in this report. Typically, facilities selected for these inspections either were not included in the annual FISMA sample or had previously performed poorly. Appendix C provides more detail on the inspection's scope and methodology.

The OIG conducted this inspection to determine whether the Health Eligibility Center (HEC) in Atlanta, Georgia, was meeting federal security guidance. The OIG selected the HEC because it had previously performed poorly during the FY 2022 FISMA audit.[17] Although the findings and recommendations in this report are specific to the HEC, other facilities across VA could benefit from reviewing this information and considering these recommendations.

Security Controls

Both OMB and NIST provide the criteria for the implementation of security controls.[18] These criteria provide requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.

According to VA Directive 6500, responsibility for developing and maintaining information security policies, procedures, and control techniques lies with the assistant secretary for information and technology, who also serves as VA's chief information officer. In addition, VA Handbook 6500 describes the risk-based process for selecting system security controls,

[15] Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. §§ 3551–3558; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No 23-01105-69, May 14, 2024.

[16] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No 23-01105-69, May 14, 2024.

[17] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*.

[18] OMB, "Security of Federal Automated Information Resources," app. III in OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016; NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations,* September 23, 2020.

including the operational requirements.[19] VA established guidance outlining both NIST- and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.[20]

This information security inspection focused on four security control areas and selected based on their level of risk, as shown in table 1.

Table 1. Security Controls Evaluated by the OIG

Control area	Purpose	Examples evaluated
Configuration management	Identify and manage security features for all hardware and software components of an information system	Component inventory, baseline configurations, configuration settings, change management, vulnerability management, and flaw remediation
Contingency planning	Provide reasonable assurance that information resources are protected from unplanned interruption, minimize risk, and provide for recovery of critical operations should interruptions occur	Backing up critical systems and storing backups of critical systems at a secure offsite facility
Security management	Establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures	Risk management, assessment, authorization, and monitoring
Access	Provide reasonable assurance that computer resources are restricted to authorized individuals	Access, identification, authentication, audit, and accountability, including related physical security controls

Source: VA OIG analysis.

Without these critical controls, VA's systems would be at risk of unauthorized access or modifications. A cyberattack could disrupt access to, destroy, or allow malicious control of personal information belonging to VA patients, dependents, beneficiaries, employees, contractors, or volunteers.

Office of Information and Technology Structure and Responsibilities

The assistant secretary for information and technology, who also serves as the chief information officer, leads the Office of Information and Technology (OIT). According to VA, OIT delivers

[19] VA Handbook 6500, *Risk Management Framework for VA Information Systems: VA Information Security Program*, February 24, 2021.

[20] VA Handbook 6500.

available, adaptable, secure, and cost-effective technology services to VA. The Cybersecurity Operations Center, which is part of OIT's Office of Information Security, is responsible for protecting VA information and information systems by identifying and reporting emerging and imminent threats and vulnerabilities.

OIT's Office of Development, Security, and Operations focuses on software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration. The Office of Development, Security, and Operations; End User Operations; Office of Information Security; and Cybersecurity Operations Center are the OIT offices relevant to the areas assessed at the HEC, as shown in figure 1.

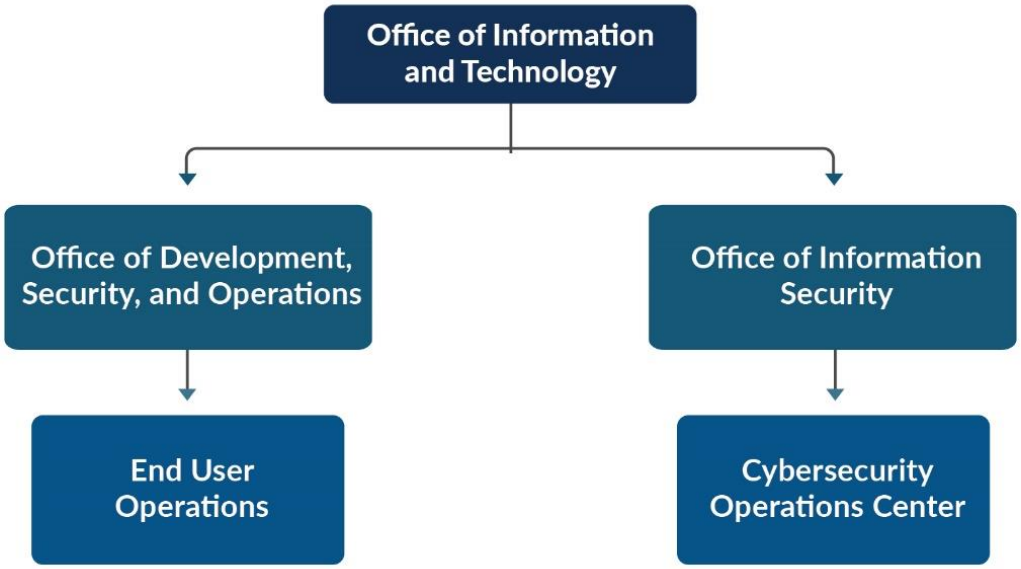
Office of Information and Technology
Office of Development, Security, and Operations
Office of Information Security
End User Operations
Cybersecurity Operations Center

Figure 1. *Organizational structure of Office of Information and Technology entities relevant to this inspection.*
Source: VA OIG analysis.

End User Operations provides on-site support to information technology (IT) customers across all VA administrations and program offices, including direct support of approximately 400,000 VA employees and approximately 100,000 contractors with government furnished IT equipment and access. End User Operations provisions computing devices, activates new facilities, executes local system implementations, and engages VA's customers across the nation to meet IT support needs. OIT assigns infrastructure operations services' personnel to the HEC, including system stewards responsible for managing system plans of action and milestones to ensure all assessed and scanned vulnerabilities are documented.

Results of Previous Projects

The OIG's FY 2023 FISMA audit, conducted by independent public accounting firm CliftonLarsonAllen LLP, evaluated 45 major applications and general support systems hosted at

23 VA facilities and tested selected security and privacy controls outlined by NIST.[21] CliftonLarsonAllen LLP made 25 recommendations, which are listed in appendix A. All 25 recommendations were repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[22] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls. The Government Accountability Office (GAO) has also found that VA has a deficient information security program, noting in 2019 that VA faced several security challenges while securing and modernizing its information systems, including effectively implementing information security controls; mitigating known vulnerabilities; establishing elements of its cybersecurity risk management program; identifying critical cybersecurity staffing needs; and managing IT supply chain risks.[23]

Health Eligibility Center

The HEC, located within the VA Atlanta Healthcare System, determines eligibility for VA healthcare benefits and manages veterans' enrollments. Staff at the HEC made 609,115 final eligibility determinations in FY 2023. Every healthcare applicant must deliver physical paper records—or send them via fax machine—to the HEC. These documents are scanned into the Workload Reporting and Productivity Assessing (WRAP) application, at which point HEC staff determine whether the applicant is eligible to receive healthcare benefits.[24] In FY 2024, the HEC had an annual budget of about $54.7 million.

[21] OMB, Circular A-130, app. 3, "Security of Federal Automated Information Resources," November 28, 2000, which defines a general support system as an interconnected set of information resources under the same direct management control which share common functionality.

[22] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No 23-01105-69, May 14, 2024. See Appendix B for more information.

[23] GAO, *Information Security: VA and Other Federal Agencies Need to Address Significant Challenges,* GAO-20-256T, November 14, 2019.

[24] The WRAP application is a tool that tracks Health Eligibility Center (HEC) Enrollment Eligibility Department (EED) and Income Verification Department (IVD) employees' workload and performance.

Results and Recommendations

I. Configuration Management

According to the GAO's *Federal Information System Controls Audit Manual* (*FISCAM*), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle. The inspection team examined whether the HEC identified and remediated vulnerabilities within established times and securely configured its servers.

An effective configuration management process should be described in a configuration management plan and implemented according to the plan. OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities. Vulnerabilities that cannot be remediated by OIT's Enterprise Vulnerability Management are assigned to system personnel or the information security officer for action. This process helps to secure devices from attack.

Finding 1: The HEC Had Three Deficiencies in Configuration Management

The team concluded that the HEC had deficiencies in three configuration management controls:

- **Vulnerability remediation.** Analysis of OIT vulnerability scan results and plans of action and milestones indicated that the HEC did not create plans of action and milestones for vulnerabilities not remediated within the 30- and 60-day limits set by VA.
- **System life-cycle management.** The OIG team found that HEC's network devices were running outdated software, including software not securely configured.
- **Unauthorized Software.** The HEC was not remediating unauthorized software on the network.

Vulnerability Remediation

VA's vulnerability management program can be improved. FISMA audits have repeatedly found deficiencies in the department's vulnerability management controls. Consistent with those findings, the team identified deficient controls at the HEC.[25]

[25] GAO, *FISCAM*. Vulnerabilities are "weaknesses in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."

Vulnerability management is the process by which an organization identifies, classifies, and reduces weaknesses. Vulnerability management also helps organizations assess risks and monitor the effectiveness of the overall security program. At VA, OIT conducts routine scans and separate random vulnerability scans. OIT uses the Information Central Analytics and Metrics Platform to report vulnerabilities to facilities for remediation. In calendar year 2023, OIT implemented a formal process to track the monitoring and remediation of vulnerabilities by using a plan of action and milestones vulnerability portal. However, at the time of the OIG's inspection, the new process had not been in place long enough to demonstrate that it will effectively remediate security vulnerabilities on time.

Discovered vulnerabilities that cannot be remediated within established timelines are entered into a plan of action and milestones for remediation by the system steward. Information system stewards then use the Remediation Effort Entry Form to document the plan of action and milestones for each deficiency identified from the scan and to provide evidence that the deficiencies have been mitigated.[26]

NIST guidance calls for a severity level to be assigned to each vulnerability using the Common Vulnerability Scoring System.[27] The scoring system captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. The inspection's information security vulnerability remediation test work focused on the remediation of critical and high vulnerabilities in the agency approved timelines, as shown in table 2.

Table 2. Vulnerability Remediation Timelines by Severity Level

Severity score	Severity level	OIT time to remediate
9.0 - 10	Critical	30 days
7.0-8.9	High	60 days

Source: VA OIG analysis of VA's Development, Security, and Operations, Information System Vulnerability Management Plan, Version 1.0 March 28, 2022.

The inspection team compared OIT-provided network vulnerability scan results from the HEC against OIG scans conducted from March 18 through March 21, 2024. The team and OIT used the same vulnerability scanning tools. The OIG's scan results, however, indicated seven unique

[26] An information system steward is an agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

[27] "Vulnerability Metrics," NIST National Vulnerability Database, accessed August 7, 2023, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.1, Specification Document, Revision 1," Forum of Incident Response and Security Teams, accessed August 7, 2023, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

critical vulnerabilities hosted on 44 network systems and devices and 14 unique high vulnerabilities on 52 hosts that were not detected by OIT's scans. As of February 2024, the HEC had 22 critical vulnerabilities on 17 hosts and 42 high vulnerabilities on 164 hosts that persisted past the established deadlines. While the OIG and OIT used the same scanning tools, scanning results differ when vulnerability testing is conducted on different dates. Of the unmitigated vulnerabilities, 13 critical and 15 high vulnerabilities did not have plans of action and milestones laying out corrective actions.

System Life-Cycle Management

During the inspection, the team scanned the HEC servers' configurable settings for compliance to secure baselines. The OIG noted that 91 percent of servers (73 of 80) had software configuration settings that did not meet baseline security requirements; according to the Defense Information Systems Agency, these are classified as category 1 and category 2 security failures.[28] In accordance with VA policy, these servers should be securely configured as part of the standard system development life-cycle process, and systems should be configured using baselines that have been documented, formally reviewed, and agreed upon by management.[29] Category 1 failures would allow primary security protections to be bypassed allowing immediate access by unauthorized personnel or unauthorized assumption of superuser privileges. Category 2 failures have the potential to lead to unauthorized system access or activity. Baseline configurations serve as a basis for measurement against future changes to systems including the implementation of security and privacy controls.[30] Security configuration of servers is not just a defensive strategy but a proactive one that helps protect the confidentiality, continuous availability, and integrity of VA systems.

Use of Unauthorized Software

OIT uses endpoint management software to report unapproved software on computers. On March 21, 2024, the endpoint management software report for the HEC's network identified 60 different versions of unapproved software that were installed 169 times on the healthcare system's computers; however, the reports had not been reviewed by the systems OIT employees for actions to be taken to address the unapproved software. This software was installed without proper authorization or without a plan of action and milestones to mitigate the security deficiency. VA allows unauthorized software if there is a signed plan of action and milestones to

[28] The Defense Information Systems Agency's Application Security and Development Security Technical Implementation Guide Overview, V6 R1, dated July 24, 2024.

[29] VA Development, Security, and Operations, *Information System Vulnerability Management Plan,* Version 1.0, dated March 28, 2022.

[30] NIST Special Publication 800-53.

document the acceptance of risk.[31] By not remediating unauthorized software, VA has no assurance that corresponding system security and privacy plans have identified appropriate security controls for all components at the facility. Continuous monitoring facilitates ongoing awareness of system security and privacy issues and supports risk management.[32]

Finding 1 Conclusion

System vulnerabilities at the HEC were not always mitigated on time, and software did not meet baseline requirements. These vulnerabilities created security weaknesses on the HEC’s network that could be exploited by malicious individuals to gain unauthorized access to sensitive information or disrupt operations. Further, OIT did not take actions to address unauthorized software installed on computers within the HEC.

Recommendations 1–2

The OIG made the following recommendations to the assistant secretary for information and technology and chief information officer:

1. Improve vulnerability management processes to ensure all vulnerabilities are identified and that plans of action and milestones are created for vulnerabilities that cannot be mitigated by VA deadlines.
2. Implement a more effective system life-cycle process to ensure network devices are running authorized software and operating systems that are configured to approved baselines and free of vulnerabilities.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 2. For recommendation 1, the assistant secretary indicated that OIT will document and manage vulnerabilities that fall out of compliance with the VA established time frames with a Plan of Actions and Milestone (POAM). In response to recommendation 2, the assistant secretary indicated that OIT has implemented a process to identify, track, and remediate unauthorized software and ensure approval of baselines; further, all identified vulnerabilities are scheduled to be remediated by the end of October 2024. The full text of the assistant secretary’s response is included in appendix D.

[31] VA Technical Reference Model version 24.8.

[32] NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations,* September 2011.

OIG Response

For recommendations 1 and 2, the planned corrective actions are responsive to the intent of the recommendations. The OIG will monitor implementation of the planned actions and will close the recommendations when VA provides evidence demonstrating progress in addressing the issues identified.

II. Contingency Planning

According to *FISCAM*, “[r]outinely copying data files and software and storing these files at a secure, remote location are usually the most cost-effective actions that an entity can take to mitigate service interruptions.”[33] FISMA requires that each federal agency implement an information security program that includes “plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.”[34] Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions.[35] These may include minor interruptions, such as temporary power failures, as well as fires, natural disasters, and terrorism, which would require reestablishing operations at a remote location. To determine if the facility met federal guidance and VA requirements, the inspection team evaluated whether the WRAP application was encrypted and backed up to a secure location.

Finding 2: The Facility Had No Contingency Planning Deficiencies

To assess contingency planning controls, the inspection team interviewed the area manager, the information system security officer, members of OIT’s Office of Development, Security and Operations, and facility management. The team also reviewed local policies and procedures. The OIG found that encrypted backups of the WRAP application and data were stored at a secure offsite location. Accordingly, the OIG did not make any recommendations for improvement.

[33] GAO, *FISCAM*.

[34] FISMA § 3554(b)(8).

[35] GAO, *FISCAM*.

III. Security Management

According to *FISCAM*, security management controls establish a framework and continuous cycle for assessing risk, developing security procedures, and monitoring the effectiveness of the procedures. The inspection team evaluated whether sensitive information within the WRAP applications had been secured, and whether the HEC was monitoring for and remediating unapproved software at the HEC.

Finding 3: The HEC Had One Deficiency in Configuration Management

To assess security controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies. These included documentation from the Enterprise Mission Assurance Support Service, VA's cybersecurity management service for workflow automation and continuous monitoring. Among the topics reviewed were application user management and security of sensitive information for known deficiencies. The team interviewed the information systems security manager, the information systems security officers, and the area manager. The team also conducted a walk-through of the facility.

Sensitive Veterans' Information Not Encrypted

The OIG identified about 3.3 million veterans' records containing sensitive personal information that were unencrypted on the WRAP application file server. While WRAP application backup tapes and data were encrypted, the production data on the file server were not encrypted. NIST allows agencies "the flexibility to encrypt information on system components or media or encrypt data structures, including files, records, or fields."[36] VA also requires the encryption of sensitive information.[37] HEC representatives stated that the WRAP application went live in February 2016, which they thought was before VA's requirement for encryption; however, the VA and NIST requirement for encrypting data was established in 2010.[38] A compromise of this server could result in financial and reputational loss to VA which is entrusted to protect sensitive veteran data.

Finding 3 Conclusion

Veteran information within HEC's WRAP system was not encrypted. Without effective security management processes, managers may not be able to properly respond, may lose public trust, and may incur costs to recover from a loss of data or destruction of computer resources.

[36] NIST Special Publication 800-53.

[37] VA Directive 6500.

[38] VA Handbook 6500.6, March 12, 2010, and NIST Special Publication 800-53 Revision 3, August 2010.

Recommendation 3

The OIG made the following recommendation to the assistant secretary for information and technology and chief information officer:

3. Ensure all file systems holding veteran information are encrypted in accordance with NIST and VA policy requirements.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 3. The assistant secretary indicated that OIT is in the process of implementing a new system that will ensure all file systems are encrypted in accordance with VA policy requirements, and noted that this would be completed by November 1, 2024. The full text of the assistant secretary's response is included in appendix D.

OIG Response

The planned corrective actions are responsive to the intent of recommendation 3. The OIG will monitor implementation of the planned actions and will close the recommendation when VA provides evidence demonstrating progress in addressing the issue identified.

IV. Access Controls

Previous FISMA reports have repeatedly identified access controls as a nationwide issue for VA. Access controls, including boundary protections, sensitive system resources, physical security, and audit and monitoring controls, provide reasonable assurance that computer resources are restricted to authorized individuals.[39] Access controls can be both logical and physical. Logical access controls require users to authenticate themselves, limit the resources that users can access, and restrict actions users can take. Physical access controls involve restricting physical access to computer resources and protecting them from loss or impairment. Identification, authentication, and authorization controls ensure that users have the proper access, and that access is restricted to authorized individuals. At the HEC, the inspection team reviewed access and environmental control elements over the computer room, communication closets, and a file room that contained sensitive records.[40]

Finding 4: The HEC Had Deficiencies in Two Access Controls

To evaluate the HEC's access controls, the inspection team reviewed physical access, environmental controls, logging and monitoring, and local policies and procedures; conducted walk-throughs of the facility; and analyzed audit logs.[41] The OIG found issues with key inventory and audit and monitoring.

Key Inventory

The inspection team discovered that physical access to the facility and its IT resources was not effectively controlled. Specifically, there was no inventory of facility keys to allow the OIG to determine whether all keys were on hand or that they had been issued only to authorized individuals. While the facility had a process for assigning keys, there was no process for maintaining a key inventory. Facility personnel indicated that they were transitioning from physical key access to an automated physical access control system that restricted badge access to the server room, communication closets, and file room.

Audit and Monitoring

The OIG determined that improvements are needed for logging administrative actions, log retention, and log reviews for the WRAP application file server. These controls should be routinely used to assess the effectiveness of other security controls, to recognize an attack, and to investigate during or after an attack.[42] Although the HEC had deployed mechanisms to monitor

[39] NIST Special Publication 800-53.

[40] *FISCAM* critical elements for access controls are listed in appendix B.

[41] See appendix C for additional information about the inspection's scope and methodology.

[42] NIST Special Publication 800-53.

audit logs from the WRAP file server for some items—like server functionality—the auditing mechanism would not capture whether administrators accessed files on the server that contained sensitive information. Logs help with investigating security incidents and performing subsequent analysis. They provide information on which accounts were accessed and what actions were performed. If this information is not available, an investigation may be limited or unsuccessful in determining the unauthorized use or modification of information.

Finding 4 Conclusion

The HEC's access controls did not ensure that the key inventory to computer resources was protected from theft or damage. Additionally, comprehensive audit logging was not enabled to capture when administrators would access the WRAP file servers, which could be helpful when investigating security incidents and performing subsequent analysis. If the deficiencies are not corrected, the facility may not be able to properly respond, may lose public trust, and may incur costs to recover from a loss of data or destruction of computer resources.

Recommendations 4–5

The OIG made two recommendations to the VA HEC director in conjunction with the assistant secretary for information and technology:

4. Maintain an accurate inventory of personnel with key access to the facility.
5. Enable improved audit logging capability to monitor administrator access to sensitive information hosted on the Workload Reporting and Productivity Assessing file server.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 4 and 5 and requested recommendation 4 be closed due to corrective actions he said were completed. For recommendation 4, the assistant secretary reported that a key inventory was completed on July 31, 2024, and will be conducted on a semi-annual basis. Regarding recommendation 5, the assistant secretary stated that OIT is in the process of replacing its WRAP file server that will record administrator access to sensitive information and log files for monitoring purposes. The full text of the assistant secretary's response is included in appendix D.

OIG Response

For recommendations 4 and 5, the planned corrective actions are responsive to the intent of the recommendations. The assistant secretary provided sufficient evidence to support that actions taken in response to recommendation 4 were complete. The OIG considers recommendation 4 closed. For recommendation 5, the OIG will monitor implementation of the planned actions and will close the recommendation when VA provides evidence demonstrating progress in addressing the issues identified.

Appendix A: FISMA Audit for FY 2023 Report Recommendations

In the Federal Information Security Act of 2014 (FISMA) audit for fiscal year 2023, CliftonLarsonAllen LLP made 25 recommendations.[43] Of these, all 25 were repeat recommendations from the prior year. The FISMA audit assesses the agencywide security management program, and recommendations in the FISMA report are not specific to the Health Eligibility Center in Atlanta. The 25 recommendations made to the assistant secretary for information and technology are listed below.

1. 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.
2. 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.
3. Implement controls to ensure that system stewards and responsible officials obtain appropriate documentation prior to closing Plans of Action and Milestones.
4. 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.
5. Implement improved processes for reviewing and updating key security documentation, including control assessments on a risk-based rotation or as needed. Such updates will ensure all required information is included and accurately reflects the current environment.
6. Implement improved processes to ensure compliance with VA password policy and security standards on domain controls, operating systems, databases, applications, and network devices.
7. Implement periodic reviews to minimize accounts and permissions in excess of required functional responsibilities, and to remove unauthorized or unnecessary accounts.
8. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.

[43] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2023*, Report No 23-01105-69, May 14, 2024.

9. Implement improved processes for establishing and maintaining accurate investigation data within VA systems used for background investigations.
10. Strengthen processes to ensure appropriate levels of background investigations are completed for applicable VA employees and contractors.
11. Implement more effective automated mechanisms to continuously identify and remediate security deficiencies on VA's network infrastructure, database platforms, and web application servers.
12. Implement improved processes for tracking and resolving vulnerabilities that cannot be addressed within policy timeframes. Implement more effective patch and vulnerability management processes to mitigate identified security deficiencies and reduce applicable security risks.
13. Maintain a complete and accurate security baseline configuration for all platforms and ensure all baselines are appropriately monitored for compliance with established VA security standards.
14. Implement improved controls that restrict vulnerable medical devices from unnecessary access to the general network.
15. Enhance procedures for tracking security responsibilities for networks, devices, and components not managed by the Office of Information and Technology to ensure vulnerabilities are remediated in a timely manner.
16. Implement improved processes to ensure that all devices and platforms are evaluated using credentialed vulnerability assessments.
17. Implement improved procedures to enforce standardized system development and change control processes that integrates information security throughout the life cycle of each system.
18. Implement improved procedures to ensure that system outages and disruptions are tracked to specific system boundaries and that interdependent systems are considered for the purposes of tracking and measuring against stated system recovery time objectives.
19. Ensure contingency plans for all systems and applications are updated and tested in accordance with VA requirements.
20. Ensure that systems and applications are adequately logged and monitored to facilitate an agencywide awareness of information security events.
21. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.

22. 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 POA&Ms.
23. Implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms.
24. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA applications and operations.
25. Implement improved procedures for monitoring contractor-managed systems and services and ensure information security controls adequately protect VA sensitive systems and data.

Appendix B: Background

Federal Information System Controls Audit Manual (FISCAM)

The Government Accountability Office developed *FISCAM* to give auditors and information system control specialists a specific methodology for evaluating the confidentiality, integrity, and availability of information systems. *FISCAM* groups controls into categories that have similar risks. To assist auditors in evaluating information systems, *FISCAM* maps control categories to National Institute of Standards and Technology (NIST) controls.

FISCAM breaks configuration management controls into the following critical elements.

- **Develop and document configuration management policies, plans, and procedures** at the entity, system, and application levels to ensure effective configuration management processes. These procedures should cover employee roles and responsibilities, change control, system documentation requirements, establishment of decision-making structure, and configuration management training.

- **Maintain current configuration information,** which involves naming and describing physical and functional characteristics of a controlled item, as well as performing activities to define, track, store, manage, and retrieve configuration items. Examples of these controls are baseline configurations, configuration settings, and component inventories.

- **Authorize, test, approve, and track changes** by formally establishing a change management process, with management's authorization and approval of the changes. This element includes documenting and approving test plans, comprehensive and appropriate testing of changes, and creating an audit trail to clearly document and track changes.

- **Conduct routine configuration monitoring** to determine the accuracy of the changes that should address baseline and operational configuration of hardware, software, and firmware.[44] Products should comply with applicable standards and the vendors' good security practices. The organization should have the ability to monitor and test to determine if a system is functioning as intended, as well as to determine if networks are appropriately configured and paths are protected between information systems.

- **Update software on a timely basis** by scanning software and updating it frequently to guard against known vulnerabilities. In addition, security software should be kept current by establishing effective programs for patch management, virus protection, and identification of other emerging threats. Software releases should be controlled to prevent

[44] Firmware are computer programs and data stored in hardware, typically in read-only memory, that cannot be written or modified during the execution of the program.

the use of noncurrent software. Examples of these controls are software usage restrictions, user-installed software, malicious code protection, security alerts, and advisories. Examples of controls in this element are vulnerability scanning, flaw remediation, malicious code protection, security alerts, and advisories.

- **Document and have emergency changes approved** by appropriate entity officials and notify appropriate personnel for follow-up and analysis of the changes. It is not uncommon for program changes to be needed on an emergency basis to keep a system operating. However, due to the increased risk of errors, emergency changes should be kept to a minimum.

FISCAM identifies the following critical elements for contingency planning:

- **Computerized operations criticality and sensitivity assessment** is an analysis of data and operations by management to determine which are the most critical and what resources are needed to recover and support them.
- **Prevent and minimize damage and interruption** by implementing backup procedures and installing environmental controls. These controls are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters. This control also includes effective maintenance, problem management, and change management for hardware.
- **A comprehensive contingency plan** or suite for related plans, should be developed for restoring critical applications; this includes arrangements for alternate processing facilities in case the usual facilities are damaged or cannot be accessed.
- **Contingency testing** determines whether plans will function as intended and can reveal important weaknesses which leads to plan improvement.

FISCAM has seven critical elements for security management:

- **Institute a security management program** that establishes policies, plans, and procedures clearly describing all major systems and facilities and that outlines the duties of those responsible for overseeing security as well as those who own, use, or rely on the organization’s computer resources. There should be a clear security management structure for systems and devices as well as for business processes. Examples of specific controls are system security plans, plan updates, activity planning, and resource allocation.
- **Assess and validate risk** by comprehensively identifying and considering all threats and vulnerabilities. This step ensures that agencies address the greatest risks and

appropriately decide to accept or mitigate risks. Examples of these controls are security certification, accreditation, categorization, and risk assessment.

- **Document and implement security control policies and procedures** that appropriately address general and application controls and ensure users can be held accountable for their actions. These controls, which are more general at the entity-wide level and more specific at the system level, should be approved by managers.
- **Implement security awareness and personnel policies** that provide training for new employees, contractors, and users; periodic refresher training; and distribution of security policies detailing rules and expected behaviors. This element also addresses hiring, transfers, terminations, and performance for employees, contractors, and users. Examples of controls in this area are security awareness training, rules of behavior, position categorization, personnel policies, personnel screening, termination, transfer, access agreements, third-party personnel security, and personnel sanctions.
- **Monitor the program** to ensure that policies and controls effectively reduce risk on an ongoing basis. Effective monitoring involves testing controls to evaluate and determine whether they are appropriately designed and operating effectively. Examples of these controls are security assessments, continuous monitoring, privacy impact assessments, and vulnerability scanning.
- **Remediate information security weaknesses** when they are identified, which involves reassessment of related risks, applying appropriate corrective actions, and follow-up monitoring to ensure actions are effective. Agencies develop plans of actions and milestones to track weaknesses and corresponding corrective actions.
- **Ensure third parties are secure,** as vendors, business partners, and contractors are often granted access to systems for purposes such as outsourced software development or system transactions.[45]

FISCAM lists six access control critical elements:

- **Boundary protection controls** protect a logical or physical boundary around a set of information resources and implement measures to prevent unauthorized information exchange across the boundary. Firewall devices are the most common boundary protection technology.
- **Sensitive system resources controls** are designed to ensure the confidentiality, integrity, and availability of system data such as passwords and keys during transmission and

[45] GAO, *FISCAM.*

storage. Technologies used to control sensitive data include encryption and certificate management.

- **Physical security** restricts access to computer resources and protects them from loss or impairment. Physical security controls include guards, gates, locks, and environmental controls such as smoke detectors, fire alarms and extinguishers, and uninterruptible power supplies.
- **Audit and monitoring controls** involve the collection, review, and analysis of events for indications of inappropriate or unusual activity. These controls should be routinely used to assess the effectiveness of other security controls, to recognize an attack, and to investigate during or after an attack.
- **Identification and authentication controls** distinguish one user from another and establish the validity of a user's claimed identity.
- **Authorization controls** determine what users can do, such as granting access to various resources, and depend on valid identification and authentication controls. These controls establish the validity of a user's claimed identity.

Federal Information Security Modernization Act (FISMA) of 2014

The following are the stated goals of FISMA:

- Provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support federal operations and assets.
- Recognize the highly networked nature of the current federal computing environment and provide effective government-wide management and oversight of the related information security risks.
- Provide for development and maintenance of minimum controls required to protect federal information and information systems.
- Provide a mechanism for improved oversight of federal agency information security programs.
- Acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions.
- Recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.[46]

[46] FISMA § 3551.

FISMA also requires an annual independent assessment of each agency's information security program to determine its effectiveness. Inspectors general or independent external auditors must conduct annual evaluations. The VA Office of Inspector General (OIG) accomplishes the annual FISMA evaluation through a contracted external auditor and provides oversight of the contractor's performance.

NIST Information Security Guidelines

The Joint Task Force Interagency Working Group created the NIST information security guidelines.

Appendix C: Scope and Methodology

Scope

The inspection team conducted its work from January 2024 through August 2024. The team evaluated configuration management, contingency planning, security management, and access controls of operational VA information security assets and resources in accordance with FISMA, NIST security guidelines, and VA's information security policy. In addition, the team assessed the capabilities and effectiveness of information security controls used to protect VA systems and data from unauthorized access, use, modification, or destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies and inspected the HEC and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the facility's IT security, operations, and privacy compliance. The team conducted vulnerability and configuration testing to determine local systems' security compliance. Finally, the team analyzed the results of testing, interviews, and the inspection to identify policy violations and threats to security.

Internal Controls

The inspection team determined that internal controls were significant to the inspection's objectives. The overall scope of information security inspections is the evaluation of general security and application controls that support VA's programs and operations. According to the risk management framework for VA information systems, the information security program is the foundation for VA's information security and privacy program and practices. The framework is documented in VA Handbook 6500.

The team used GAO's *Federal Information System Controls Audit Manual (FISCAM)* as a template to plan the inspection. When planning for this inspection, the team identified potential information system controls that would significantly affect the review. Specifically, the team used *FISCAM* appendix II as a guide to help develop evidence requests and interview questions for HEC personnel. The team used the *FISCAM* controls identified in appendix B of this report to determine the FISMA controls used by VA to protect and secure its information systems. Although similar to the contractor-conducted annual FISMA audits, this review focused on security controls that are implemented at the local level. However, there are some controls that overlap and are included in both assessments due to redundant roles and responsibilities among VA's local, regional, and national facilities and offices.

The inspection team determined that all controls applicable to the HEC are aligned with the control activities category. Control activities are the actions that managers establish through policies and procedures to achieve objectives and respond to risks in the internal control system, which includes the entity's information systems. When the team identified control activity deficiencies, team members assessed whether other relevant controls contributed to those deficiencies. The team did not address risk assessment controls because VA's risk management framework is based on NIST security and privacy controls.

Data Reliability

The inspection team generated computer-processed data by using network scanning tools. The results of the scans were provided to the Office of Information and Technology Quality Performance and Risk team. The team used an industry-standard information system security tool to identify information systems on the VA network and to take snapshots of their configurations, which were used to identify vulnerabilities. In this process, the team was not testing VA data or systems for transactional accuracy. The security tools identified a version of software present on a system and then compared it to the expected version. If the system did not have the current software version, the tool identified that as a vulnerability. The team relied on the results of the scanning tool and network device configuration. The team performed its own scans to determine whether the agency scans were complete and accurate, met intended purposes, and were not subject to alteration. The team did not find any material differences between OIG and agency scan data and determined the data used as complete and accurate.

Government Standards

The OIG conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation*.

Appendix D: VA Management Comments

Department of Veterans Affairs Memorandum

Date: September 24, 2024

From: Assistant Secretary for Information and Technology and Chief Information Officer (005)

Subj: Inspection of Information Security at the Health Eligibility Center in Atlanta, Georgia (Draft Report) (VIEWS 12150098)

To: Assistant Inspector General for Audits and Evaluations (52)

1. Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, *Inspection of Information Security at the Health Eligibility Center in Atlanta, Georgia* (Project Number 2024-01232-AE-0050).

2. The Office of Information and Technology (OIT) submits the attached written comments, including a target completion date or closure evidence for each of the OIG's recommendations to the Department.

The OIG removed point of contact information prior to publication.

(Original signed by)

Kurt D. DelBene

Attachment

Attachment

Office of Information and Technology
Comments on Office of Inspector General Draft Report,
Inspection of Information Security at the Health Eligibility Center in Atlanta, Georgia,

Project Number 2024-01232-AE-0050
(VIEWS 12150098)

Recommendation 1: Improve vulnerability management processes to ensure all vulnerabilities are identified and that plans of action and milestones are created for vulnerabilities that cannot be mitigated by VA deadlines.

Comments: The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs. OIT has processes that identify and maintain aged vulnerabilities in the critical, high, and medium categories. OIT will document and manage vulnerabilities that fall out of compliance with the VA established time frames with a Plan of Actions and Milestone (POAM).

Expected Completion Date: December 27, 2024.

Recommendation 2: Implement a more effective system life-cycle process to ensure network devices are running authorized software and operating systems that are configured to approved baselines and free of vulnerabilities.

Comments: Concur. OIT has implemented a process to identify, track, and remediate unauthorized software, and ensure approval of baselines. All identified vulnerabilities are scheduled to be remediated by the end of October 2024.

Expected Completion Date: October 30, 2024.

Recommendation 3: Ensure all file systems holding veteran information are encrypted in accordance with NIST and VA policy requirements.

Comments: Concur. OIT is in the process of implementing a new system that will ensure all file systems are encrypted in accordance with VA policy requirements. Overall, VA is 98% compliant with industry encryption standards.

Expected Completion Date: November 1, 2024.

Recommendation 4: Maintain an accurate inventory of personnel with key access to the facility.

Comments: Concur. Key inventory was completed on July 31, 2024, and will be conducted on a semi-annual bases, per End User Services Standard Operating Procedure – Physical and Environmental Protection. Evidence was entered in the Enterprise Mission Assurance Support Service.

Expected Completion Date: Completed. Completion date: July 31, 2024.

VA requests closure of Recommendation 4.

Recommendation 5: Enable improved audit logging capability to monitor administrator access to sensitive information hosted on the Workload Reporting and Productivity Assessing file server.

Comments: Concur. OIT is in the process of replacing its Workload Reporting and Productivity Assessing file server. The new system will record administrator access to sensitive information and log files for monitoring purposes as recommended by the Office of Inspector General.

Expected Completion Date: November 1, 2024.

For accessibility, the original format of this appendix has been modified to comply with Section 508 of the Rehabilitation Act of 1973, as amended.

OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Inspection Team	Michael Bowman, Director Sachin Bagai Timothy Moorehead Nicholas Neagle Albert Schmidt Justin Skeen Brandon Zahn
Other Contributors	Charles Hoskinson Rashiya Washington

Report Distribution

VA Distribution

Office of the Secretary
Veterans Benefits Administration
Veterans Health Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals
Director, VISN 7: VA Southeast Network
Executive Director of the Atlanta VA Health Care System
Director, Health Eligibility Center

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Accountability
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget

OIG reports are available at www.vaoig.gov.