US DEPARTMENT OF VETERANS AFFAIRS
OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the VA Dublin Healthcare System in Georgia

Information Security Inspection	23-01138-203	September 28, 2023

BE A

VOICE FOR VETERANS

REPORT WRONGDOING

va.gov/oig/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.
va.gov/oig

Executive Summary

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 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 applicable National Institute of Standards and Technology (NIST) information security guidelines.[2]

The fiscal year 2022 FISMA audit indicated that VA continues to face significant challenges meeting the law's requirements. The audit made 26 recommendations to VA, including repeat recommendations to address deficiencies in configuration management, security management, and access controls.[3] Appendix A details these recommendations.

In 2020, the OIG also started an information security inspection program. These inspections assess whether VA facilities are meeting federal and VA security requirements related to three control areas the OIG determined to be at highest risk.[4] Typically, facilities selected for these inspections either were not included in the annual audit sample or had previously performed poorly. The OIG conducted this inspection to determine whether the VA Dublin Healthcare System in Georgia was meeting federal and VA security guidance. The OIG selected this healthcare system because it had not been previously visited as part of the annual FISMA audit. The inspection scope and methodology are described in appendix C.

The OIG's inspections are focused on three security control areas:

1. **Configuration management controls** identify and manage security features for all hardware and software components of an information system.[5]
2. **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]

[1] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-001576-72, May 17, 2023. Appendix A lists the recommendations from the fiscal year (FY) 2022 FISMA audit, the most recent audit.

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

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

[4] The OIG recently removed a fourth control area—contingency planning—from its information security inspections because this area is largely enterprise controlled and is not a significant risk at the local level. Appendix B presents background information on federal information security requirements.

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

[6] GAO, *FISCAM*.

3. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals. Access also 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 VA Dublin Healthcare System in Georgia, other healthcare systems across VA could benefit from reviewing this information and considering these recommendations.

What the Inspection Found

The OIG identified security deficiencies with configuration management, security management, and access controls.[8]

Configuration Management Controls Had One Deficiency

Configuration management controls identify and manage security features for all hardware and software components of an information system.[9] Effective configuration management prevents unauthorized changes to information system resources and provides reasonable assurance that systems are configured and operating securely and as intended. The one deficiency identified in this control area at the VA Dublin Healthcare System involved flaw remediation of security vulnerabilities.

Prior FISMA audits have repeatedly found deficiencies in VA's vulnerability management, which is the process by which the Office of Information and Technology (OIT) identifies, classifies, and addresses weaknesses. OIT scans for vulnerabilities both routinely and randomly or when new vulnerabilities are identified and uses the Information Central Analytics and Metrics Platform to report vulnerabilities to facilities for remediation. Vulnerabilities are classified according to risk level (low, medium, high, or critical) to help VA assess and prioritize vulnerability management.

The inspection team reviewed 13 months of VA vulnerability scans (January 2022–January 2023) provided by OIT. Based on these scan results, there were

- 216 high vulnerabilities on about 18 percent of computers that had been mitigated after the 60-day timeline established by OIT,
- 217 critical vulnerabilities on about 17 percent of computers that had been mitigated after the OIT-established 30-day timeline,

[7] GAO, *FISCAM*.

[8] For more information on this inspection's scope and methodology, see appendix C.

[9] GAO, *FISCAM*.

- 135 high vulnerabilities on about 1 percent of computers that had not been mitigated and were past OIT’s 60-day timeline, and
- 76 critical vulnerabilities on about 4 percent of computers that had not been mitigated and were past OIT’s 30-day timeline.

Without an effective patch management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

Security Management Controls Had Three Deficiencies

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.”[10] The OIG identified three security management control weaknesses at the VA Dublin Healthcare System: authorization to operate, security categorization, and the remediation of unapproved software.

OIT issues an authorization to operate an information system and explicitly accepts the risk to agency operations, assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.[11] The OIG determined that the VA Dublin Healthcare System’s special-purpose system did not have an authorization to operate because it had not cleared the NIST risk management framework.[12] The special-purpose system included systems that support and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services, and functional support areas throughout the hospital; alert facility police of emergencies via panic buttons; control room access; and control the facility’s climate.

Without an authorization to operate, facility managers do not have assurance that the implemented security and privacy controls reduce the risk of a system compromise to an acceptable level. A compromise of the special-purpose system’s security could threaten the safety of patients, staff members, and visitors.

[10] GAO, *FISCAM*.

[11] NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 23, 2021.

[12] VA’s Enterprise Mission Assurance Support Service system states a special-purpose system “is comprised of operational technology devices/systems that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services functional support areas.” Per NIST Special Publication 800-53, the risk management framework provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. Managing organizational risk is paramount to effective information security and privacy programs.

The VA Dublin Healthcare System owned one of the 137 special-purpose systems for which OIT did not consider all information types when establishing the security category level. The OIG previously identified this issue during the information security inspection of the Beckley Healthcare System in West Virginia.[13] NIST's risk management framework requires the baseline controls for information systems be set based on the system's security categorization. The security categorization is determined by the risk of loss of confidentiality, integrity, and availability of the information within each system. The system's security categorization—low, medium, or high—is used to select the system's security controls.

OIT used a single standard for all special-purpose systems, and the security categorization only included the "general information" type. As a result, managers assigned those special-purpose systems a security risk categorization of low for confidentiality, moderate for integrity, and moderate for availability. However, the inspection team determined that the facility special-purpose systems included two systems that warranted higher security levels:

- A network panic button system, which falls under the "emergency-response information" type, should have a security categorization of low for confidentiality, high for integrity, and high for availability, as recommended by NIST.[14]
- A system used to transfer laboratory results from an external vendor should have a security categorization of high for confidentiality, high for integrity, and high for availability, per the healthcare system's special-purpose system documentation.

Although NIST allows the security categorization to be adjusted, OIT would need to document the rationale or justification for adjustments, which was not done. Furthermore, the VA Dublin Healthcare System's special-purpose system security plan only considered security controls based on the lower security categorization developed by OIT. By not considering all information types during the security categorization, healthcare system leaders do not have assurance that appropriate security and privacy controls for special-purpose systems reduce the risk of compromise to an acceptable level.

Continuous monitoring facilitates ongoing awareness of system security and privacy issues and supports risk management. Frequent updates to software and hardware inventories are a key component of VA's continuous monitoring program. OIT uses end-point management software to report unapproved software on computers. These reports identified 40 different versions of unapproved software that were installed 5,006 times on the healthcare system's computers; however, actions were not taken to remediate the unapproved software. This software was

[13] VA OIG, *Information Security Inspection at the VA Beckley Healthcare System in West Virginia*, Report No. 23-00089-144, September 21, 2023.

[14] NIST 800-60, *Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

installed without proper authorization or without a plan of action and milestones. VA allows unauthorized software if there is a signed plan of action and milestones to document the acceptance of risk.[15] Without an accurate inventory of software, VA has no assurance that corresponding system security and privacy plans have identified the appropriate security controls for all components.

Access Controls Had Deficiencies in Four Elements

Access controls provide reasonable assurance that computer resources are restricted to authorized individuals. The inspection team found that the VA Dublin Healthcare System's Carl Vinson VA Medical Center had deficiencies in physical building access security, monitoring of physical controls, emergency power, and environmental controls.[16]

Physical Building Access Security

The inspection team discovered that physical access to the facility and its information technology (IT) resources was not effectively controlled. Physical access controls include devices and barriers to prevent movement from publicly accessible areas to nonpublic areas.[17] The facility had an automated physical access control system that allowed only individuals with badges to enter the server room. However, employees used keys to access communication closets. Badge access to the server room was not adequately restricted. The system allowed access to the server room for 11 individuals, including two former employees, but the OIG team was unable to verify whether these 11 individuals accessed the server room. Further, the medical center could not account for all the keys:

- Nine master keys and four communication closet keys were missing.
- Two master key and 24 communication closet keys were issued to VA employees who no longer needed access.

The medical center's police manager indicated they began managing these keys in early calendar year 2023. Before 2023, key management was a shared responsibility, with no group taking the lead. To strengthen controls, the facility is seeking to replace the keys with an electronic key system.

Monitoring of Physical Building Access

The medical center also did not have controls to monitor access to the facility server room and communication closets. During the facility walk-through, the inspection team discovered that the medical center did not have a comprehensive video surveillance system, which is required for

[15] VA Technical Reference Model version 23.2.

[16] Environmental controls include electrical grounding, fire protection, and temperature and humidity controls.

[17] NIST Special Publication 800-53.

data centers.[18] According to the healthcare system's physical security specialist, the medical center is in the process of upgrading its surveillance system, which would significantly expand its surveillance capability. Although the electronic badge access system allows monitoring of the server room, it does not monitor individuals who access the computer room with a master key, nor can it be used to monitor access to the communication closets. Ineffective monitoring of physical access to information systems inhibits the facility's incident response capabilities in the event of a security breach and can undermine managers' awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

Emergency Power

During the site visit, the inspection team found

- 20 percent of communication closets were missing uninterruptible power supply devices, and a quarter of these also did not have emergency power outlets;
- approximately 5 percent of the communication closets had uninterruptible power supply devices that were actively alerting with an audio alarm;[19] and
- 9 percent of the communication closets had uninterruptible power supply devices that were not plugged into emergency power outlets.[20]

An uninterruptible power supply is an electrical system or mechanism that provides emergency power when the main power source fails.[21] They are typically used to protect devices, data centers, and telecommunications equipment where an unexpected disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. Without operational uninterruptible power supplies, equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

During utility power outages, facilities rely on generators to keep the facility operating. The inspection team found three generators at the facility that did not have adequate physical controls:

[18] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection"; NIST Special Publication 800-53.

[19] The audio alarm indicated an issue with the uninterruptible power supply devices.

[20] In the event of a prolonged power outage, the uninterruptible power supply devices would not be able to support the equipment.

[21] NIST Special Publication 800-53.

- All three generators and connected fuel tanks were not monitored by cameras and did not have required physical barriers.[22]
- One generator was in an unlocked container.

Facility managers were unaware of the security requirements for generators and fuel tanks. By not adequately restricting access to these areas, the Carl Vinson VA Medical Center is placing assets at risk of accidental or intentional shutdown or destruction.

Environmental Controls

The team found deficiencies with environmental controls over electrical grounding and temperature and humidity within the facility's communication closets.

The team found the equipment was not grounded in about 13 percent of the communication closets, and facility staff were unaware of this issue. VA requires equipment in communication closets to be properly grounded. Without proper grounding, the equipment's functionality could be hindered because of increased electromagnetic interference and power surges.

The inspection team discovered about 45 percent of communication closets did not have temperature or humidity controls. Environmental controls maintain and monitor temperature and humidity where communications equipment is located.[23] Insufficient environmental controls can have a significant adverse impact on the availability of systems that are needed to support VA's mission and business functions.

What the OIG Recommended

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

1. Improve vulnerability management processes to ensure system changes occur within organization timelines.
2. Develop and approve an authorization to operate for the special-purpose systems.
3. Include system personnel during the security categorization process to ensure that all necessary information types are considered when determining the security categorization for special-purpose systems.
4. Review the list of unauthorized software and remediate or remove unneeded software at the facility.

[22] Required physical barriers include both anti-vehicle barriers around fuel tanks and generators and fences that can prevent pedestrian access to fuel tanks.

[23] NIST Special Publication 800-53.

The OIG also made three recommendations to the Carl Vinson VA Medical Center director:

5. Implement the appropriate physical security controls to restrict and monitor access to the facility, its server room, communication closets, and generators.
6. Implement and monitor emergency power and uninterruptible power supplies that support information technology resources.
7. Validate that appropriate physical and environmental security measures are implemented and functioning as intended.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1–7 and requested that recommendations 1 and 4 be closed due to corrective actions he said were completed. For recommendations 1–7, the planned corrective actions are responsive to the intent of the recommendations. The full text of the assistant secretary's response is included in appendix D.

Regarding recommendation 1, the assistant secretary provided evidence to close the recommendation that does not fully address the OIG's findings regarding vulnerability remediation. The process developed to link vulnerability to plans of actions and milestones constitutes a first step toward correcting the deficiency; however, evidence does not yet demonstrate that this new process will work as intended. The OIG will continue to monitor the remediation of vulnerabilities and the creation of plans of action and milestones for vulnerabilities that cannot be remediated during the information security inspections. Recommendation 1 will be closed when VA can demonstrate that the plan of action and milestones process effectively mitigates security risks for unremedied security vulnerabilities. The assistant secretary provided evidence to support actions addressing recommendation 4 were completed, and the OIG considers this recommendation closed.

The OIG will monitor implementation of the planned actions and will close the open recommendations when VA provides evidence demonstrating progress in addressing the issues identified.

Larry M. Reinkemeyer

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

Contents

Abbreviations

FISCAM	Federal Information System Controls Audit Manual
FISMA	Federal Information Security Modernization Act of 2014
FY	fiscal year
GAO	Government Accountability Office
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

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.[24] The FISMA audit is conducted in accordance with guidelines issued by the Office of Management and Budget (OMB) and applicable National Institute of Standards and Technology (NIST) information security guidelines.[25] Appendix A provides more details about the most recent FISMA audit.

In 2020, the OIG started an information security inspection program. These inspections assess whether VA facilities are meeting federal and VA security requirements that protect systems and data from unauthorized access, use, modification, or destruction.[26] They are typically conducted at selected facilities that have not been assessed in the sample for the annual FISMA audit or at facilities that previously performed poorly. Inspections provide recommendations to VA on enhancing information security oversight at local and regional facilities.[27] Appendix C provides more detail on the inspection scope and methodology.

The OIG conducted this inspection to determine whether the VA Dublin Healthcare System in Georgia was meeting federal and VA security guidance. The OIG selected this healthcare system because it had not been previously visited as part of the annual FISMA audit. Although the findings and recommendations in this report are specific to the VA Dublin Healthcare System, other VA healthcare systems could benefit from reviewing this information and considering these recommendations.

Security Controls

Both the OMB and NIST provide criteria to evaluate security controls. These criteria provide requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system.

[24] Federal Information Security Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, § 128 (2014).

[25] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*, Report No. 22-01576-72, May 17, 2023. Appendix A lists the recommendations from the fiscal year (FY) 2022 FISMA audit, the most recent audit.

[26] Appendix B discusses federal information security requirements in further detail.

[27] The OIG provided VA with a memorandum related to this inspection containing "VA Sensitive Data" as defined in 38 U.S.C. § 5727. Federal law, including FISMA and its implementing regulations, requires federal agencies to protect sensitive data and information systems due to the risk of harm that could result from improper disclosure. Accordingly, the memorandum is not being published by the OIG or distributed outside of VA to prevent intentional or inadvertent disclosure of specific vulnerabilities or other information that could be exploited to interfere with VA's network operations and adversely affect the agency's ability to accomplish its mission.

According to VA Handbook 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, including the operational requirements. VA established guidance outlining both NIST-specific and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

OIG information security inspections are focused on three security control areas that apply to local facilities and have been selected based on their level of risk, as shown in table 1.[28]

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
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 are at risk of unauthorized access or modifications. A cyberattack could disrupt access to, destroy, or allow malicious control of personal information belonging to patients, dependents, beneficiaries, VA employees, contractors, or volunteers.

Office of Information and Technology Structure and Responsibilities

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

[28] The OIG recently removed a fourth control area—contingency planning—from its information security inspections because this area is largely enterprise controlled and not a significant risk at the local level.

information and information systems by identifying and reporting emerging and imminent threats and vulnerabilities. OIT's Office of Development, Security, and Operations unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration throughout the entire solution delivery process. Figure 1 provides an overview of the relevant entities' organizational structure.

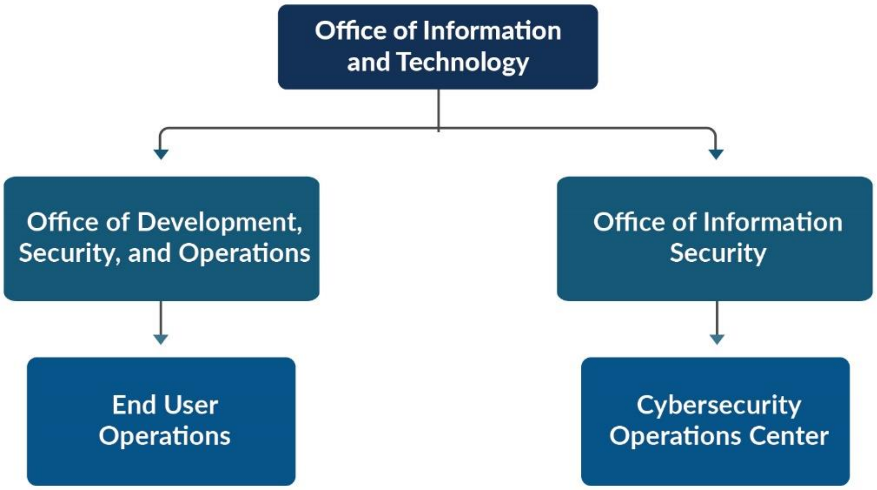
Office of Information and Technology
Office of Development, Security, and Operations
Office of Information Security
End User Operations
Cybersecurity Operations Center

Figure 1. *Organizational structure of OIT entities relevant to this inspection.*
Source: VA OIG analysis.

End User Operations provides on-site and remote support to information technology (IT) customers across all VA administrations and special program offices, including direct support of approximately 400,000 VA employees and approximately 100,000 contractors who are issued government-furnished IT equipment and access. End User Operations provides computing devices; conducts new facility activations; performs moves, adds, and changes; executes local system implementations; and engages VA's customers across the nation to meet IT support needs. OIT assigns dedicated End User Operations and Office of Information Security personnel to the VA Dublin Healthcare System, 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

As previously mentioned, the OIG issues annual reports on VA's information security program. The FISMA audit is conducted in accordance with guidelines issued by the OMB and applicable

NIST information security guidelines.[29] The fiscal year (FY) 2022 FISMA audit, conducted by independent public accounting firm CliftonLarsonAllen LLP, evaluated 47 major applications and general support systems hosted at 23 VA facilities, including the testing of selected management, technical, and operational controls outlined by NIST.[30] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A. All 26 recommendations are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[31] Repeat recommendations included addressing deficiencies in configuration management, security management, and access controls.

A statement prepared by the Government Accountability Office (GAO) for a House Veterans' Affairs subcommittee hearing in November 2019 said VA was one of the federal agencies that continued to have a deficient information security program.[32] According to the GAO, 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.

The GAO concluded that "until VA adequately mitigates security control deficiencies, the sensitive data maintained on its systems will remain at increased risk of unauthorized modification and disclosure, and the systems will remain at risk of disruption."[33]

VA Dublin Healthcare System

The VA Dublin Healthcare System consists of the Carl Vinson VA Medical Center, shown in figure 2, and the Albany, Brunswick, Kathleen, Macon, Milledgeville, Perry, and Tifton VA

[29] OMB Memo M-21-02, "Fiscal Year 2020–2021 Guidance on Federal Information Security and Privacy Management Requirements," November 9, 2020; NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 23, 2021; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*. Appendix A details the FISMA audit's recommendations.

[30] OMB, "Security of Federal Automated Information Resources," app. 3 in OMB Circular A-130, *Managing Information as a Strategic Resource*, November 28, 2000. The circular's appendix defines a general support system as an interconnected set of information resources under the same direct management control that share common functionality.

[31] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2022*. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

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

[33] GAO, *Information Security: VA and Other Federal Agencies Need to Address Significant Challenges*.

clinics. The Carl Vinson VA Medical Center managed 37,834 unique outpatients in FY 2022. It also houses 340 operating beds, including 161 nursing care beds and a 145-bed domiciliary for veterans who are experiencing homelessness or at risk of homelessness. The facility has 1,942 full-time employees and a budget of $509 million for FY 2023.

Figure 2. *Carl Vinson VA Medical Center in Dublin, Georgia.*

Source: Carl Vinson VA Medical Center; Public Affairs Office, November 30, 2018.

Results and Recommendations

I. Configuration Management Controls

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.[34] Effective configuration management prevents unauthorized changes to information system resources and provides reasonable assurance that systems are configured and operating securely and as intended. The inspection team reviewed and evaluated 12 configuration management controls drawn from NIST criteria for VA-hosted systems at the VA Dublin Healthcare System to determine if the controls met federal guidance and VA requirements.

An effective configuration management process should be described in a configuration management plan and implemented according to the plan.[35] VA should first establish an accurate component inventory to identify all devices on the network.[36] The component inventory affects the success of other controls, such as vulnerability and patch management. 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 VA Dublin Healthcare System Had One Configuration Management Control Deficiency

To assess configuration management controls, the inspection team interviewed the area manager, information system security officer, and local IT specialists. The team reviewed local policies, procedures, and inventory lists and scanned the VA Dublin Healthcare System's network to identify devices. The team compared the devices found on the network with the device inventories provided by VA, received vulnerability lists provided by OIT, and scanned the network to identify vulnerabilities.[37] The team also conducted a walk-through of the facility.

Analysis of the OIT vulnerability scan results indicated they did not provide medical center leaders with complete and accurate information related to the vulnerabilities discovered. The

[34] GAO, *FISCAM*

[35] GAO, *FISCAM*.

[36] GAO, *FISCAM*

[37] OIT imports its vulnerability scan results into the Information Central Analytics and Metrics Platform for reporting vulnerabilities to system owners. See appendix C for additional information about the inspection's scope and methodology.

OIG team found that these security vulnerabilities were not being remediated within VA's established time frames.

Vulnerability Management and Flaw Remediation

VA has a vulnerability management program, but it can be improved. Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management controls. Consistent with those findings, the team identified deficient controls at the VA Dublin Healthcare System.[38] Vulnerability management is the process by which OIT identifies, classifies, and reduces weaknesses and is part of assessing and validating risks as well as monitoring the effectiveness of a security program. OIT identifies and reports on threats and vulnerabilities and conducts scans for vulnerabilities both routinely and randomly, or when new vulnerabilities are identified and reported.[39]

VA conducts periodic independent scans of all its systems. Discovered vulnerabilities are entered into a plan of action and milestones for remediation by the system steward. System technicians then use the Remediation Effort Entry Form to document mitigation or remediation efforts for each deficiency identified from the scan and provide evidence that the deficiencies have been mitigated.

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[40] The scoring system captures the principal characteristics of a vulnerability and produces a numerical score reflecting its severity. Numerical scores are classified as risk levels (low, medium, high, or critical) to help organizations properly assess and prioritize vulnerability management processes. For example, on a scale of zero to 10, critical-risk vulnerabilities have a score between 9.0 and 10, while high-risk vulnerabilities have a score between 7.0 and 8.9. VA requires critical-risk vulnerabilities be remediated within 30 days and high-risk vulnerabilities be remediated within 60 days.[41]

[38] 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."

[39] VA Directive 6500, *VA Cybersecurity Program*, February 24, 2021.

[40] "Vulnerability Metrics" (web page), NIST National Vulnerability Database, accessed July 5, 2022, https://nvd.nist.gov/vuln-metrics/cvss; "Common Vulnerability Scoring System ver. 3.14, Specification Document, Revision 1" (web page), Forum of Incident Response and Security Teams (FIRST), accessed July 5, 2022, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[41] Information System Vulnerability Management Plan Version 1.0, March 28, 2022.

The inspection team reviewed OIT-provided network vulnerability scan results at the Carl Vinson VA Medical Center from January 2022 through January 2023. Based on these scan results, there were

- 216 high vulnerabilities on about 18 percent of computers that had been mitigated after the timelines established by OIT,
- 217 critical vulnerabilities on about 17 percent of computers that had been mitigated after the OIT-established timelines,
- 135 high vulnerabilities on about 1 percent of computers that had not been mitigated, and
- 76 critical vulnerabilities on about 4 percent of computers that had not been mitigated.

Without an effective patch management program, vulnerabilities such as security and functionality problems in software and firmware might not be mitigated, increasing opportunities for exploitation.

Finding 1 Conclusion

System vulnerabilities were not always mitigated within OIT-established timelines. Security weaknesses on the medical center's network could be exploited by malicious individuals to gain unauthorized access to sensitive information or disrupt operations.

Recommendation 1

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 system changes occur within organization timelines.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 1. The assistant secretary also requested closure of the recommendation, reporting that an enterprise-wide process to link vulnerabilities to plan of action and milestones items has already been established. The documentation he submitted indicates that the vulnerabilities identified by the OIG have either been remediated or a plan has been established for their remediation. The full text of the assistant secretary's response is included in appendix D.

OIG Response

The assistant secretary for information and technology and chief information officer submitted a responsive action plan for recommendation 1. However, the evidence provided by the assistant secretary to close the recommendation does not fully address the OIG's findings regarding vulnerability remediation. While the linking process described above constitutes a first step toward correcting the deficiency, the evidence does not yet demonstrate that this new process will work as intended. The OIG will continue to monitor the remediation of vulnerabilities and the creation of plans of action and milestones for vulnerabilities that cannot be remediated during the information security inspections. Recommendation 1 will be closed when VA can demonstrate that the plan of action and milestones process effectively mitigates security risks for unremedied security vulnerabilities.

II. Security Management Controls

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 three critical elements of security management: authorization to operate, security categorization, and continuous monitoring.[42]

Finding 2: The VA Dublin Healthcare System Had Deficiencies in Three Security Management Controls

To assess security management controls, the inspection team reviewed local security management policies, standard operating procedures, and applicable VA policies, including documentation from the Enterprise Mission Assurance Support Service—VA's cybersecurity management service for workflow automation and continuous monitoring. Among the topics reviewed were the system security plan, security authorization and risk assessment, security control policies and procedures, and plans of action and milestones for known deficiencies. The team also interviewed the area manager and information system security officer. Finally, the team conducted a walk-through of the facility.

Regarding system security authorizations, the inspection team found that the VA Dublin Healthcare System's special-purpose system did not have an authorization to operate as required by policy.[43] Furthermore, this special-purpose system was assigned a moderate risk security categorization without consideration of higher risk information types included in the system. Finally, the team identified a deficiency in continuous monitoring of software and hardware inventories at the VA Dublin Healthcare System.[44]

Authorization to Operate

OIT issues an authorization to operate an information system and explicitly accepts the risk to agency operations, assets, individuals, other organizations, and the nation based on the implementation of an agreed-upon set of security and privacy controls.[45] The inspection team determined that the VA Dublin Healthcare System's special-purpose IT system did not have an

[42] The security categorization indicates the minimum baseline controls needed to secure the system. FISCAM critical elements for security management are listed in appendix B.

[43] OMB, Circular A-130; VA Directive 6500.

[44] Unapproved software is software that has not been approved to be on VA's network.

[45] NIST Special Publication 800-53.

authorization to operate because it had not cleared the NIST risk management framework.[46] The special-purpose system included systems that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services, and functional support areas throughout the hospital; alert facility police of emergencies via panic buttons; control room access; and control the facility's climate.

Without an authorization to operate, facility managers do not have assurance that the implemented security and privacy controls reduce the risk of a system compromise to an acceptable level. A compromise of the special-purpose system's security could threaten the safety of patients, staff members, and visitors.

Security Categorization

During the information security inspection of the VA Beckley Healthcare System in West Virginia, the OIG identified 137 special-purpose systems where OIT did not consider all information types when establishing the security category level for the special-purpose systems; the VA Dublin Healthcare System owned one of these special-purpose systems.[47] NIST's risk management framework requires the baseline controls for information systems to be set based on the needs for confidentiality, integrity, and availability of the information within each system.[48] Minimum security category settings—low, medium, or high—are used when determining baseline controls.

OIT used a single standard for all special-purpose systems, and the security categorization only included the "general information" type. As a result, managers assigned those special-purpose systems a security risk categorization of low for confidentiality, moderate for integrity, and moderate for availability. However, the inspection team determined that the healthcare system's special-purpose systems included two systems that warranted higher security levels:

- The network panic button system falls under the "emergency-response information" type and should have a security categorization of low for confidentiality, high for integrity, and high for availability, as recommended by NIST.[49]

[46] VA's Enterprise Mission Assurance Support Service system states a special-purpose system "is comprised of operational technology devices/systems that assist, support, and maintain mission capabilities and operations for building safety, healthcare services, security services and other general services functional support areas." Per NIST Special Publication 800-53, the risk management framework integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. Managing organizational risk is paramount to effective information security and privacy programs.

[47] VA OIG, *Information Security Inspection at the VA Beckley Healthcare System in West Virginia*, Report No. 23-00089-144, September 21, 2023.

[48] NIST Special Publication 800-53B, *Control Baselines for Information Systems and Organizations*, September 23, 2020.

[49] NIST Special Publication 800-60, vol. II.

- A system used to transfer laboratory results from an external vendor should have a security categorization of high for confidentiality, high for integrity, and high for availability, per the healthcare system's documentation.[50]

Although NIST allows the security categorization to be adjusted, OIT would need to document the rationale or justification for any adjustments, which was not done. Furthermore, the VA Dublin Healthcare System's special-purpose system security plan only considers security controls based on the lower security categorization developed by OIT.

By not considering all information types during the security categorization, healthcare system leaders do not have assurance that appropriate security and privacy controls have been selected for special-purpose systems at their facilities.

Software Inventories

Continuous monitoring facilitates ongoing awareness of system security and privacy issues and supports risk management. Frequent updates to software and hardware inventories are a key component of VA's continuous monitoring program. OIT uses end-point management software to report unapproved software on computers. These reports for the VA Dublin Healthcare System's network identified 40 different versions of unapproved software that were installed 5,006 times on the healthcare system's computers; however, actions were not taken to address the unapproved software. This software was installed without proper authorization or without a plan of action and milestones. VA allows unauthorized software if there is a signed plan of action and milestones to document the acceptance of risk.[51] Without an accurate inventory of software, VA has no assurance that corresponding system security and privacy plans have identified appropriate security controls for all components at the facility.

Finding 2 Conclusion

The VA Dublin Healthcare System's special-purpose IT system did not have an authorization to operate. Further, OIT did not consider all information types when performing risk assessments of similar systems at 137 VA facilities, and instead created a single security category for all special-purpose systems that did not have an authorization to operate. OIT did not take actions to address unauthorized software installed on computers within the VA Dublin Healthcare System. Without effective security management processes, users do not have adequate assurance that their IT systems and networks will perform as intended and to the extent needed to support VA missions.

[50] An Interconnection Security Agreement and Memorandum of Understanding between the Department of Veterans Affairs and the lab vendor.

[51] VA Technical Reference Model version 23.2.

Recommendations 2–4

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

2. Develop and approve an authorization to operate for the special-purpose systems.
3. Include system personnel during the security categorization process to ensure that all necessary information types are considered when determining the security categorization for special-purpose systems.
4. Review the list of unauthorized software and remediate or remove unneeded software at the facility.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 2–4 and requested that recommendation 4 be closed due to corrective actions he said were completed.

Regarding recommendation 2, the assistant secretary reported that VA will implement special-purpose systems on the VA network and that an authorizing official will assess the systems' security plans and boundaries to support an authorization-to-operate decision. The assistant secretary also stated that, to address recommendation 3, VA will consider all necessary information types when determining the security categorization for special-purpose systems. To support his request to close recommendation 4, the assistant secretary provided evidence that the Dublin VA medical center completed the review of unauthorized software and remediated unneeded software. The cleanup of the unapproved software, according to the assistant secretary, was complete on May 25, 2023.

OIG Response

OIT's corrective action plans are responsive to the intent of the recommendations. OIT representatives indicated they are in the process of consolidating all special-purpose systems into a VA-wide authorization to operate. The OIG considers the planned September and December 2025 completion dates to be reasonable for the actions planned in response to recommendations 2 and 3. Because the assistant secretary submitted evidence that demonstrates actions responsive to recommendation 4 have been completed, the OIG considers this recommendation closed. The OIG will monitor implementation of the planned actions and will close recommendations 2 and 3 when VA provides evidence demonstrating progress in addressing the issues identified.

III. 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.[52] 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 Carl Vinson VA Medical Center, the main facility within the VA Dublin Healthcare System, the inspection team reviewed two critical access control elements: physical access security and monitoring of physical and environmental controls.[53]

Finding 3: The VA Dublin Healthcare System Had Deficiencies in Four Access Control Elements

To evaluate logical access controls on the VA Dublin Healthcare System's network, the inspection team reviewed the configuration of network equipment. To evaluate the medical center's physical access controls, the inspection team interviewed the area manager, information system security officer, biomedical supervisor, and local IT specialists. The team also reviewed local policies and procedures, conducted walk-throughs of the facility, and analyzed audit logs.[54]

The VA Dublin Healthcare System's server room and communication closets at the facility did not have adequate physical and environmental controls:

- Physical access to the facility, server room, and communication closets was not adequately restricted.
- Access to the server room and communication closets was not adequately monitored.
- Emergency power and uninterruptible power supplies were not implemented or properly functioning in the communication closets. Physical security over generators also needs improvement.
- Environmental controls, including electrical grounding and temperature and humidity controls, were not implemented in all communication closets.

[52] Boundary protections include access control lists that restrict the flow of network traffic between network segments.

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

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

Physical Access Controls

The inspection team discovered that physical access to the facility and its IT resources was not effectively controlled. Physical access controls include devices and barriers to prevent movement from publicly accessible areas to nonpublic areas.[55] The facility had an automated physical access control system that required users to present a badge to enter the server room. However, employees used keys to access communication closets. Badge access to the server room was not adequately restricted. The system allowed access to the server room for 11 individuals, including two former employees. The OIG was unable to verify whether these 11 individuals accessed the server room. Further, the medical center could not locate all of the keys:

- Nine master keys and four communication closet keys were missing.
- Two master key and 24 communication closet keys were issued to VA employees who no longer needed access.

The center's police managers told the team they started managing the keys in early calendar year 2023. Before 2023, key management was a shared responsibility. To strengthen controls, the facility is seeking to replace the keys with an electronic key system.

Monitoring of Physical Security Controls

The Carl Vinson VA Medical Center did not have controls to monitor access to the server room and communication closets. During the facility walk-through, the inspection team discovered that the medical center did not have a comprehensive video surveillance system. Video surveillance is the use of cameras installed at strategic locations and is required for data centers.[56] According to Dublin's physical security specialist, the medical center is in the process of upgrading its surveillance system, which would significantly expand its surveillance capability. Although the electronic badging access system allows monitoring of the server room, it does not monitor access to either the computer room or the communication closets. Ineffective monitoring of access to information systems minimizes the facility's incident response capabilities in the event of a security compromise. The lack of an effective incident response can undermine managers' awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

Emergency Power Controls

At the facility, the team found

[55] NIST Special Publication 800-53.

[56] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection"; NIST Special Publication 800-53.

- 20 percent (13/64) of communication closets were missing uninterruptible power supply devices, and roughly a quarter (3) of these 13 closets also did not have emergency power outlets;
- approximately 5 percent of the communication closets had uninterruptible power supplies that were actively alerting with an audio alarm;[57] and
- 9 percent of the communication closets had uninterruptible power supplies that were not plugged into emergency power outlets.[58]

Uninterruptible power supplies are electrical systems or mechanisms that provide emergency power when the main power source fails.[59] They are typically used to protect devices, data centers, and telecommunications equipment where an unexpected disruption could cause injuries, fatalities, serious mission or business disruption, or loss of data or information. Uninterruptible power supplies differ from emergency power systems for backup generators because they provide near-instantaneous protection from interruptions. The emergency power outlets provide power from the electric company or, in the event of an emergency, the generator. Without operational uninterruptible power supplies, equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

During utility power outages, facilities rely on generators to maintain operations. The team also found three generators at the medical center that did not have adequate physical controls:

- All three generators and connected fuel tanks were not monitored by cameras and did not have required physical barriers.[60]
- One generator was in an unlocked container.

Facility managers had not previously identified these security weaknesses with the generators and fuel tanks. By not adequately restricting access to these areas, the Carl Vinson VA Medical Center is placing assets at risk of accidental or intentional shutdown or destruction.

Monitoring of Environmental Controls

The team found deficiencies with environmental controls over electrical grounding and temperature and humidity within the facility’s communication closets.

[57] The audio alarm indicates a problem with the uninterruptible power supply.

[58] In the event of a prolonged power outage, the uninterruptible power supplies would not be able to support the equipment.

[59] NIST Special Publication 800-53.

[60] Required physical barriers include both anti-vehicle barriers around fuel tanks and generators and fences that can prevent pedestrian access to fuel tanks.

Electrical Grounding Controls

The team found the equipment was not grounded in about 13 percent of the communication closets, and facility personnel were unaware of this issue. VA requires this equipment to be properly grounded.[61] Without proper grounding, the equipment could be damaged by electromagnetic interference and power surges.

Temperature and Humidity Controls

The inspection team discovered about 45 percent of communication closets did not have temperature or humidity controls. Environmental controls maintain and monitor temperature and humidity where communications equipment is located.[62] Temperature extremes can cause reduced efficiency and various problems, including premature aging and failure of equipment. High humidity can cause corrosion of internal components and degradation of electrical functionality. This is a risk because insufficient environmental controls can significantly hinder systems that are needed to support VA mission and business functions.

Finding 3 Conclusion

The VA Dublin Healthcare System's server room and communication closets at the facility did not have adequate physical and environmental controls. Additionally, physical access to the facility, server room, and communication closets was not adequately restricted or monitored. Emergency power and uninterruptible power supplies were not implemented or properly functioning in the communication closets. Physical security over generators also needs improvement. Finally, electrical grounding and temperature and humidity controls were not implemented in all communication closets.

Unless the healthcare system takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information.

Recommendations 5–7

The OIG made three recommendations to the Carl Vinson VA Medical Center director:

5. Implement the appropriate physical security controls to restrict and monitor access to the facility, its server room, communication closets, and generators.
6. Implement and monitor emergency power and uninterruptible power supplies that support information technology resources.

[61] NIST Special Publication 800-53; VA Telecommunications and Special Telecommunications System Design Manual, February 2016.

[62] NIST Special Publication 800-53.

7. Validate that appropriate physical and environmental security measures are implemented and functioning as intended.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 5–7. For recommendation 5, the assistant secretary provided documentation to support that the generator has appropriate barriers and has been locked and that badge access to the computer room has been restricted. Further, the medical center will replace the server room doors and locks as part of the electronic health record modernization project, and a project was approved to install cameras in key areas. Regarding recommendation 6, the assistant secretary indicated that VA remediated the issue with defective uninterrupted power supplies and plans to have emergency power outlets in communications closets replaced by October 30, 2023. For recommendation 7, the assistant secretary indicated OIT is updating VA's Physical and Environmental Protection Standard Operating Procedures to remediate this issue.

OIG Response

OIT's corrective action plans are responsive to the intent of the recommendations. The OIG will monitor implementation of the planned actions and will close recommendations 5–7 when VA provides evidence demonstrating progress in addressing the issues identified.

Appendix A: FISMA Audit for FY 2022 Report Recommendations

In the Federal Information Security Modernization Act of 2014 (FISMA) audit for FY 2022, CliftonLarsonAllen LLP made 26 recommendations, all repeated from the prior year. The FISMA audit assesses the agency-wide security management program, and recommendations in the FISMA report are not specific to the VA Dublin Healthcare System. The 26 recommendations are listed below:

1. Consistently implement an improved continuous monitoring program in accordance with the National Institute of Standards and Technology Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions.
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 access by system users with incompatible roles, permissions in excess of required functional responsibilities, and unauthorized accounts.
8. Enable system audit logs on all critical systems and platforms and conduct centralized reviews of security violations across the enterprise.
9. Implement improved processes for establishing and maintaining accurate 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 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.
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 network access controls that restrict medical devices from systems hosted on 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.[63]
17. Implement improved procedures to enforce standardized system development and change control processes that integrate information security throughout the life cycle of each system.
18. Review system boundaries, recovery priorities, system components, and system interdependencies and implement appropriate mechanisms to ensure that established system recovery objectives can be measured and met.
19. Ensure that contingency plans for all systems are updated to include critical inventory components and are tested in accordance with VA requirements.
20. 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.
21. Ensure that systems and applications are adequately logged and monitored to facilitate an agency-wide awareness of information security events.

[63] Credentialed vulnerability assessments are vulnerability scans performed using a user account and password.

22. Implement improved safeguards to identify and prevent unauthorized vulnerability scans on VA networks.
23. 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.
24. Implement improved processes to monitor for unauthorized changes to system components and the installation of prohibited software on all agency devices and platforms.
25. Develop a comprehensive inventory process to identify connected hardware, software, and firmware used to support VA programs and operations.
26. 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

The Government Accountability Office developed the *Federal Information System Controls Audit Manual* (FISCAM) to provide auditors and information system control specialists with a methodology for evaluating the confidentiality, integrity, and availability of information systems. FISCAM categorizes related controls 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** by naming and describing the 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.[64] 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

[64] Firmware comprises 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 management, 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.
- **Backup procedures and environmental controls** help prevent and minimize damage and interruption. 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 that lead 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 management.
- **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 doing follow-up monitoring to ensure actions are effective. Agencies develop plans of action 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.[65]

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.
- **Controls over sensitive system resources** are designed to ensure the confidentiality, integrity, and availability of system data, and include things such as passwords and keys during transmission and storage. Technologies used to control sensitive data include encryption and certificate management.

[65] GAO, *FISCAM.*

- **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 authorized users can do, it grants or restricts user, service, or device access to various resources based on the identity of the user, service, device.

Federal Information Security Modernization Act of 2014

The stated goals of Federal Information Security Modernization Act of 2014 (FISMA) are as follows:

- 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.[66]

FISMA also requires an annual independent assessment of each agency's information security

[66] FISMA.

program to determine its effectiveness. Inspectors general or independent external auditors must conduct annual evaluations. The 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 2023 through July 2023. The team evaluated configuration management, security management, and access controls of operational VA information technology (IT) assets and resources in accordance with the Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST) security guidelines, and VA's IT security policy. In addition, the team assessed the capabilities and effectiveness of IT security controls used to protect VA systems and data from unauthorized access, use, modification, and destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies and inspected the center and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the VA Dublin Healthcare System's IT security, operations, and privacy compliance. To determine local systems' security compliance, the team conducted vulnerability and configuration testing. 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 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 the GAO's *Federal Information System Controls Audit Manual* (FISCAM) as a template to plan for the inspection. When planning for this review, the team identified potential information system controls that would significantly affect the review. Specifically, the team used the FISCAM appendix II as a guide to help develop evidence requests and interview questions for healthcare system 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 VA Dublin Healthcare System 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.

Fraud Assessment

The inspection team assessed the risk that fraud and noncompliance with provisions of laws, regulations, contracts, and grant agreements, significant in the context of the inspection objectives, could occur during this inspection. The team exercised due diligence in staying alert to any fraud indicators. The VA Office of Inspector General (OIG) did not identify any instances of fraud or potential fraud during this inspection.

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 inspection team used industry-standard information system security tools 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.

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: August 22, 2023

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

Subj: Office of Inspector General Draft Report: Inspection of Information Security at the VA Dublin Healthcare System in Georgia, Project Number 2023-01138-AE-004 (VIEWS 10631151)

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

1. Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, Inspection of Information Security at the VA Dublin Healthcare System in Georgia (Project Number 2023-01138-AE-004).

2. The Office of Information and Technology (OIT) submits the attached written comments.

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 VA Dublin Healthcare System in Georgia*,**
Project Number 2023-01138-AE-0042
(VIEWS 10631151)

Recommendation 1: Improve vulnerability management processes to ensure system changes occur within organization timelines.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information Technology (OIT) concurs with Recommendation 1. VA had already developed, and was implementing, an enterprise-wide process to link vulnerabilities to Plan of Action and Milestones (POAM) items. However, at the time of the Office of Inspector General's (OIG) inspection, VA had not yet fully implemented this process for all the area boundaries, including the Dublin VA Medical Center. VA completed this milestone on July 30, 2023. The Dublin VA Medical Center has now completed their implementation of POAM Vulnerability Portal-to-POAM item linkage, as is evidenced in the data export provided in support of VA's request to close this recommendation.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 1**.**

Recommendation 2: Develop and approve an authorization to operate for the special-purpose systems.

Comments: Concur.

VA OIT's Specialized Device Cybersecurity Department is working to implement special-purpose systems (SPS) onto the VA network. A VA Authorizing Official (AO) will assess the SPS systems' security plans and boundaries for an Authority to Operate (ATO).

Expected Completion Date: December 31, 2025.

Recommendation 3: Include system personnel during the security categorization process to ensure that all necessary information types are considered when determining the security categorization for special-purpose systems.

Comments: Concur.

VA OIT is in the process of obtaining an ATO that will ensure system personnel are included during the security categorization process. Once the project is completed in fiscal year 2025, OIT will consider all necessary information types when determining the security categorization for SPS. As a result, the existing categorization applies until ATO determinations are made for SPS based on the SPS Categorization Report.

Expected Completion Date: September 30, 2025.

Recommendation 4: Review the list of unauthorized software and remediate or remove unneeded software at the facility.

Comments: Concur.

The Dublin VA Medical Center completed the review of unauthorized software and remediated unneeded software. The cleanup of the unapproved software was completed on May 25, 2023.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 4.

<u>Recommendation 5</u>: Implement the appropriate physical security controls to restrict and monitor access to the facility, its server room, communication closets, and generators.

Comments: Concur.

- The VA Physical Design Manual addresses generators: VA Handbook 0730, *Security and Law Enforcement* is the companion document. Both documents indicate physical barriers in the specific area are not required for pedestrian control, because other concentric layers of security are in place. Moreover, the generators are secured on an elevated concrete foundation which protects them from vehicular damage, thus eliminating the need for bollards. VA requests closure of this finding.
- The Dublin VA Medical Center immediately locked the unlocked generator container onsite once identified by OIG. The finding has been remediated and VA requests closure.
- The Dublin VA Medical Center removed the individuals with badge access and updated the access memorandum to the server room. Individuals identified by OIG no longer have access. The finding has been remediated and VA requests closure.
- Electronic Health Record Modernization redesign for the server room will replace doors and locks. The project will remediate the key deficiencies identified by OIG. The acquisition package has been approved and sent to contracting for review and bid. Estimated contract award is by quarter one, fiscal year 2024.
- The Dublin VA Medical Center began the project design for additional cameras and other key areas in 2019. The project was approved with an estimated completion date of October 30, 2023.

Expected Completion Date: September 30, 2024.

VA OIT requests partial closure of Recommendation 5 (bullets 1, 2 and 3).

<u>Recommendation 6</u>: Implement and monitor emergency power and uninterruptible power supplies that support information technology resources.

Comments: Concur.

Dublin VA Medical Center Engineering and Electric Shop remediated the issue with defective uninterruptible power supplies on July 31, 2023. Emergency power outlets in information technology closets will be replaced by October 30, 2023.

Expected Completion Date: October 30, 2023.

<u>Recommendation 7</u>: Validate that appropriate physical and environmental security measures are implemented and functioning as intended.

Comments: Concur.

VA OIT End User Operations (EUO) is updating the relevant standard operating procedure (SOP) to address the issue. EUO will update the Physical and Environmental Protection SOP to clarify the verbiage to remediate the finding.

Expected Completion Date: October 30, 2023.

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 Keith Hargrove Timothy Moorehead Albert Schmidt Brandon Zahn
Other Contributors	Dustin Campbell Melinda Peal Bishop Jill Russell Clifford Stoddard

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

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
US Senate: Jon Ossoff, Raphael Warnock
US House of Representatives: Rick Allen

OIG reports are available at www.va.gov/oig.