DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the Tuscaloosa VA Medical Center in Alabama

INFORMATION SECURITY INSPECTION | REPORT #22-01854-13 | JANUARY 18, 2023

MISSION

The mission of the Office of Inspector General is to serve veterans and the public by conducting meaningful independent oversight of the Department of Veterans Affairs.

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.

Report suspected wrongdoing in VA programs and operations to the VA OIG Hotline:

www.va.gov/oig/hotline

1-800-488-8244

Executive Summary

Information technology (IT) 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.[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 2021 FISMA audit indicated that VA continues to face significant challenges meeting the law's requirements. The audit resulted in 26 recommendations made to VA. Repeat recommendations included addressing deficiencies in configuration management, contingency planning, 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 IT security requirements related to four control areas the OIG determined to be at highest risk.[4] They are typically conducted at selected facilities that have not been assessed in the sample for the annual audit or at facilities that previously performed poorly.

The OIG conducted this inspection to determine whether the Tuscaloosa VA Medical Center (VAMC) was meeting those requirements. The OIG selected the Tuscaloosa VAMC 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 the following four security control areas:

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

[1] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014) § 3555(b)(1).

[2] NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, December 10, 2020.

[3] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*, Report No. 21-01309-74, April 13, 2022.

[4] Appendix B presents background information on federal information security requirements.

[5] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G, February 2009, p. 12.

2. **Contingency planning controls** provide reasonable assurance that information resources are protected, minimize risk from unplanned interruptions, and provide for recovery of critical operations should interruptions occur.[6]
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."[7]
4. **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.

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

What the Inspection Found

The OIG identified deficiencies with configuration management, security management, and access controls. The inspection team did not identify deficiencies with contingency planning controls.

Three Configuration Management Controls Had Deficiencies

The Tuscaloosa VAMC had security deficiencies in the following configuration management controls:

- **Vulnerability management** is the process by which the Office of Information and Technology (OIT) identifies, classifies, and reduces weaknesses.
- **Flaw remediation** is how organizations correct software defects and often includes system updates, such as security patches.[8]
- **Database scans** are a specialized tool used to specifically identify vulnerabilities in database applications.[9]

VA has a vulnerability management program, but it can be improved. Prior FISMA audits repeatedly found deficiencies in VA's vulnerability management. Consistent with those findings,

[6] *FISCAM*, p. 12.
[7] *FISCAM*, p. 11.
[8] NIST Special Publication 800-53, rev 5.
[9] NIST Special Publication 800-53.

the team identified deficiencies at the Tuscaloosa VAMC. OIT scans for vulnerabilities routinely, randomly, and when new vulnerabilities are identified and reported.[10] Although the inspection team and OIT used the same vulnerability-scanning tools, OIT did not detect all the vulnerabilities the team found. For example, the OIG found 119 critical-risk vulnerabilities that OIT did not detect. The inspection team also identified 301 vulnerabilities—167 critical-risk vulnerabilities on 14 percent of the devices and 134 high-risk vulnerabilities on 46 percent of the devices—which were not mitigated within the required 30- or 60-day windows. While OIT is aware of many of the vulnerabilities, its plans of actions and milestones did not always list remediations.[11]

Despite VA's significant patch management measures, the inspection team identified several devices that were missing security patches. For instance, several devices with critical- and high-risk vulnerabilities had patches available that were not applied. Without these controls, VA may be placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

OIT requires database scans to be performed on a quarterly basis. However, OIT could only provide scans for half of the database servers supporting the Tuscaloosa VAMC. All the databases were configured to be scanned; however, according to OIT, the Cybersecurity Operations Center was unable to reach the databases due to a port-filtering issue. Data stored within a database management system have become targets of attack for malicious users with increased frequency. Such an attack can lead to identity theft, credit card theft, financial loss, loss of privacy, or any other type of corruption that can result from unauthorized access to sensitive database information. Without periodic database scans, OIT is unaware of security control weaknesses that could adversely impact the security posture of databases supporting the facility.

One Security Management Control Was Deficient

The OIG identified one security management control weakness: several plans of actions and milestones were missing or lacked sufficient details to be actionable. For the purpose of inspections, the OIG considers a vulnerability managed if the plan of actions and milestones accurately identifies the devices impacted, details mitigation efforts, and includes a timely schedule of milestones. During the inspection, the OIG discovered that the plans of actions and milestones did not always list remediation actions or resource constraints for remediations not yet implemented. For instance, a plan of actions and milestones created for a vulnerability related

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

[11] Plans of action and milestones identify tasks necessary to address a vulnerability, deficiency, or risk and detail resources required to accomplish the tasks, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

to server components mentioned updating software according to vendor requirements but did not specify what actions needed to be taken or what resource limitations prevented implementation. The OIG also found that plans of actions and milestones were created for a very small percentage of the hosts with critical-risk vulnerabilities. Further, a high-risk vulnerability identified by OIT in 2015 did not have a plan of actions and milestones created, and no evidence suggested that OIT acted or developed a plan to remediate the deficiency. Without a plan of actions and milestones, the risk presented by the vulnerability cannot be managed and resources will less likely be available for remediation.

Four Access Controls Had Deficiencies

The Tuscaloosa VAMC had security deficiencies in the following access controls:

- **Network segmentation controls** regulate where information can travel within a system and between systems.[12]
- **Audit and monitoring controls** involve the collection, review, and analysis of events for indications of inappropriate or unusual activity.
- **Environmental controls** maintain and monitor temperature and humidity where communication equipment is located.[13]
- **Emergency power** provides near-instantaneous protection from unanticipated power interruptions and protects equipment where unexpected power disruption could cause injuries, fatalities, mission or business disruption, or loss of information.

The Tuscaloosa VAMC did not have network segmentation controls in place for several network segments that contained medical and special-purpose systems.[14] Network-connected medical devices and special-purpose systems are placed on isolated network segments for protection. However, the OIG identified 19 network segments containing 221 medical devices and special-purpose systems that did not have access control lists applied. Without network segmentation controls in place, any user can access these potentially vulnerable medical and special-purpose devices.

[12] NIST Special Publication 800-53.

[13] NIST Special Publication 800-53.

[14] A special-purpose system is a nonmedical, network-connected systems that supports building safety, security, or environmental controls and cannot obtain a VA-approved baseline configuration due to vendor-controlled system policies, proprietary software, and other system-specific controls and configurations. Examples of special-purpose systems include, but are not limited to, energy management systems, heating, ventilation, and air conditioning, temperature controls, building/facility access controls, and security camera systems.

The OIG determined that improvements are needed for log retention and reviews because logs were missing for half the databases supporting the Tuscaloosa VAMC. These controls should be routinely used to evaluate the effectiveness of other security controls, recognize attacks, and investigate during or after attacks.[15] OIT was unable to demonstrate that log data was collected for half of the databases supporting the Tuscaloosa VAMC. More specifically, the databases did not have the application installed that OIT uses to collect log data for databases. The team determined that the databases without log data were the same databases that did not have vulnerability scans conducted. Logs frequently help with incident analysis as they provide information, such as 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.

During a walk-through, the inspection team discovered several communication rooms without temperature or humidity controls. Insufficient environmental controls can have a significant adverse impact on the availability of systems needed to support the organizational mission and business functions.

The inspection team also found several communication rooms missing uninterruptible power supplies supporting the VAMC. The facility purchased but never installed the equipment. Without operational uninterruptible power supplies, the infrastructure equipment will not function during power fluctuations or outages, resulting in interruption of data flow and disruption of access to network resources.

What the OIG Recommended

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

1. Implement a more effective vulnerability management program to address security deficiencies identified during the inspection.
2. Ensure vulnerabilities are remediated within established time frames.
3. Ensure all databases at the facility are part of the periodic database scan process.
4. Implement improved mechanisms to ensure system stewards are updating plans of action and milestones for all known security risks, including those identified during security control assessments.
5. Ensure network segmentation controls are applied to all network segments with medical devices and special-purpose systems.

[15] *FISCAM*.

6. Implement capabilities for generating database audit logs and forwarding audit events for analysis.

The OIG made these recommendations to the assistant secretary because they are related to enterprise-wide IT security issues, similar to those identified on previous FISMA audits and IT security reviews.

The OIG also made two recommendations to the Tuscaloosa VAMC director:

7. Ensure communication rooms with infrastructure equipment have adequate environmental controls.
8. Install uninterruptible power supplies in the communication rooms supporting infrastructure equipment.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1, 2, 4, and 6 through 8; partially concurred with recommendation 5; and did not concur with recommendation 3.

Responsive action plans were submitted for the seven recommendations that received concurrences or partial concurrences from the assistant secretary. Regarding recommendation 3—to ensure all databases at the Tuscaloosa VAMC are part of the periodic database scan process—the assistant secretary reported that although VA was initially unable to provide historical vulnerability scan results for specific devices, VA's Cybersecurity Operations Center later provided the requested evidence to the OIG. However, the evidence provided did not include the specific devices missing from the original response to the OIG's request for scan results. Further, the OIG accessed OIT's most recent scan results, which show the devices are still not present. Because the claim that all databases are included in the VAMC's scanning process could not be validated, the OIG stands by its recommendation, and it will remain open.

Recommendation 5—to ensure network segmentation controls are applied to all segments with medical devices and special-purpose systems—received a partial concurrence from the assistant secretary, who reported, but did not provide evidence, that the OIG's analysis was not completely accurate. The assistant secretary agreed, however, that several network segments were not configured in accordance with VA policy, and VA has since submitted work orders to bring the network configurations into compliance.

The assistant secretary concurred with recommendation 1 but reported that VA's latest analysis of the OIG's scan results for the facility displayed a 99.84 percent rate of policy compliance. However, no evidence was provided that would allow the OIG to validate this assertion. In fact, OIT's own results that the OIG received on November 16, 2022, indicated that 84 percent of the

critical- and high-risk vulnerabilities had remediations completed, while the remaining vulnerabilities were awaiting updates or had corresponding plans of actions and milestones.

Regarding recommendation 2, the assistant secretary concurred but stated that VA's overall patch and vulnerability compliance percentages provide evidence that an effective vulnerability management and flaw remediation program has in fact been implemented. However, the assistant secretary's statement runs counter to the OIG's results, which showed 301 vulnerabilities (167 critical-risk vulnerabilities on 14 percent of the devices and 134 high-risk vulnerabilities on 46 percent of the devices) that were not mitigated within the time frames established by OIT. Moreover, OIT's security scans did not identify 119 critical-risk vulnerabilities that the team detected. The OIG will monitor the implementation of the planned actions for these and the remaining recommendations and will close them when VA provides sufficient evidence demonstrating progress in addressing the issues identified. The full text of the assistant secretary's response is included in appendix D.

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
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
VAMC	VA medical center

Introduction

Information technology (IT) 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.[16] 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.[17]

In 2020, the OIG also started an information security inspection program. These inspections assess whether VA facilities are meeting federal IT security requirements that protect systems and data from unauthorized access, use, modification, or destruction.[18] 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 facilities.[19] Appendix C provides more detail on the inspection scope and methodology.

The OIG conducted this inspection to determine whether the Tuscaloosa VA Medical Center (VAMC) was meeting those requirements. The OIG selected the Tuscaloosa VAMC 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 Tuscaloosa VAMC, other facilities across VA could benefit from reviewing this information and considering these recommendations.

[16] Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. No. 113-283, 128 Stat. 3073 (2014).

[17] NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, December 10, 2020.

[18] Appendix B presents background information on federal information security requirements.

[19] 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.

Security Controls

Both 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.[20]

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 is also VA's chief information officer. VA Handbook 6500 describes the risk-based process for selecting system security controls, including the operational requirements.[21] VA established guidance outlining both NIST- and VA-specific requirements to help information system owners select the appropriate controls to secure their systems.

The OIG's information security inspections are focused on four security control areas that apply to local facilities and have been selected based on their level of risk, as shown in table 1.

[20] OMB, "Security of Federal Automated Information Resources," app. 3 in OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016; NIST Special Publication 800-53.

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

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 and risk of unplanned interruptions is minimized, as well as provide for recovery of critical operations should interruptions occur	Continuity of operations, contingency planning, disaster recovery, environmental, and maintenance
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 and environmental security controls, such as authorization, visitors, monitoring delivery and removal

Source: VA OIG analysis.

Without these critical controls, VA's systems are at risk of unauthorized access or modifications. A cyberattack could disrupt, 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 and acts as a steward for VA's IT assets and resources. 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 unifies software development, software operations, service management, information assurance, cybersecurity compliance, performance monitoring, and technical integration throughout the entire solution delivery process. Figure 1 shows the organization of offices within OIT that are relevant to this inspection.

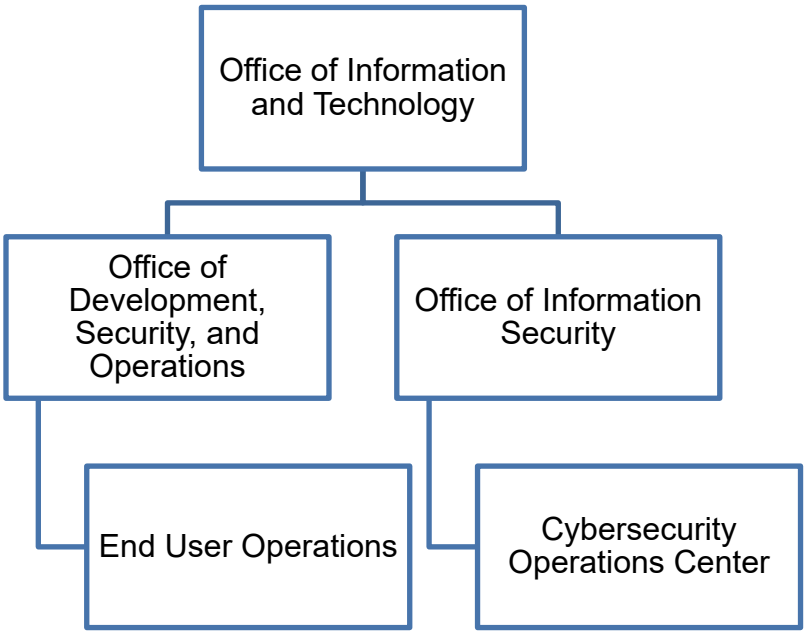

Figure 1. *Organizational structure of OIT entities relevant to this inspection.*

Source: VA OIG analysis.

End User Operations provides on-site and remote support to IT customers across all VA administrations and special program offices, including direct support of over 340,000 VA employees and thousands of contractors who are issued government-furnished IT equipment and access. End User Operations provisions 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 personnel to the Tuscaloosa VAMC, including system stewards who are responsible for managing system plans of actions and milestones to ensure that 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 OMB and applicable NIST information security guidelines.[22] The fiscal year 2021 FISMA audit, conducted by independent public accounting firm CliftonLarsonAllen LLP, evaluated 50 major applications and general support systems hosted at 24 VA facilities, including the testing of selected

[22] 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.

management, technical, and operational controls outlined by NIST.[23] CliftonLarsonAllen LLP made 26 recommendations, listed in appendix A, all of which are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[24] Recommendations included addressing deficiencies in configuration management, contingency planning, 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.[25] According to GAO, VA faced several security challenges while securing and modernizing its information systems, including

- effectively implementing information security controls,
- mitigating known vulnerabilities,[26]
- 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."[27]

Tuscaloosa VAMC

The Tuscaloosa VAMC in Alabama is part of the VA Tuscaloosa Healthcare System. The VAMC provides primary care, long-term health care, and mental health care to veterans in the VA southeast network. The medical center is a teaching hospital and maintains affiliations with the University of Alabama; University of Alabama at Birmingham; and other leading colleges, universities, and professional schools throughout the United States.

[23] General support system is defined as an "interconnected set of information resources under the same direct management control which shares common functionality." OMB, "Security of Federal Automated Information Resources."

[24] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*, Report No. 21-01309-74, April 13, 2022; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021. Appendix B presents information about FISMA and other federal criteria and standards discussed in this report.

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

[26] A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." *FISCAM*, p. 590.

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

Figure 2. *Tuscaloosa VAMC.*
Source: https://www.va.gov/tuscaloosa-health-care/, June 13, 2022.

Results and Recommendations

I. Configuration Management Controls

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 reviewed and evaluated the 12 configuration management controls drawn from NIST criteria for VA-hosted systems at the Tuscaloosa VAMC to determine if they 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.[28] VA should first establish an accurate component inventory to identify all devices on the network.[29] The component inventory affects the success of other controls, such as vulnerability and patch management. According to the configuration management standard operating procedure, OIT's Cybersecurity Operations Center identifies and reports on threats and vulnerabilities, and OIT's Patch and Vulnerability Team develops procedures to remediate these issues, which can include applying patches. This process helps to secure devices from attack.[30]

Finding 1: The Tuscaloosa VAMC Had Deficiencies in Two Configuration Management Controls

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 Tuscaloosa VAMC'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 Tuscaloosa VAMC's network to identify vulnerabilities.[31] Comparisons of the vulnerability scans showed that OIT did not identify all critical- or high-risk vulnerabilities in the network or remediate flaws, including unsupported versions of applications, missing patches, and vulnerable plug-ins. Also, database scans were not being conducted for half of the databases supporting the Tuscaloosa VAMC. By not implementing more effective configuration management controls,

[28] *FISCAM*, p. 268.

[29] *FISCAM*, p. 270.

[30] OIT Area Tuscaloosa, "Configuration Management" (standard operating procedure), December 3, 2020; VA Handbook 6500.

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

VA is placing critical systems at unnecessary risk of unauthorized access, alteration, or destruction.

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. 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. The Cybersecurity Operations Center identifies and reports on threats and vulnerabilities, while OIT conducts scans for vulnerabilities, both routinely and randomly, or when new vulnerabilities are identified and reported.[32]

VA conducts periodic independent scans of all of its systems. According to the standard operating procedures, the discovered vulnerabilities are entered into a plan of action and milestones for remediation by the system steward. The system technicians remediate vulnerabilities and document those efforts in the Remediation Effort Entry Form.[33]

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[34] 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 in 60 days.

The inspection team compared OIT-provided network vulnerability scan results from the Tuscaloosa VAMC against its own scans conducted from April 11 to April 15, 2022. The team and OIT used the same vulnerability-scanning tools. The team identified 301 vulnerabilities (167 critical-risk vulnerabilities on 22 percent of the devices and 134 high-risk vulnerabilities on 46 percent of the devices) that were not mitigated within the time frames established by OIT. Moreover, OIT's security scans did not identify 119 critical-risk vulnerabilities the team

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

[33] A 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. OIT Area Tuscaloosa, "Configuration Management."

[34] "Vulnerability Metrics," 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," Forum of Incident Response and Security Teams (FIRST), accessed July 5, 2022, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

detected. Similarly, the prior FISMA audit found that "VA did not have a complete inventory of all vulnerabilities present on locally hosted systems."[35] While OIT is aware of many of the vulnerabilities, its plans of actions and milestones did not always list remediations.[36] Several of the plans of actions and milestones were missing or lacked sufficient detail to be actionable. Further, less than 3 percent of the hosts with critical-risk vulnerabilities were accounted for in the plans of actions and milestones. The OIG identified critical- and high-risk vulnerabilities on 50 percent of the devices at the Tuscaloosa VAMC. 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.

The medical center did not remediate all flaws affecting devices in its network. For example, the inspection team identified vulnerabilities, such as operating systems that were no longer supported by the vendor and applications with missing security patches. The flaw remediation process identifies, reports, and corrects system flaws, including installing security-relevant software and firmware updates.[37] Security-relevant updates include patches, service packs, and malicious code signatures. Security patches are usually the most effective way to mitigate software flaw vulnerabilities. According to GAO, a patch is a piece of software code inserted into a program to temporarily fix a defect until an updated software version is released. NIST further explains that patches correct security and functionality problems in software and firmware.[38] Patch management is how an organization acquires, tests, applies, and monitors updates that address security and functionality problems. Although patch management is a critical process used to help alleviate many of the challenges in securing systems from cyberattack, previous FISMA audits have repeatedly found deficiencies in this area.[39]

Database Vulnerability Scans

Database scans are a specialized tool used to specifically identify vulnerabilities in database applications. OIT requires database scans to be performed on a quarterly basis. However, OIT could only provide evidence of scans for half of the servers supporting the Tuscaloosa VAMC.

---

[35] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*.

[36] Plans of actions and milestones identify tasks that need to be accomplished. They detail resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. They also describe the measures planned to correct deficiencies identified in the controls and to address known vulnerabilities or security and privacy risks. For the purpose of inspections, the OIG considers a vulnerability managed—even if it still exists—if the plan of action and milestones accurately identifies the devices impacted and details mitigation efforts, and the schedule of milestones is accurate and timely.

[37] NIST Special Publication 800-53.

[38] *FISCAM,* p. 292.

[39] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2019*, Report No. 19-06935-96, March 31, 2020; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2018*, Report No. 18-02127-64, March 12, 2019.

According to OIT, the reason for the limited number of scans was that, even though all the databases were configured to be scanned, the Cybersecurity Operations Center was unable to reach some databases due to a port-filtering issue.[40] Data stored within a database management system has become a target of attack for malicious users, with increased frequency. The effect of such an attack can result in identity theft, credit card theft, financial loss, loss of privacy, or any other type of corruption that can result from unauthorized access to sensitive data. Without periodic database scans, OIT is unaware of security control weaknesses that could adversely impact the security posture of databases supporting the facility.

Finding 1 Conclusion

The Tuscaloosa VAMC vulnerability management controls did not identify all network weaknesses, such as unsupported versions of applications, and flaw remediation controls did not ensure comprehensive patch management. Further, vulnerabilities were not always remediated within OIT-established time frames and database scans were not being conducted for half of the databases supporting the Tuscaloosa VAMC. Without effective configuration management, users do not have adequate assurance that the system and network will perform as intended and to the extent needed to support VA missions.

Recommendations 1–3

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

1. Implement a more effective vulnerability management program to address security deficiencies identified during the inspection.
2. Ensure vulnerabilities are remediated within established time frames.
3. Ensure all databases at the Tuscaloosa VA Medical Center are part of the periodic database scan process.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 2. To address both recommendations, the assistant secretary reported that VA consistently maintains a 90 percent or greater management rate of critical vulnerabilities across the enterprise. He reported VA's continuous monitoring and existing vulnerability management program continues to track items to a compliant status. According to the assistant secretary, VA's updated scan results displayed evidence of a fully compliant status

[40] Port filtering is a security control that restricts network traffic into or out of a device based on authorized network protocols.

for all OIG-detected items, including hosts with vulnerabilities that exist beyond their established remediation timeframes. The assistant secretary also reported that VA's latest analysis of the OIG's scan results for the facility displayed a 99.84 percent rate of policy compliance. VA will follow up on remaining pending or status update vulnerability items to ensure those vulnerabilities are addressed to a compliant state.

The assistant secretary did not concur with recommendation 3, reporting that although VA was initially unable to provide historical vulnerability scan results for specific devices, the Cybersecurity Operations Center later provided the requested evidence to the OIG.

OIG Response

The assistant secretary provided in-progress corrective actions for recommendations 1 and 2 that are responsive to their intent. Despite concurring with each of these recommendations, the assistant secretary stated that VA's latest analysis of OIG's scan results displayed a 99.84 percent rate of policy compliance. However, no evidence was provided that would allow the OIG to validate this assertion. In fact, OIT's own scan results that were provided to the OIG on November 16, 2022, showed that 84 percent of the critical- and high-risk vulnerabilities had remediations completed, while the remaining vulnerabilities were awaiting updates or had corresponding plans of actions and milestones.

The assistant secretary also stated that VA's overall patch and vulnerability compliance percentages provide evidence that an effective vulnerability management and flaw remediation program has already been implemented. However, this statement runs counter to the OIG's results that showed 301 vulnerabilities (167 critical-risk vulnerabilities on 14 percent of the devices and 134 high-risk vulnerabilities on 46 percent of the devices) that were not mitigated within the time frames established by OIT. Moreover, OIT's security scans did not identify 119 critical-risk vulnerabilities the team detected. 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.

Regarding recommendation 3, the evidence provided by the Cybersecurity Operations Center, which was meant to demonstrate that all databases at the medical center are included in the scanning process, does not include the specific devices missing from the original response to the OIG's request for scan results. Further, the OIG accessed OIT's most recent scan results, and the devices are still not present. Consequently, the OIG was unable to validate the claim that all databases are included in the medical center's scanning process and therefore stands by this recommendation, and it will remain open. The full text of the response from the assistant secretary is included in appendix D.

II. Contingency Planning Controls

If contingency planning controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.[41] Federal agencies are mandated by law to 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."[42] Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions.[43] 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 Tuscaloosa VAMC met federal guidance and VA requirements, the inspection team evaluated six contingency planning controls.

Finding 2: Contingency Planning Controls Had No Deficiencies

To assess contingency planning controls, the inspection team interviewed the area manager and information system security officer, reviewed local policies and procedures, and conducted a walk-through of the facility. The OIG found that the facility's contingency plan addressed control criteria, such as identifying essential mission and business functions, provided recovery objectives, and addressed roles and responsibilities. The team verified that the Tuscaloosa VAMC had no critical information systems that would require an alternate processing facility. Instead, the enterprise manages the systems at regional data centers. The team did not identify deficiencies in the Tuscaloosa VAMC's contingency planning controls. Accordingly, the OIG did not make any recommendations for improvement.

[41] *FISCAM*, p. 312.
[42] FISMA § 3554 (b)(8).
[43] *FISCAM*, p. 312.

III. Security Management Controls

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 two security management critical elements: instituting a security management program and assessing and validating risk.[44]

Finding 3: The Tuscaloosa VAMC Had One Security Management Control Deficiency

To assess security management controls, the inspection team reviewed local security management policies and standard operating procedures, as well as 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 assessing and validating risks, security control policies and procedures, and plans of actions 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.

Plans of Actions and Milestones

The OIG identified one security management control weakness: several plans of actions and milestones were missing or lacked sufficient details to be actionable.

During the inspection, the OIG discovered that the plans of actions and milestones did not always list remediations or resource constraints for remediations not yet implemented. For instance, a plan of actions and milestones created for a vulnerability related to server components only mentioned updating software according to vendor requirements. It did not specify what actions needed to be followed or what resource limitations were preventing implementation. As stated previously, less than 3 percent of the hosts with critical-risk vulnerabilities were accounted for in the plans of actions and milestones. Further, a high-risk vulnerability identified by OIT in 2015 did not have a plan of actions or milestones created, and there was no evidence to suggest OIT either acted or developed a plan to remediate the deficiency. Without a plan of actions and milestones, the risk presented by the vulnerability cannot be managed and it is less likely that resources will be available for remediation.

[44] *FISCAM* critical elements for security management are listed in appendix B.

Recommendation 4

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

4. Implement improved mechanisms to ensure system stewards are updating plans of actions and milestones for all known risks and weaknesses, including those identified during security control assessments.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 4. The assistant secretary reported that VA is addressing the issues via national changes to the vulnerability management program and assignment of new personnel with responsibility for the implementation and updating of evidence within the organization's governance, risk, and compliance tool.

OIG Response

The assistant secretary reported corrective action for recommendation 4 is in progress and provided an estimated completion date. The planned corrective actions are responsive to the intent of the recommendation. 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. The full text of the response from the assistant secretary is included in appendix D.

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. Access also includes physical and environmental controls associated with physical security, such as authorization, visitors, monitoring, delivery, and removal. Identification, authentication, and authorization controls ensure that users have the proper access and access is restricted to authorized individuals. At the Tuscaloosa VAMC, the inspection team reviewed three critical access control elements, each of which contain multiple controls.[45]

Finding 4: The Tuscaloosa VAMC Had Deficiencies in Four Access Controls

To evaluate the Tuscaloosa VAMC's access controls, the inspection team interviewed the area manager, information system security officer, biomedical supervisor, and database administrators; reviewed local policies and procedures; conducted walk-throughs of the facility; and analyzed audit logs.[46]

The OIG found these issues with access controls at the Tuscaloosa VAMC:

- Network segmentation controls to isolate several medical devices and special-purpose systems were missing.
- Audit and monitoring controls had weaknesses because approximately half of the databases were not generating or forwarding log data.
- Several rooms containing infrastructure network equipment lacked environmental controls.
- Uninterruptible power supplies to support network infrastructure equipment were lacking.

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

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

Network Segmentation Controls

The Tuscaloosa VAMC did not have network segmentation controls in place for several network segments that contained medical and special-purpose systems.[47] Network segmentation controls regulate where information can travel within a system and between systems.[48]

Network-connected medical devices and special-purpose systems are placed on isolation network segments for protection. Protection is provided through access control lists. However, during the inspection, the OIG identified 19 network segments containing 221 medical devices and special-purpose systems that did not have access control lists applied. Without effective network segmentation controls in place, any user can access these potentially vulnerable medical and special-purpose devices.

Audit and Monitoring Controls

The OIG determined that improvements are needed for log retention and log reviews for approximately half the databases supporting the Tuscaloosa VAMC.[49] 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, recognize an attack, and investigate during or after an attack.[50] OIT was unable to demonstrate that log data was collected for approximately half of the databases supporting the Tuscaloosa VAMC. More specifically, the databases did not have the application installed that OIT uses to collect log data for databases. Logs frequently help with incident analysis, such as providing information regarding 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.

Temperature and Humidity Controls

During a walk-through, the inspection team discovered several communication rooms without temperature or humidity controls. Environmental controls maintain and monitor temperature and humidity where communication equipment is located.[51] Equipment was installed in

[47] A special-purpose system is a nonmedical, network-connected system that supports building safety, security, or environmental controls and cannot obtain a VA-approved baseline configuration due to vendor-controlled system policies, proprietary software, and other system-specific controls and configurations. Examples of special-purpose systems include energy management systems, heating, ventilation, air conditioning, temperature controls, building/facility access controls, and security camera systems.

[48] NIST Special Publication, 800-53.

[49] The team determined that the databases without log data were the same databases that did not have vulnerability scans conducted.

[50] *FISCAM*, p. 244.

[51] NIST Special Publication, 800-53.

communication rooms without sufficient environmental controls. This is a risk because insufficient environmental controls can have a significant adverse impact on the availability of systems that are needed to support the organizational mission and business functions.

Emergency Power

The team also found several communication rooms missing uninterruptible power supplies supporting the VAMC. An uninterruptible power supply is an electrical system or mechanism that provides emergency power when there is a failure of the main power source.[52] 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 facility purchased the equipment for uninterruptible power in September 2019. According to the area manager, the equipment was not installed due to the impact of COVID-19 on technician availability. 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.

Finding 4 Conclusion

The Tuscaloosa VAMC did not have network segmentation controls for some medical devices and special-purpose systems to protect them from unauthorized access. Additionally, audit logs were not collected or retained for approximately half of the databases supporting the Tuscaloosa VAMC, which could impact incident analysis. Furthermore, several communication rooms did not have temperature or humidity controls, which could have a significant adverse impact on the availability of systems. Finally, uninterruptible power supplies, which protect equipment in case of a power outage, were purchased for several communication rooms but not installed. Unless the VAMC takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information.

Recommendations 5–8

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

5. Ensure network segmentation controls are applied to all network segments with medical devices and special-purpose systems.

[52] NIST Special Publication, 800-53.

6. Implement capabilities for generating database audit logs and forwarding audit events for review, analysis, and reporting.

The OIG made the following recommendations to the Tuscaloosa VAMC director:

7. Ensure communication rooms with infrastructure equipment have adequate environmental controls.
8. Install uninterruptible power supplies in the communication rooms supporting infrastructure equipment.

VA Management Comments

The assistant secretary for information and technology and chief information officer partially concurred with recommendation 5. The assistant secretary reported that OIT does not agree that OIG's analysis was completely accurate but agrees that several network segments were not configured in accordance with VA policy. VA has submitted work orders to bring the network configuration into compliance.

The assistant secretary concurred with recommendations 6, 7, and 8. To address recommendation 6, he reported that OIT will implement capabilities for generating database audit logs and forwarding audit events for review, analysis, and reporting. To address recommendations 7 and 8, he said the Tuscaloosa VAMC will implement infrastructure upgrades to address all temperature and humidity concerns and install new uninterruptible power supplies.

OIG Response

For recommendation 5, the assistant secretary did not provide evidence allowing the OIG to validate the assertion that the analysis was not completely accurate. However, the planned corrective actions are responsive to the intent of the recommendation. The OIG will monitor the implementation of planned actions and will close the recommendation when VA provides evidence demonstrating progress in addressing the issue identified.

The assistant secretary reported that corrective actions for recommendations 6, 7, and 8 were in progress and provided estimated completion dates. 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. The full text of the response from the assistant secretary is included in appendix D.

Appendix A: FISMA Audit for Fiscal Year 2021 Report Recommendations

In the FISMA audit for fiscal year 2021, CliftonLarsonAllen LLP made 26 recommendations. All 26 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 Tuscaloosa VAMC. The 26 recommendations are listed below:

1. Consistently implement an improved continuous monitoring program in accordance with the NIST Risk Management Framework. Specifically, implement an independent security control assessment process to evaluate the effectiveness of security controls prior to granting authorization decisions.
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 documents such as security plans, risk assessments, and interconnection agreements on an annual basis and ensure the information 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's authoritative system of record 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 implemented 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. Consolidate the security responsibilities for networks not managed by the Office of Information and Technology, under a common control for each site and ensure vulnerabilities are remediated in a timely manner.
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 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 agencywide incident response procedures to ensure timely notification, reporting, updating, and resolution of computer security incidents in accordance with VA standards.
21. Ensure that VA's Cybersecurity Operations Center has full access to all security incident data to facilitate an agencywide awareness of information security events.
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. Fully develop a comprehensive list of approved and unapproved software and implement continuous monitoring processes to prevent the use of prohibited software on agency devices.
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

GAO developed *FISCAM* to provide auditors and information system control specialists with a specific methodology for evaluating the confidentiality, integrity, and availability of information systems. *FISCAM* groups related controls into categories that have similar risks. To assist auditors in evaluating information systems, *FISCAM* maps control categories to 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.[53] 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 the use of noncurrent software. Examples of these controls are software usage

[53] 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.

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 and 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 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 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.[54]

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

[54] *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 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 of 2014

FISMA has six stated goals:

- 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.[55]

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

[55] FISMA § 3551.

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 March 2022 through September 2022. The team evaluated configuration management, contingency planning, security management, and access controls of operational VA IT assets and resources in accordance with FISMA, 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, or destruction.

Methodology

To accomplish the objective, the inspection team examined relevant laws and policies. The team also inspected the facility and systems for security compliance. Additionally, the team interviewed VA personnel responsible for the Tuscaloosa VAMC IT security and 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 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 *FISCAM* as a template to plan for inspections. When planning for this inspection, the team identified potential information system controls that would significantly affect the inspection. Specifically, the team used *FISCAM* appendix II as a guide to help develop evidence requests and a base set of interview questions for the Tuscaloosa VAMC and its personnel. The team used the *FISCAM* controls identified in appendix B as an overlay to correlate FISMA controls used by VA to protect and secure its information systems. Although similar to the contractor-conducted annual FISMA audits, this inspection focused on security controls that are implemented at the local level. However, there are some controls that overlap and are assessed 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 Tuscaloosa VAMC 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 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 OIT Quality and Compliance Readiness Office. The 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. As the security tools did not alter data, the team determined that the output was reliable. The data were complete and accurate, met intended purposes, and were not subject to alteration.

In addition, computer-processed data included vulnerabilities provided by the cybersecurity operation center. The team used this data to compare vulnerabilities identified by VA with those identified by the OIG. To test for reliability, the team determined whether any data were missing from key fields or were outside the timeframe requested. The review team also assessed whether the data contained obvious duplication of records, alphabetic or numeric characters in incorrect fields, or illogical relationships among data elements. Testing of the data disclosed that they were sufficiently reliable for the inspection objectives.

Government Standards

The OIG conducted this inspection 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: October 30, 2022

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

Subj: OIG Draft Report: Inspection of Information Technology Security at the Tuscaloosa VA Medical Center, Project Number 2022-01854-AE-0082 (VIEWS 08545733)

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

1. The Office of Information and Technology (OIT) is responding to the Office of Inspector General (OIG) draft report, Inspection of Information Technology Security at the Tuscaloosa VA Medical Center (Project Number 2022-01854-AE-0082).

2. OIT submits written comments, supporting documentation and a target completion date for each recommendation.

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 Technology Security at the Tuscaloosa VA Medical Center, Project Number 2022-01854-AE-0082
(VIEWS 08545733)

Recommendation 1: Implement a more effective vulnerability management program to address security deficiencies identified during the inspection.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs. VA's overall patch and vulnerability compliance percentages provide evidence that VA has implemented, and is managing, an effective vulnerability management and flaw remediation program aligned with industry standards. VA consistently maintains a 90% or greater management rate of critical vulnerabilities across the enterprise. VA's latest analysis of the Office of the Inspector General's (OIG) scan results for Tuscaloosa VA Medical Center displays 99.84% policy compliance. VA will follow up on remaining pending or status update vulnerability items to ensure those vulnerabilities are addressed to a compliant state.

VA's continuous monitoring and existing vulnerability management program continues to track items to a compliant status. VA's updated scan results displayed evidence of a fully compliant status for all OIG-detected items, including hosts with vulnerabilities that exist beyond their established remediation timeframes.

VA Cybersecurity Operations Center (CSOC) scans showed data for all subnets except for one. VA identified and will remove the one subnet for which CSOC did not show scan data.

Expected Completion Date: January 31, 2023.

Recommendation 2: Ensure vulnerabilities are remediated within established time frames.

Comments: Concur.

The Department's overall patch and vulnerability compliance percentages provide evidence that VA has implemented, and is managing, an effective vulnerability management and flaw remediation program, aligned with federal and industry standards. VA consistently maintains a 90% or greater management rate of critical vulnerabilities across the enterprise. VA's latest analysis of OIG's scan results for the Tuscaloosa VA Medical Center displays 99.84% policy compliance. VA will follow up on remaining pending or status update vulnerability items to ensure those vulnerabilities are addressed to a compliant state.

Expected Completion Date: January 31, 2023.

Recommendation 3: Ensure all databases at the Tuscaloosa VA Medical Center are part of the periodic database scan process.

Comments: Non-concur.

VA CSOC disagrees with OIG's finding. Although VA was initially unable to provide historical vulnerability scan results for specific devices, CSOC later provided the requested evidence to the auditors.

Expected Completion Date: Completed.

VA OIT requests removal or closure of Recommendation 3.

Recommendation 4: Implement improved mechanisms to ensure system stewards are updating plans of action and milestones for all known risks and weaknesses, including those identified during security control assessments.

Comments: Concur.

Tuscaloosa OIT acknowledges the issues with Tuscaloosa's vulnerability management program. VA is addressing the issues via national changes to the vulnerability management program and assignment of new personnel with responsibility for the implementation and updating of evidence within the organization's governance, risk and compliance tool.

Expected Completion Date: June 30, 2023.

Recommendation 5: Ensure network segmentation controls are applied to all network segments with medical devices and special purpose systems.

Comments: Partially concur.

Although OIT does not agree that OIG's analysis was completely accurate, OIT agrees that several network segments were not configured in accordance with VA policy. VA has submitted work orders to bring the network configuration into compliance.

Expected Completion Date: December 31, 2022.

Recommendation 6: Implement capabilities for generating database audit logs and forwarding audit events for review, analysis, and reporting.

Comments: Concur.

OIT will implement capabilities for generating database audit logs and forwarding audit events for review, analysis and reporting.

Expected Completion Date: December 31, 2022.

Recommendation 7: Ensure communication rooms with infrastructure equipment have adequate environmental controls.

Comments: Concur.

Tuscaloosa VA Medical Center will implement infrastructure upgrades to address all temperature and humidity concerns identified by OIG.

Expected Completion Date: October 31, 2024.

Recommendation 8: Install uninterruptible power supplies in the communication rooms supporting infrastructure equipment.

Comments: Concur.

Tuscaloosa VA Medical Center chief of engineering will install new uninterruptible power supplies in the information technology closets identified by OIG.

Expected Completion Date: December 31, 2022.

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 Ginalynn Alvarado Jack Henserling Kimberly Moss Adam Sowells Brandon Zahn
Other Contributors	Charles Hoskinson

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, Tuscaloosa VAMC

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
U.S. Senate: Katie Boyd Britt, Tommy Tuberville
U.S. House of Representatives: Robert Aderholt, Jerry Carl, Barry Moore, Gary Palmer, Mike Rogers, Terri Sewell, Dale Strong

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