DEPARTMENT OF VETERANS AFFAIRS

OFFICE OF INSPECTOR GENERAL

Office of Audits and Evaluations

VETERANS HEALTH ADMINISTRATION

Inspection of Information Security at the St. Cloud VA Medical Center in Minnesota

INFORMATION SECURITY INSPECTION | REPORT #22-02961-71 | JUNE 8, 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 made 26 recommendations 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 IT security inspection program. These IT inspections assess whether VA facilities are meeting federal 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 St. Cloud VA Medical Center in Minnesota was meeting federal security guidance. The OIG selected the St. Cloud VA Medical Center 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]
2. **Contingency planning controls** provide reasonable assurance that information resources are protected from unplanned interruptions, minimize risk, and provide

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

[2] NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of 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] 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.

for recovery of critical operations should interruptions occur.[6] Contingency planning also includes physical and environmental controls, such as fire protection, water damage protection, and emergency power and lighting.

3. **Security management controls** "establish a framework and continuous cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures."[7]
4. **Access controls** provide reasonable assurance that computer resources are restricted to authorized individuals and ensure users have the proper access and are uniquely identified. 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 St. Cloud VA Medical Center, 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, contingency planning, and access controls. The inspection team did not identify deficiencies with security management.

The St. Cloud VA Medical Center had 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]
- **Component inventories** are descriptive records of IT assets in an organization down to the system level.
- **Unauthorized software** is the prohibition of programs that are not approved on an organization's systems.[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] Government Accountability Office (GAO), *Federal Information System Controls Audit Manual (FISCAM)*, GAO-09-232G, February 2009.

[7] GAO, *FISCAM*.

[8] NIST Special Publication 800-53.

[9] NIST Special Publication 800-53.

the team identified operating systems that were no longer supported by the vendor and applications with missing security patches at the St. Cloud VA Medical Center. OIT scans for vulnerabilities routinely, randomly, and when new vulnerabilities are identified and reported. Although the inspection team and OIT used the same vulnerability-scanning tools, OIT did not detect all the vulnerabilities the inspection team found. For example, the OIG found 24 critical vulnerabilities that OIT did not detect. The team also identified 133 vulnerabilities—57 critical vulnerabilities on 15 percent of the devices and 76 high-risk vulnerabilities on 46 percent of the devices—which were not mitigated within the required 30-day or 60-day windows.[10] Although OIT is aware of many of the vulnerabilities, its plans of actions and milestones did not always list remediations.[11]

Despite VA's 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.

A complete, accurate, and up-to-date inventory is required to implement an effective information security program because it provides greater visibility into and control over these systems.[12] The inspection team identified inaccuracies in the component inventory at the St. Cloud VA Medical Center, despite OIT and VA's use of automated systems to maintain inventories of its information systems. The OIG discovered 13 devices that were not accounted for in any inventory and were operating in a network segment that was not reported. These devices present a risk to other network devices as the system function was not known by OIT.

The OIG identified 37 devices at the St. Cloud VA Medical Center that were using software not authorized by the OIT Technical Reference Model.[13] Although OIT scan results did identify the devices, the critical-risk vulnerability associated with the software was not addressed nor were the devices removed from the network. Additionally, the OIG identified 19 special-purpose systems using Windows XP, which has not been supported in over eight years and is prohibited by OIT. The devices were not accounted for on an inventory but were protected by network segmentation controls. Using unapproved software can present numerous risks, such as unknown vulnerabilities, unauthorized storage of personally identifiable information or protected health

[10] VA OIT, "OIT's Authorization Requirements: Standard Operating Procedures," version 1.38 dated July 12, 2022.

[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.

[12] GAO, *FISCAM*.

[13] The Technical Reference Model provides guidance, along with any known applicable constraints, on the permissible range of technologies or standards that a VA user, OIT administration support team, or project development team may select or shall use.

information, and a lack of other security controls. These discrepancies could lead to a loss of confidentiality, integrity, or availability of VA sensitive data.

The OIG identified one contingency planning control weakness: the emergency power shutoff for the data center was not tested. The emergency power shutoff bypasses power from the uninterruptible power supply. Routine testing ensures that the bypass will function properly during an emergency. This control primarily applies to the safety of personnel. However, it could protect equipment from damage caused by a malfunctioning uninterruptible power supply. Without routine testing, the emergency power shutoff could malfunction during an emergency and risk the safety of personnel and the integrity and availability of sensitive VA data.

The inspection team did not identify deficiencies in the controls implemented for security management.

During the inspection of the St. Cloud VA Medical Center, the team identified six deficiencies in the following access controls:

- Network segmentation controls regulate where information can travel within a system and between systems.[14]
- Video surveillance is the use of cameras installed at strategic locations and is required for data centers.[15]
- Physical access authorization is a list of individuals that have been approved to access the facility where a system resides.
- Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats.
- Visitor access records are used to account for persons other than regularly authorized personnel who have been granted access to sensitive areas.
- Environmental controls maintain and monitor temperature and humidity where communication equipment is located.[16]

[14] NIST Special Publication 800-53.

[15] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection" (standard operating procedure), March 23, 2022; NIST Special Publication 800-53.

[16] NIST Special Publication 800-53.

The St. Cloud VA Medical Center did not have network segmentation controls in place for several network segments that contained medical and special-purpose systems.[17] Network-connected medical devices and special-purpose systems are placed on isolated network segments for protection. Protection is provided through access control lists. However, the OIG identified five network segments containing 97 medical devices and special-purpose systems that did not have access control lists applied.[18] After the OIG identified the network segments, the area manager began the process of decommissioning and removing them. Without these types of network segmentation controls in place, any user can access these potentially vulnerable medical and special-purpose devices.

During the facility walk-through, the inspection team discovered that the St. Cloud VA Medical Center's video surveillance system for the data center was not operational. The facility only had one camera, and it had been unplugged and consequently not monitored. Although the facility does have surveillance cameras in the outlying communication rooms, the cameras did not have the capability to record video. Ineffective monitoring and recording of facility activities in and around the data center minimizes incident response capabilities of the security force in the event of compromised security controls. The lack of an effective incident response can undermine management's awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

Several communication rooms were missing access authorization memorandums. The memorandums are used by those with physical access to verify whether other individuals are authorized entry to communication rooms prior to granting access. Without the memorandums, personnel may gain access without authorization, which could lead to compromised infrastructure equipment. Further, without an updated authorization memorandum, authorized individuals may be prevented from gaining access to perform their duties.

The OIG also discovered that the physical access logs were not being reviewed as required by OIT policy.[19] The area manager is required to review access logs on a quarterly basis. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential

[17] According to OIT, many medical devices are certified through the Food and Drug Administration Premarket Review Process, which inhibits the ability to install agents and perform patching to reduce security risks. This means that VA does not modify medical devices without written permission from the device manufacturer. The networking of medical devices provides many benefits for information sharing and data analytics but also poses security risks to both the data and device integrity that must be addressed. 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 but are not limited to energy management systems, heating, ventilation, and air conditioning, temperature controls, building/facility access controls, and security camera systems.

[18] Access control lists are filters which manage the traffic that can access network segments for medical devices or special-purpose systems.

[19] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection."

threats.[20] The lack of log reviews increases the likelihood that potential threats are not identified in a timely manner, resulting in the potential loss of confidentiality, integrity, or access of VA sensitive data.

During the facility walk-through, the inspection team discovered missing visitor access records in two communication rooms. OIT policy requires visitor records to be located where the systems reside and be reviewed on a quarterly basis.[21] A lack of visitor access records could adversely impact management's ability to respond to security incidents resulting from those gaining unauthorized access to OIT infrastructure equipment.

During a walk-through, the inspection team discovered several communication rooms without temperature or humidity controls. Temperature extremes can cause reduced efficiency and a variety of problems, including premature aging and failure of equipment. High humidity can cause corrosion of internal components and degradation of electrical functions. Insufficient environmental controls can have a significant adverse impact on the availability of systems needed to support the organizational mission and business functions.[22]

What the OIG Recommended

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

1. Implement a more effective vulnerability management program to identify all critical security deficiencies on the network and to remediate vulnerabilities within policy timelines.
2. Implement a more effective inventory process to identify network devices.
3. Implement processes to prevent the use of prohibited software on agency devices.
4. Test the emergency power bypass during annual uninterruptible power supply testing and document results.
5. Ensure network segmentation controls are applied to all network segments with medical devices and special-purpose systems.
6. Ensure access authorization memorandums are present in all communication rooms.
7. Ensure that physical access for the data center and communication rooms are reviewed on a quarterly basis.

[20] Examples of suspicious activity are access outside of normal work hours, repeated access to areas not normally accessed, and access for unusual lengths of time or out of sequence.

[21] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection."

[22] NIST Special Publication 800-53.

8. Ensure visitor access records are available and reviewed on a quarterly basis.

The OIG made these recommendations to the assistant secretary because they are related to enterprise-wide IT security issues, similar to those identified during previous FISMA audits and IT security reviews. The OIG also made two recommendations to the St. Cloud VA Medical Center director, including ensuring video surveillance systems are operational and monitored for the data center and communication rooms with infrastructure equipment have adequate environmental controls.

VA Comments and OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 3 through 10. The assistant secretary did not concur with recommendation 2. Responsive action plans were submitted for the nine recommendations that received concurrences from the assistant secretary. The assistant secretary provided evidence to support actions addressing recommendations 6, 7, and 8 were completed, and the OIG considers these recommendations closed.

Regarding recommendation 2—to implement a more effective inventory process to identify network devices—the assistant secretary reported that both the trusted agent and the vulnerability scanning service team looked for the devices identified in the OIG's scan data but could not find them on the network or in any of the past 12 months of vulnerability scans. VA's position is that the devices were not identified properly during the OIG scan. The OIG evaluated OIT's scan results and agrees that the network segments and devices were not identified by OIT using their standard vulnerability management processes. The OIG was able to identify the devices by performing scans that did not rely on VA's standard network vulnerability identification methods. The OIG shared with OIT that the devices did not respond to network management protocols, which could have contributed to the lack of visibility. The OIG ran the scans again in May 2023 and confirmed that the devices were no longer on the network. The fact is that the OIG shared its results with VA so VA could see what was obtained by the OIG and seek to understand why OIT did not have similar results. It should be noted, however, that the OIG did not identify any critical or high-risk vulnerabilities on these devices and does not consider the security issues associated with this network segment to be a significant risk to VA systems or data. Consequently, the OIG considers this recommendation closed.

The assistant secretary concurred with recommendation 1 but stated that VA consistently maintains a management rate of 90 percent or greater for critical vulnerabilities across the enterprise. However, VA did not provide evidence that would allow the OIG to validate this assertion. In fact, OIT's own results that the OIG received April 12, 2023, indicated that 60 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 133 vulnerabilities (57 critical-risk vulnerabilities on 15 percent of the devices and 76 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 24 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. 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
SDIA	specialized device isolation architecture

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.[23] 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.[24]

In 2020, the OIG also started an IT security inspection program. These IT inspections assess whether VA facilities are meeting federal security requirements that protect systems and data from unauthorized access, use, modification, or destruction.[25] 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.[26] Appendix C provides more detail on the inspection scope and methodology.

The OIG conducted this inspection to determine whether the St. Cloud VA Medical Center in Minnesota was meeting federal security guidance. The OIG selected the St. Cloud VA Medical Center 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 St. Cloud VA Medical Center, other facilities across VA could benefit from reviewing this information and considering these recommendations.

Security Controls

Both the Office of Management and Budget and NIST provide criteria to evaluate security controls. These criteria provide requirements for establishing, implementing, operating,

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

[24] NIST Special Publication 800-53, rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020, includes updates as of December 10, 2020. Appendix A provides the recommendations from the fiscal year 2021 FISMA audit.

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

[26] 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.

monitoring, reviewing, maintaining, and improving a documented information security management system.[27]

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

The OIG IT 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.

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 security controls

Source: VA OIG analysis.

[27] 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.

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

Without these critical controls, VA's systems are at risk of unauthorized access or modifications. A cyberattack could destroy, disrupt access to, 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 is part of OIT's Office of Information Security. It 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.

The Office of Information Security; Cybersecurity Operations Center; Office of Development, Security, and Operations; and End User Operations are OIT offices relevant to the areas assessed at the St. Cloud VA Medical Center, as shown in figure 1.

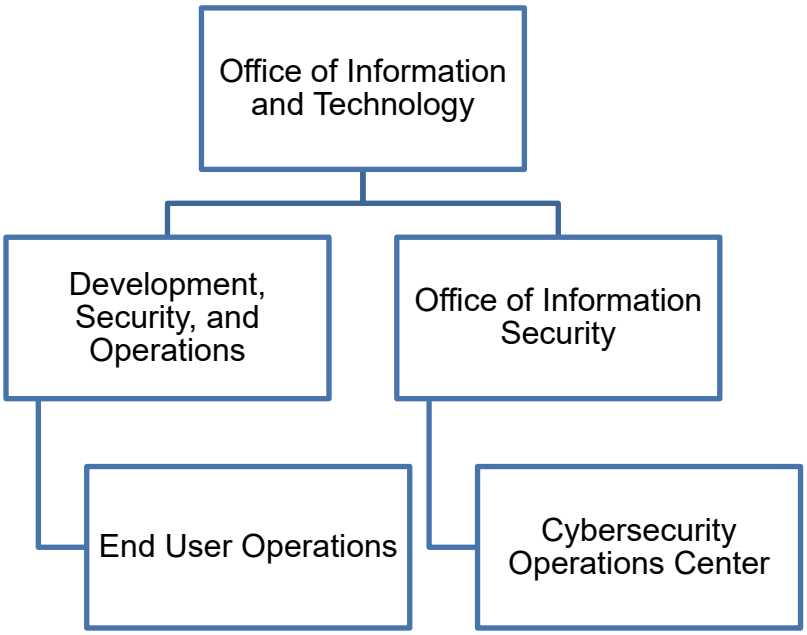

Figure 1. *Organizational structure of OIT entities relevant to this inspection.*
Source: VA OIG analysis.

According to VA, End User Operations provides on-site and remote support to IT customers across all VA administrations and special program offices, including direct support of approximately 400,000 VA employees and over 100,000 contractors as of February 2021, 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 and Office of Information Security personnel to the St. Cloud VA Medical Center, including system stewards who are responsible for managing system plans of action 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 the Office of Management and Budget and applicable NIST information security guidelines.[29] The fiscal year 2021 FISMA audit, conducted by CliftonLarsonAllen LLP, an independent public accounting firm, evaluated 50 major applications and general support systems hosted at 24 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 of which are repeated from the prior annual audit, indicating that VA continues to face significant challenges in complying with FISMA requirements.[31] 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.[32] According to GAO, as VA secured and modernized its information systems, it faced several security challenges, including

- effectively implementing information security controls,
- mitigating known vulnerabilities,
- establishing elements of its cybersecurity risk management program,

[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.

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

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

- identifying critical cybersecurity staffing needs, and
- managing IT supply chain risks.

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 system will remain at risk of disruption."[33]

St. Cloud VA Medical Center

The St. Cloud VA Medical Center in Minnesota is the main campus for the St. Cloud VA Health Care System. The St. Cloud VA Medical Center provides primary care and specialty health services including mental health, cardiology, dentistry, and women's health care (figure 2).

Figure 2. *St. Cloud VA Medical Center in Minnesota.*
Source: VA OIG inspection team, July 18, 2022.

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

Results and Recommendations

I. Configuration Management Controls

According to GAO's *Federal Information System Controls Audit Manual* (FISCAM), configuration management involves identifying and managing security features for all hardware, software, and firmware components of an information system at a given point and systematically controlling changes to that configuration during the system's life cycle. The inspection team reviewed and evaluated the 10 configuration management controls drawn from NIST criteria for VA-hosted systems at the St. Cloud VA Medical Center to determine whether 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.[34] VA should first establish an accurate component inventory to identify all devices on the network.[35] 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 Enterprise Vulnerability Management are assigned to the system personnel or the information security officer for action. This process helps to secure devices from attack.

Finding 1: The St. Cloud VA Medical Center Had Deficiencies in Four Configuration Management Controls

To assess configuration management controls, the inspection team interviewed the system owner, information system security officers, and system steward. The team reviewed local policies, procedures, and inventory lists and scanned the St. Cloud VA Medical Center'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 St. Cloud VA Medical Center's network to identify vulnerabilities.[36]

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, the OIG discovered 11 devices that were running an operating system that had not been supported by the vendor in over 18 years. These devices were not accounted for during the inventory process and were operating in network segments that were not identified by OIT's monitoring efforts. By not implementing more effective

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

[35] GAO, *FISCAM*.

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

configuration management controls, 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. Consistent with those findings, the team identified deficient controls at the St. Cloud VA Medical Center.[37] 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, and OIT conducts scans for vulnerabilities both routinely and randomly or when new vulnerabilities are identified and reported.

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 to provide evidence that the deficiencies have been mitigated.[38]

NIST assigns severity levels to vulnerabilities by using the Common Vulnerability Scoring System, a framework for communicating the characteristics of software vulnerabilities.[39] 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.[40]

---

[37] 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."

[38] 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.

[39] "Vulnerability Metrics" (web page), NIST National Vulnerability Database, accessed September 29, 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 September 29, 2022, https://www.first.org/cvss/v3-1/cvss-v31-specification_r1.pdf.

[40] "Security Controls Explorer, Department of Veterans Affairs Information Security Knowledge Service" (web page), Office of Information Security, accessed September 29, 2022, https://dvagov.sharepoint.com/sites/OITOIS/KnowledgeService/Lists/ControlCorrelationIdentifiers/DispForm.aspx?ID=1602. The Information Security Knowledge Service is the approved source for VA cybersecurity and privacy policies, procedures, processes, and guidance.

The inspection team compared OIT-provided network vulnerability scan results from the St. Cloud VA Medical Center against its own scans conducted from July 18 to July 22, 2022. The team and OIT used the same vulnerability-scanning tools. The team identified 133 vulnerabilities (57 critical-risk vulnerabilities on 15 percent of the devices and 76 high-risk vulnerabilities on 46 percent of the devices) that were not mitigated within the time frames established by OIT.[41] Moreover, OIT's security scans did not identify 24 critical-risk vulnerabilities the team detected.[42] Similarly, the prior FISMA audit found that "VA did not have a complete inventory of all vulnerabilities present on locally hosted systems."[43] The OIG identified critical and high-risk vulnerabilities on 48 percent of the devices at the St. Cloud VA Medical Center. Although OIT is aware of many of the vulnerabilities, its plans of action and milestones did not list specific vulnerabilities, strategies for remediation, or any resource constraints.[44] 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.[45] 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. Patch management is how OIT acquires, tests, applies, and monitors updates that address security and functionality problems. Although patch management is a critical process

[41] VA OIT, "OIT's Authorization Requirements: Standard Operating Procedures," version 1.38 dated July 12, 2022.

[42] The difference in scan results can be attributed to multiple factors. First, the scans are conducted at different points in time, so devices could have been added to or removed from the network between scans. Second, the OIG uses all available plug-ins for its vulnerability scanner, while OIT does not. According to OIT, they do not use all plug-ins because of potential impact on medical devices. Finally, the scans are conducted from different places in the network, which could be impacted by access controls.

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

[44] Plans of action 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 IT inspections, the OIG considers a vulnerability managed—even if it still exists—if the plan of action and milestones accurately identify the devices impacted and detail mitigation efforts, and the schedule of milestones is accurate and timely.

[45] NIST Special Publication 800-53.

used to help alleviate many of the challenges in securing systems from cyberattack, previous FISMA audits have repeatedly found deficiencies in this area.[46]

Component Inventory

Previous FISMA reports have repeatedly identified inventory deficiencies as a nationwide issue for VA. Component inventories are descriptive records of IT assets in an organization down to the system level. A complete, accurate, and up-to-date inventory is required to implement an effective information security program because it provides greater visibility into and control over these systems.[47] The inspection team identified inaccuracies in the component inventory at the St. Cloud VA Medical Center, despite OIT's and VA's use of automated systems to maintain inventories of its information systems. The OIG discovered 13 devices that were not accounted for during the inventory process and were operating in a network segment that was not identified by OIT's monitoring processes. The devices did not respond to network management protocols, which could have contributed to the lack of visibility. The OIG was able to identify the devices by performing scans that do not rely on network management protocols. The OIG shared with OIT the limitation of network management protocols to identify the devices on multiple occasions. These devices present a risk to other network devices as the system function was not known by OIT.

Unauthorized Software

The OIG identified 37 devices at the St. Cloud VA Medical Center that were not authorized by the OIT Technical Reference Model.[48] Previous FISMA reports have also identified unauthorized software as a nationwide issue for VA. According to NIST, organizations should only allow software that has been reviewed and approved; likewise, it should prohibit the use of programs on its systems that are not approved. OIT scan results did identify the devices. However, the critical-risk vulnerability associated with the software was not addressed nor were the devices removed from the network. Additionally, the OIG identified 19 special-purpose systems using Windows XP, which has not been supported by the vendor in over eight years and is prohibited by OIT.[49] These devices were not accounted for during the inventory process but

[46] VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2021*; VA OIG, *Federal Information Security Modernization Act Audit for Fiscal Year 2020*, Report No. 20-01927-104, April 29, 2021; 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.

[47] GAO, *FISCAM*.

[48] The Technical Reference Model provides guidance, along with any known applicable constraints, on the permissible range of technologies or standards that a VA user, OIT administration support team, or project development team may select or shall use.

[49] "VA Technical Reference Model v22.11, Windows Client" (web page), Architecture and Engineering Services, accessed September 8, 2022, https://www.oit.va.gov/Services/TRM/ToolPage.aspx?tid=31#.

were protected by network segmentation controls. Using unapproved software can present numerous risks such as unknown vulnerabilities, unauthorized storage of personally identifiable information or protected health information, and a lack of other security controls used in unapproved software. These discrepancies could lead to a loss of confidentiality, integrity, or availability of VA sensitive data.

Finding 1 Conclusion

The St. Cloud VA Medical Center 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 time frames established by OIT. Additionally, the component inventory at St. Cloud VA Medical Center was incomplete. Finally, there were several instances of unauthorized software on systems on the network. 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's mission.

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 identify all critical security deficiencies on the network and to remediate vulnerabilities within policy timelines.
2. Implement a more effective inventory process to identify network devices.
3. Implement processes to prevent the use of prohibited software on agency devices.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendations 1 and 3. In addressing recommendation 1, the assistant secretary reported that VA consistently maintains a 90 percent or greater management rate of critical vulnerabilities across the enterprise. The assistant secretary also stated VA OIT will follow up on remaining vulnerability items in a pending status to ensure those vulnerabilities are addressed in a timely manner and their status is updated, in compliance with policy. Regarding recommendation 3, the assistant secretary reported that a plan of action and milestones to upgrade devices running on an unapproved operating system had been submitted by the medical center to the authorizing official for approval.

The assistant secretary did not concur with recommendation 2, reporting that both the trusted agent and the vulnerability scanning service team looked for the devices identified in the OIG's

scan data but could not find them on the network nor in any of the past 12 months of vulnerability scans. VA's position is that the devices were not identified properly during the OIG scan.

OIG Response

The assistant secretary provided details on in-progress corrective actions for recommendations 1 and 3 that are responsive to the intent of the recommendations.

Despite concurring with recommendation 1, the assistant secretary reported that VA consistently maintains a management rate of 90 percent or greater for critical vulnerabilities across the enterprise. However, VA did not provide evidence that would allow the OIG to validate this assertion. In fact, OIT's own scan results that the OIG received April 12, 2023, showed that 60 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 of an effective vulnerability management and flaw remediation program. However, this statement runs counter to the OIG's results that showed 133 vulnerabilities (57 critical-risk vulnerabilities on 15 percent of the devices and 76 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 24 critical-risk vulnerabilities the OIG 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.

The secretary did not concur with recommendation 2, reporting that VA has implemented an effective inventory process to identify network devices. VA did not concur that the devices identified by the OIG team existed on the VA network because VA's trusted agent and vulnerability scanning service team looked for the devices but could not find them on the network.

The OIG agrees that OIT's standard vulnerability management processes did not identify the network segments and devices. The OIG was able to identify the devices by performing scans that do not rely on VA's standard network vulnerability identification methods. The OIG communicated with OIT that the devices did not respond to network management protocols, which could have contributed to the lack of visibility. The OIG ran the scans again in May 2023 and confirmed that the devices were no longer on the network. The fact is that the OIG shared its results with VA so it could see what was obtained by the OIG and seek to understand why OIT did not have similar results. It should be noted, however, that the OIG did not identify any critical or high-risk vulnerabilities on these devices and does not consider the security issues associated with this network segment to be a significant risk to VA systems or data.

Consequently, the OIG considers this recommendation closed. The full text of the response from the assistant secretary is included in appendix D.

II. Contingency Planning Controls

Contingency planning controls are important because if they 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. FISMA requires that each federal agency implement an information security program that includes "plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency."[50] Although often referred to as disaster recovery or contingency plans, controls to ensure service continuity should address the entire range of potential disruptions. 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 whether the St. Cloud VA Medical Center met federal guidance and VA requirements, the inspection team evaluated four contingency planning controls.

Finding 2: The St. Cloud VA Medical Center Had a Single Deficiency in Contingency Planning Controls

To assess contingency planning controls, the inspection team interviewed the area manager and information system security officer. The team also reviewed policies and procedures and conducted a walk-through of the facility to identify contingency planning weaknesses.

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 St. Cloud VA Medical Center had no critical information systems that would require an alternate processing facility. Instead, the enterprise manages the systems at regional data centers. However, the OIG did discover that the emergency power shutoff had not been tested.

Emergency Power Shutoff

The area manager at the St. Cloud VA Medical Center could not provide evidence that the emergency power shutoff for the data center had been tested. The emergency power shutoff bypasses power from the uninterruptible power supply and is primarily applied to facilities that contain concentrations of system resources, including data centers, mainframe computer rooms, server rooms, and areas with computer-controlled machinery. The standard operating procedure requires the emergency power shutoff to be inspected annually during uninterruptible power

[50] FISMA § 128.

supply testing.[51] Routine testing helps ensure that the bypass will function properly during an emergency. This control primarily applies to the safety of personnel. However, it could protect equipment from damage caused by a malfunctioning uninterruptible power supply. Without routine testing, the emergency power shutoff could malfunction during an emergency and could adversely impact the safety of personnel and the integrity and availability of sensitive VA data.

Finding 2 Conclusion

The emergency power shutoff was not tested at the St. Cloud VA Medical Center. Routine testing helps ensure that the bypass is functional during an emergency, thereby protecting personnel and equipment.

Recommendation 4

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

4. Test the emergency power bypass during annual uninterruptible power supply testing and document results.

VA Management Comments

The assistant secretary for information and technology and chief information officer concurred with recommendation 4. To address the recommendation, the assistant secretary reported that the St. Cloud VA Medical Center performed a complete test of the emergency power shutoff during the new data center construction turn over and found it to be functional. The chief of facilities management performed the test and added manual inspection of the emergency power shutoff as an action to be performed during testing of the uninterruptible power supply per the preventive maintenance schedule.

OIG Response

The assistant secretary reported that corrective actions for recommendation 4 were complete. The corrective actions are responsive to the recommendation. The OIG will close the recommendation when VA provides evidence demonstrating that testing has been performed. The full text of the response from the assistant secretary is included in appendix D.

[51] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection" (standard operating procedure), March 23, 2022; NIST Special Publication 800-53.

III. 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 five security management critical elements: establish a security management program, assess and validate risk, document and implement security control policies and procedures, monitor the effectiveness of the security program, and effectively remediate information security weaknesses.[52]

Finding 3: No Deficiencies Were Found in Security Management Controls

To assess security controls, the inspection team reviewed security management policies, standard operating procedures, and applicable VA policies. 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, information system security officer, and chief of facilities management. Finally, the team conducted a walk-through of the facility.

The OIG found that the St. Cloud VA Medical Center has a system security plan and comprehensive risk assessment that has been documented and approved by management. Each security control has documented security control policies and procedures in place that are signed and approved. For each security control weakness that has been identified, the St. Cloud VA Medical Center has developed and implemented a plan of action and milestones. The plans of action and milestones have been periodically reviewed and tested to determine whether they remain effective on a continuing basis. The team did not identify deficiencies in the St. Cloud VA Medical Center's security management controls. Accordingly, the OIG did not make any recommendations for improvement.

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

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. Identification, authentication, and authorization controls ensure that users have the proper access and access is restricted to authorized individuals. At the St. Cloud VA Medical Center, the inspection team reviewed three access control critical elements, each of which contain multiple controls.[53]

Finding 4: The St. Cloud VA Medical Center Had Deficiencies in Six Access Controls

To evaluate the St. Cloud VA Medical Center's access controls, the inspection team interviewed the area manager, information system security officer, biomedical engineering supervisor, database administrators, and local IT specialists; reviewed policies and procedures; and conducted walk-throughs of the facility.[54]

The OIG found these issues with access controls at the St. Cloud VA Medical Center:

- Network segmentation controls to isolate several medical devices and special-purpose systems were missing.
- Video surveillance for the data center was not operational.
- Several communication rooms lacked physical access authorization memorandums.
- Physical access logs were not reviewed.
- Two communication rooms did not have visitor access records.
- Several communication rooms containing infrastructure network equipment lacked environmental controls.

[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.

Network Segmentation Controls

The St. Cloud VA Medical Center did not have network segmentation controls in place for several network segments that contained medical and special-purpose systems.[55] Network segmentation controls regulate where information can travel within and between systems.[56]

Network-connected medical devices and special-purpose systems are placed on isolation network segments for protection. Protection is provided through access control lists.[57] However, during the inspection, the OIG identified five network segments containing 97 medical devices and special-purpose systems that did not have access control lists applied. After the OIG identified the network segments, the area manager began the process of decommissioning and removing them. Without effective network segmentation controls in place, any user can access these potentially vulnerable medical and special-purpose devices.

Video Surveillance

During the facility walk-through, the inspection team discovered that the St. Cloud VA Medical Center's video surveillance system for the data center was not operational. Video surveillance is the use of cameras installed at strategic locations and is required for data centers.[58] The facility only had one camera, and it had been unplugged and consequently not monitored. Although the facility does have surveillance cameras in the outlying communication rooms, they did not have the capability to record video. Ineffective monitoring and recording of facility activities that support information systems minimizes incident response capabilities in the event of a security compromise. The lack of an effective incident response can undermine management's awareness of security vulnerabilities that could hinder the operation of mission-critical systems.

[55] According to OIT, many medical devices are certified through the Food and Drug Administration Premarket Review Process, which inhibits the ability to install agents and perform patching to reduce security risks. This means that VA does not modify medical devices without written permission from the device manufacturer. The networking of medical devices provides many benefits for information sharing and data analytics, but also poses security risks to both the data and device integrity that must be addressed. 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, but are not limited to, energy management systems, heating, ventilation, air conditioning, temperature controls, building/facility access controls, and security camera systems.

[56] NIST Special Publication 800-53.

[57] Access control lists are filters which manage the traffic that can access network segments for medical devices or special-purpose systems.

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

Physical Access Authorization

During the facility walk-through, the inspection team discovered several communication rooms were missing access authorization memorandums. The memorandums are used by those with physical access to verify whether other individuals are authorized entry to communication rooms prior to granting access. Without the memorandums, personnel may gain access without authorization, which could lead to compromised infrastructure equipment. Further, without an updated authorization memorandum, authorized individuals may be prevented from gaining access to perform their duties.

Monitoring Physical Access

The OIG discovered that the physical access logs were not being reviewed as required by OIT policy.[59] The St. Cloud VA Medical Center uses a centralized system to control physical access to the data center and communication rooms. The system also maintains access logs to those rooms. The area manager is required to review access logs on a quarterly basis. Reviewing physical access logs can help identify suspicious activity, anomalous events, or potential threats.[60] The lack of log reviews increases the likelihood that potential threats are not identified, resulting in the loss of confidentiality of, integrity of, or access to VA sensitive data.

Visitor Access Records

During the facility walk-through, the inspection team discovered missing visitor access records in two communication rooms. Visitor access records are used to account for persons other than regularly authorized personnel who have been granted access to sensitive areas.[61] OIT policy requires visitor records to be located where the systems reside and be reviewed on a quarterly basis.[62] A lack of visitor access records could adversely impact management's ability to respond to security incidents resulting from those gaining unauthorized access to OIT infrastructure equipment.

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

[59] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection."

[60] Examples of suspicious activity are access outside of normal work hours, repeated access to areas not normally accessed, or access for unusual lengths of time or that is out of sequence.

[61] On occasion, persons other than regularly authorized personnel, such as employees from another facility, maintenance personnel, or contractors, may be granted access to sensitive areas or facilities. No visitors should be granted unrestricted access and should be escorted.

[62] Development, Security, and Operations, End User Operations, "Physical and Environmental Protection."

humidity where communication equipment is located.[63] Equipment was installed in communication rooms without sufficient environmental controls. Temperature extremes can cause reduced efficiency and a variety of 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 have a significant adverse impact on the availability of systems that are needed to support the organizational mission and business functions.

Finding 4 Conclusion

The St. Cloud VA Medical Center did not have network segmentation controls for some medical devices and special-purpose systems to protect them from unauthorized access. Additionally, the video surveillance camera in the data center was not operational or monitored. Physical access authorizations were not present in several communication rooms. The area manager is not monitoring access to the data center or communication rooms. Visitor access records were not present in two communication rooms. Finally, several communication rooms did not have temperature or humidity controls, which could have a significant adverse impact on the availability of systems. Unless the medical center takes corrective actions, it risks unauthorized access to critical network resources, inability to respond effectively to incidents, and loss of personally identifiable information.

Recommendations 5–10

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.
6. Ensure access authorization memorandums are present in all communication rooms.
7. Ensure that physical access for the data center and communication rooms are reviewed on a quarterly basis.
8. Ensure visitor access records are available and reviewed on a quarterly basis.

The OIG made the following recommendation to the St. Cloud VA Medical Center director:

9. Ensure video surveillance systems are operational and monitored for the data center.
10. Ensure communication rooms with infrastructure equipment have adequate environmental controls.

[63] NIST Special Publication 800-53.

VA Management Comments

The assistant secretary for information and technology and chief information officer responded to all six recommendations, including those addressed to the facility director, and concurred with all the recommendations. To address recommendation 5, he reported that VA decommissioned the identified segments or confirmed that they are not applicable to the specialized device isolation architecture (SDIA) requirements, and other segments do not meet the requirements for SDIA. To address recommendation 6, the assistant secretary reported that OIT staff at St. Cloud VA Medical Center were briefed on the requirement and the facility updated and verified access authorization memorandums in accordance with NIST guidance and VA policy. The assistant secretary requested closure of recommendation 6. To address recommendation 7, the assistant secretary reported that a new physical access control system was installed in fiscal year 2022. Location designators were reviewed with facilities management and verified for accuracy. Facilities management sends electronic logs to OIT for review. The assistant secretary requested closure of recommendation 7. To address recommendation 8, he reported that the St. Cloud VA Medical Center posted, reviewed, and remediated all missing visitor access records in the communication rooms. The assistant secretary requested closure of recommendation 8. To address recommendation 9, the assistant secretary reported that a project to upgrade the surveillance and duress alarms for the medical center is scheduled for funding and will include surveillance for the data center. Finally, the assistant secretary reported that VA awarded the Electronic Health Record Modernization Infrastructure project, which will add temperature and humidity monitoring in OIT telecommunication rooms.

OIG Response

The assistant secretary for information and technology and chief information officer concurred with recommendations 5 through 10. Actions to address recommendations 5, 9, and 10 were in progress, and he provided estimated completion dates. The planned corrective actions are responsive to the intent of the recommendations. The OIG acknowledges that some physical and environmental security measures will not be remediated until work related to the Electronic Health Record Modernization project is completed at the facility. 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 secretary provided evidence to support recommendations 6, 7, and 8 have been addressed, and the OIG considers the recommendations closed. 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. Of these, 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 St. Cloud VA Medical Center. 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

The GAO developed FISCAM to provide auditors and information system control specialists 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.[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 whether a system is functioning as intended, as well as to determine whether 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 are computer programs and data stored in hardware, typically in read-only memory, that cannot be written or modified during the execution of the program.

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

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

FISCAM identifies the following critical elements for contingency planning:

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

FISCAM has seven critical elements for security management:

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

- **Document and implement security control policies and procedures** that appropriately address general and application controls and ensure users can be held accountable for their actions. These controls, which are more general at the entity-wide level and more specific at the system level, should be approved by 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.[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.
- **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.

[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 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

The stated goals of 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 program to determine its effectiveness. Inspectors general or independent external auditors must

[66] FISMA § 128.

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 June 2022 through January 2023. 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 St. Cloud VA Medical Center's 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 team determined that internal controls were significant to the inspection objectives. The overall scope of IT 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 FISCAM as a template to plan for inspections. When planning for this review, the team identified potential information system controls that would significantly impact the review. Specifically, the team used FISCAM appendix II as a guide to help develop evidence requests and a base set of interview questions for the St. Cloud VA Medical Center 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 their 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, some controls overlap and are reviewed in both assessments due to redundant roles and responsibilities among VA's local, regional, and national facilities and offices.

The team determined that all controls applicable to the St. Cloud VA Medical Center aligned with the control activities category. Control activities are the actions management establishes

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 within the context of the inspection objectives, could occur during this review. 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 team used network scanning tools to generate computer-processed data. 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 time frame requested. The 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: March 12, 2023

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

Subj: Office of Inspection General Draft Report, Inspection of Information Security at the St. Cloud VA Medical Center (VIEWS 09380014)

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 Security at the St. Cloud VA Medical Center (Project Number 2022-02961-AE-0119).

2. OIT is submitting 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 Security at the St. Cloud VA Medical Center,

Project Number OIG-2022-02961-AE-0119

(VIEWS 09380014)

Recommendation 1: Implement a more effective vulnerability management program to identify all critical security deficiencies on the network and to remediate vulnerabilities within policy timelines.

Comments: Concur.

The Department of Veterans Affairs (VA) Office of Information and Technology (OIT) concurs. OIT'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 VA and industry standards. VA consistently maintains a management rate of 90% or greater for critical vulnerabilities across the enterprise. VA's latest analysis of the Office of Inspector General (OIG) scan results for the St. Cloud VA Medical Center displays 98.96% policy compliance. VA OIT will follow-up on remaining vulnerability items in a pending status to ensure they are addressed in a timely manner, and their status updated, in compliance with policy.

Expected Completion Date: May 1, 2023.

Recommendation 2: Implement a more effective inventory process to identify network devices.

Comments: Non-concur. VA has implemented an effective inventory process to identify network devices. VA non-concurs that these devices existed on the VA network. Both the Trusted Agent and our Vulnerability Scanning Service team looked for the devices identified in OIG's scan data but could not find them on the network or in any of the past 12 months of vulnerability scans. It is VA's position that the devices were not identified properly during the OIG scan with the result being misidentification.

Expected Completion Date: Completed.

VA OIT requests closure of recommendation 2.

Recommendation 3: Implement processes to prevent the use of prohibited software on agency devices.

Comments: Concur.

The St. Cloud VA Medical Center submitted a Plan of Action and Milestones (POAM) to upgrade devices running on an unapproved operating system and sent the POAM to the authorizing official for approval.

Expected Completion Date: September 30, 2023.

Recommendation 4: Test the emergency power bypass during annual uninterruptible power supply testing and document results.

Comments: Concur.

The St. Cloud VA Medical Center performed a complete test of emergency power shutoff during the new data center construction turn over and found it to be functional. The chief of facilities management

performed a test and added manual inspection of the emergency power shutoff as an action to be performed during testing of the uninterruptible power supply per the preventive maintenance schedule.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 4.

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

Comments: Concur.

The St. Cloud VA Medical Center agrees that access control lists were not applied to the identified segments. VA decommissioned the identified segments or confirmed they are not applicable to the specialized device isolation architecture (SDIA) requirements, and other segments do not meet the requirements for SDIA.

Expected Completion Date: June 1, 2023.

Recommendation 6: Ensure access authorization memorandums are present in all communication rooms.

Comments: Concur.

The St. Cloud VA Medical Center OIT staff was briefed on the requirement. The facility updated and verified the access authorizations memorandum in accordance with National Institute of Standards and Technology guidance and VA policy.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 6.

Recommendation 7: Ensure that physical access for the datacenter and communication rooms are reviewed on a quarterly basis.

Comments: Concur.

The St. Cloud VA Medical Center installed a new physical access control system in fiscal year 2022. Location designators were reviewed with facilities management and verified for accuracy. Facilities management sends electronic logs to OIT for review.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 7.

Recommendation 8: Ensure visitor access records are available and reviewed on a quarterly basis.

Comments: Concur.

The St. Cloud VA Medical Center posted, reviewed and remediated all missing visitor access records in the communication rooms.

Expected Completion Date: Completed.

VA OIT requests closure of Recommendation 8.

Recommendation 9: Ensure video surveillance systems are operational and monitored for the datacenter.

Comments: Concur.

The St. Cloud VA Medical Center project to upgrade surveillance and duress alarms is scheduled for funding and will include surveillance for the data center.

Expected Completion Date: September 30, 2024.

Recommendation 10: Ensure communication rooms with infrastructure equipment have adequate environmental controls.

Comments: Concur.

VA awarded the Electronic Health Record Modernization Infrastructure project, which will add temperature and humidity monitoring in OIT telecommunication rooms.

Expected Completion Date: June 30, 2025.

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 Clifford Stoddard Bill Warhop

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, St. Cloud VA Medical Center

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Accountability
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
US Senate: Amy Klobuchar, Tina Smith
US House of Representatives: Angie Craig, Tom Emmer, Brad Finstad, Michelle Fischbach, Betty McCollum, Ilhan Omar, Dean Phillips, Pete Stauber

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