VA Office of Inspector General

OFFICE OF AUDITS AND EVALUATIONS

Department of Veterans Affairs

Review of Alleged Funding and Security Issues of the Veterans Services Adaptable Network at VA Medical Center Orlando, FL

January 31, 2018
15-03059-384

ACRONYMS

FISMA	Federal Information Security Modernization Act
IT	Information technology
OGC	Office of General Counsel
OIG	Office of Inspector General
OI&T	Office of Information and Technology
VA	Department of Veterans Affairs
VAMC	Veterans Affairs Medical Center
VSAN	Veterans Services Adaptable Network

EXECUTIVE SUMMARY

Why We Did This Audit

In March 2015, the VA Office of Inspector General received a Hotline complaint about development of the Veterans Services Adaptable Network (VSAN) at the Orlando Veterans Affairs Medical Center (VAMC). The complaint stated that VSAN development efforts were not coordinated with the Office of Information and Technology (OI&T) and that project funding was inappropriately coming from medical services appropriations rather than information technology (IT) funding.

What We Found

The OIG substantiated that the VSAN deployment was not fully coordinated with OI&T to ensure it met VA security requirements. Specifically, the Orlando VAMC and OI&T did not perform a security risk assessment or implement security controls to segregate VSAN from VA's network. The OIG did not substantiate that the Orlando VAMC inappropriately used $5.2 million in medical appropriations funds to purchase IT hardware, software, and installation services in support of the VSAN system. In 2010, the Office of General Counsel (OGC) reviewed the initial $1.7 million procurement and determined that use of the medical services appropriation was proper for the initial VSAN deployment. In July 2017, the OGC reviewed the subsequent $3.5 million procurements to determine whether other medical appropriations could be used to fund additional VSAN IT enhancements beyond the original scope of the project, which was patient Wi-Fi access. The OGC concluded that because the additional $3.5 million of IT procurements were used solely for the patient Wi-Fi network, the expenditure was justified. The OIG accepts OGC's rationale supporting the use of medical appropriations for these procurements.

The VSAN deployment was not fully coordinated because local OI&T staff did not exercise effective oversight due to completing priorities and resources. OI&T's lack of effective VSAN oversight posed unnecessary risks to VA's networks that could have resulted in unauthorized access to other VA systems.

What We Recommended

The OIG recommended that the Executive in Charge for the Office of the Under Secretary for Health, in conjunction with the Executive in Charge for the Office of Information Technology, ensure that all guest Wi-Fi access networks are appropriately secured in accordance with VA policy.

Management Comments

The Executive in Charge for the Office of the Under Secretary for Health and the Executive in Charge for the Office of Information and Technology concurred with the recommendation and requested closure of this recommendation based on actions taken.

LARRY M. REINKEMEYER
Assistant Inspector General
for Audits and Evaluations

TABLE OF CONTENTS

Introduction 1

Results and Recommendations 2

Finding 1 Controls to Ensure Proper Coordination of New IT Systems Needed Improvement 2

Recommendation 5

Appendix A Scope and Methodology 6

Appendix B Office of the Assistant Secretary for Information and Technology Comments 7

Appendix C Office of the Under Secretary for Health Comments 9

Appendix D OIG Contact and Staff Acknowledgments 10

Appendix E Report Distribution 11

INTRODUCTION

Allegations

In March 2015, the VA Office of Inspector General (OIG) received a Hotline complaint stating that the Orlando Veterans Affairs Medical Center (VAMC) at Lake Nona, FL, was developing the Veterans Services Adaptable Network (VSAN) without coordinating its efforts with the Office of Information & Technology (OI&T) or obtaining the appropriate information technology (IT) funding for the projects.

Background

VSAN is an enterprise network that is controlled and administered by Veterans Health Administration (VHA) and is completely separate from OI&T systems hosted on VA's internal network. Initially a local guest Wi-Fi network, the VSAN goal was to support the department's "MyVA" initiative[1] by expanding local capabilities and replicating them across facilities to improve customer service. The VSAN will provide a unified veteran experience across the entire organization and deliver standardized guest internet access at all VHA facilities.

The Orlando VAMC is co-located in Lake Nona, FL, with the University of Central Florida College of Medicine, the University of Florida Academic and Research Center, and Nemours Children's Hospital. The new 1.2 million-square-foot facility cost approximately $600 million to construct. The facility contains administrative and support services, a multispecialty outpatient clinic, 134 inpatient beds, a 120-bed community living center, and a 60-bed domiciliary.

Prior OIG Audits and Reviews

The *Review of Alleged Misuse of VA Funds To Develop the Health Care Claims Processing System* (Report No. 14-00730-126, March 2, 2015) reported that VHA's Chief Business Office violated appropriations law by improperly obligating $92.5 million of Medical Support and Compliance appropriations to finance the development of the Health Care Claims Processing System (HCPS). In August 2016, VA reported an Anti-Deficiency Act violation because the IT Systems account—the specific and exclusive appropriation available for developing, enhancing, and modernizing IT systems used in the administration of VHA activities—was not used in HCPS development as required. VA stated this misspending occurred because VHA did not have an oversight mechanism in place to ensure the Chief Business Office complied with VA's financial policies and Federal appropriation laws when obligating and spending appropriations. Prior Federal Information Security Modernization Act (FISMA) audits also identified weaknesses related to system risk assessments and implementation of system security controls.

[1] The goal of the "MyVA" initiative is to enhance the Veterans' experience and position VA to be a world-class service provider for Veterans.

RESULTS AND RECOMMENDATIONS

Finding 1 Controls To Ensure Proper Coordination of New IT Systems Needed Improvement

The OIG substantiated that the VSAN deployment was not fully coordinated with OI&T to ensure it met VA security requirements. Specifically, the OIG noted that the Orlando VAMC and OI&T did not perform a system security risk assessment or implement security controls to segregate VSAN from VA's internal network.

The OIG did not substantiate that the Orlando VAMC inappropriately used $5.2 million in medical appropriations funds to purchase IT hardware, software, and installation services in support of the VSAN system.

In 2010, VA's Office of General Counsel (OGC) reviewed the initial $1.7 million procurement and determined that it was proper to use medical appropriations for the initial VSAN deployment of guest Wi-Fi services. At the OIG's request in July 2017, OGC reviewed the subsequent $3.5 million of procurements to determine whether other medical appropriations could fund VSAN IT enhancements beyond the original scope of the project.[2] The intent of these upgrades, purchased in 2014 and 2015, was to allow the VSAN to host various VA industrial control systems like closed circuit television, physical access controls systems, and energy management systems. The OGC concluded that it was proper to use medical services funds for the additional $3.5 million of IT procurements, as those costs directly supported providing patient Wi-Fi services. The OIG accepts OGC's rationale supporting the use of medical appropriations for these procurements.

The VSAN deployment was also not fully coordinated because local OI&T staff did not exercise effective oversight. Due to competing priorities and resources, staff did not ensure the VSAN evaluated security controls in accordance with VA's security requirements. OI&T's lack of effective VSAN oversight posed unnecessary risks to VA's networks that could have resulted in unauthorized access to other VA systems.

Criteria

In May 2015, OI&T issued a memo on network-connected industrial control systems and air-gapped networks.[3] The memo detailed security requirements

[2] $3.5 million attributed to VHA provided response for VSAN expenditures in FY14 and FY15 with total VSAN expenditures identified by VHA as $5.2 million.
[3] Air gap is a network security measure employed to ensure that a secure computer network is physically isolated from unsecured networks.

for any non-medical systems operating in air-gapped networks connected to the internet.

Some Allegations Substantiated

The OIG substantiated that the VSAN deployment was not fully coordinated with OI&T to ensure it met VA security requirements. Specifically, the Orlando VAMC, in coordination with OI&T, did not perform a system risk assessment or security control testing to ensure implementation of appropriate VSAN security controls and segregation between VSAN and the VA's internal network. Specific requirements for such systems include performing an assessment for security risks utilizing Federal Information Processing Standards 199 and implementing VA information security controls as specified by the risk impact level. During the OIG's June 2015 and September 2016 site visits, the Orlando VAMC stated that it did not perform a risk assessment and management did not provide any evidence that VSAN was meeting these security requirements.

The OIG did not substantiate that the Orlando VAMC inappropriately used $5.2 million in medical appropriations funds to purchase IT hardware, software, and installation services in support of the VSAN IT system. In 2011, Orlando VAMC personnel purchased $1.7 million of IT hardware and installation services with Medical Services appropriations to deploy a wireless internet guest network, later named VSAN. The OGC reviewed this procurement and determined that it was proper to use medical appropriations for the initial VSAN deployment because providing internet access was a necessary expense when providing patient care.

In 2014 and 2015, the Orlando VAMC purchased an additional $3.5 million of IT networking, security equipment, and installation services to expand VSAN services using a combination of Medical Facilities, Medical Services, and Medical Support and Compliance appropriations.[4] The additional procurements were beyond the original scope of the project, as the intent of subsequent VSAN service upgrades was to host various VA industrial control systems like closed circuit television, physical access controls systems, and other building control systems. In August 2016, the OIG recommended that VA seek OGC review of the additional $3.5 million of IT procurements to determine whether the use of medical appropriations was proper to purchase the VSAN enhancements. In July 2017, OGC reviewed the subsequent $3.5 million procurements and concluded that using Medical Services funds was proper, as those costs directly supported providing patient Wi-Fi services.

To determine the authorized purposes of an appropriation, the Government Accountability Office instructs agencies to first look at the language of an

[4] $3.5 million attributed to VHA-provided response for VSAN expenditures in FY14 and FY15, with total VSAN expenditures identified by VHA as $5.2 million.

appropriations act and its legislative history. When an agency has a specific appropriation for an item, it cannot use a more general appropriation to pay for that item, nor can it augment that account with funds from other appropriations accounts without statutory authority. However, when an agency has two appropriations available for the same purpose, it must select which one to use and must continue to use that appropriation for that purpose unless the agency informs Congress of its intent to change appropriations during the annual budget process. This is commonly referred to as the "pick and stick rule." For patient expenses like patient Wi-Fi, where both medical and IT funds are available for expenditure, the OGC's opinion establishes that VA selected medical funds in the Medical Services account for patient Wi-Fi because it was for therapeutic purposes. Having selected this appropriation, VA must ensure that future patient Wi-Fi expenditure is consistent.

The VSAN deployment was not fully coordinated with OI&T because local information security officers and the facility Chief Information Officer did not exercise effective oversight to ensure formal assessment of the VSAN security risks. More specifically, the responsible information security officers did not ensure maintenance of an appropriate operational security posture by effectively monitoring the system control environment. In addition, the OIG noted that the evaluation of VSAN information security controls was not in accordance with VA's security requirements. This occurred because management did not allocate resources to ensure performance of a security risk assessment of VSAN controls. Proper risk management activities would have ensured VSAN was authorized to operate within the VA and that it deployed, maintained, and operated in accordance with established security controls.

What Resulted

OI&T's lack of effective project oversight during the implementation of the VSAN projects posed unnecessary risks to VA's networks and could have potentially allowed unauthorized access to other VA systems. Without a formal security assessment, VA could not confirm implementation of VSAN security controls in accordance with information security requirements or effective protection of other VA systems from unauthorized access, modification, or disclosure.

Conclusion

The OIG found that the VSAN procurement and deployment was not fully coordinated with OI&T, resulting in poor oversight of the VSAN project and inadequate implementation of appropriate system security controls. This lack of coordination placed the project at unnecessary risk of mismanagement that could have adversely affected other VA systems. Prior FISMA audits also identified weaknesses associated with system risk assessments and implementation of system security controls. The intent of the VSAN model was to support the department's "MyVA" initiative by providing a unified veteran experience across the entire organization and delivering standardized guest internet access at all VHA facilities and clinics. It is imperative that

VHA coordinate the development and implementation of any future VSAN projects at other medical facilities to ensure adequate protection of veterans' sensitive data. Furthermore, it is critical that OI&T provide proper oversight of all VSAN implementations to ensure implementation of appropriate security controls and to segregate such networks from the enterprise.

Recommendation

1. The OIG recommended the executive in charge for the Office of the Under Secretary for Health, in conjunction with the executive in charge for the Office of Information and Technology, ensure that all guest internet access networks, external air-gapped networks, and industrial control systems are appropriately segregated from VA networks and meet the department's information security requirements.

Management Comments

The executive in charge for the Office of the Under Secretary for Health and the executive in charge for the Office of Information and Technology concurred with the finding and recommendation and have requested closure of the report recommendation. Specifically, management stated all Industrial Control Systems were removed from the VSAN in Orlando. In addition, management stated that there is not a requirement for a full risk assessment because there are no Industrial Control Systems on the VSAN; the system only needs an air gap Memorandum of Understanding. Memorandums of Understanding are now in place for all network-based systems at each facility to ensure they are air-gapped from VA networks. VHA will continue to work with OI&T to ensure the air gap Memorandum of Understanding process is used and to ensure no Industrial Control Systems are connected to a public internet connection.

OIG Response

The OIG will monitor VHA's and the Office of Information and Technology's corrective action plans to ensure that the air gap process described above is fully implemented at all VA facilities. Based on the information provided, the OIG considers Recommendation 1 closed at this time.

Appendix A Scope and Methodology

Scope

The OIG conducted its review from June 2015 through July 2017. The review evaluated the merits of a VA Hotline allegation stating that the Orlando VAMC at Lake Nona, FL, was developing the VSAN without coordinating its efforts with the VA OI&T or obtaining the appropriate Information Technology funding for the projects.

Methodology

In June 2015, the OIG performed an onsite review at the Orlando VAMC. In September 2016, the OIG performed a subsequent onsite review to determine whether appropriate segregation existed between VSAN and VA's internal network. The OIG interviewed the Chief Technology Officer, the technical project manager, the facility Chief Information Officer, and the facility information security officer. The OIG reviewed network diagrams, technical overviews, appropriations law, Executive Decision Memorandums for the Use of Information Technology Systems Appropriation, and Veterans Guest Internet Access Initiatives. The OIG also reviewed the policy memorandum for VA's Use of NASA Solutions for Enterprise Wide Procurement Contracts, VA's Project Management Accountability System Directive, the Program Manager & Project Managers PMAS/ProPath Execution Handbook, and the Information Technology Acquisition Request System user manual. In addition, the OIG analyzed purchase and obligation documentation and reviewed memos and emails from the Veterans Health Administration and OI&T.

Data Reliability

The OIG did not request computer-processed data for this review. The OIG evaluated the sufficiency and accuracy of information provided in connection with personal testimony, staff email correspondence, and direct observation.

Government Standards

We conducted this review in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspection and Evaluation.* The evidence obtained provides a reasonable basis for our findings and conclusions based on the review objective.

Appendix B Management Comments – Office of the Assistant Secretary for Information and Technology

Department of Veterans Affairs Memorandum

Date: October 18, 2017

From: Acting Assistant Secretary for OI&T, Chief Information Officer (005)

Subj: OIG Draft Report *"Review of Alleged Funding and Security Issues of the VSAN at VAMC Orlando FL"*

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

1. Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, Review of Alleged Funding and Security Issues of the Veterans Services Adaptable Network at VA Medical Center Orlando, FL. The Office of Information and Technology (OI&T) and Veterans Health Administration (VHA) concur with the recommendation and provide the attached comments. The recommendation has been implemented and we request closure.

2. Subsequent to Orlando's implementation of Patient WiFi in May 2015, OI&T implemented several security measures. OI&T released a memo outlining updated security requirements for Network Connected Industrial Control Systems (ICS) and Air-Gapped Networks. The memo provides additional security requirements and process guidance specifically for network-connected ICS and other special purpose non-medical systems and devices. Any ICS or other special purpose system or devices that are proposed for installation within a device isolation architecture (DIA) Virtual Local Area Network (VLAN) must be assessed for security risks and receive formal approval through the assessment and authorization process before connection to the VA Network.

3. In addition, Memorandums of Understanding (MOU's) are in place for all network-based systems at each facility to ensure they are air-gapped from VA OI&T networks and separate from Veteran Guest Internet Access (VGIA). Annual reviews are conducted by the facility, OI&T and the Information Security Officer. Compliance is also ensured through external audits, such as the Federal Information Security Management Act (FISMA) review. In 2016, Orlando underwent a FISMA review and a facility-wide OI&T security controls review, which did not find any issues with VGIA.

4. If you have any questions, contact me at (202) 461-6910 or free free to contact Susan McHugh-Polley, Deputy Assistant Secretary for IT Operations and Services, at (727) 502-1379.

(original signed by:)

SCOTT BLACKBURN

Attachments

Cc: Executive in Charge for the Office of the Under Secretary for Health (10)

Attachment

Office of Information and Technology (OI&T)
Comments on OIG Draft Report:
"Review of Alleged Funding and Security Issues of the VSAN at VAMC Orlando, FL"

OIG Recommendation 1: We recommended the Executive in Charge for the Office of the Under Secretary for Health, in conjunction with the Executive in Charge for the Office of Information and Technology, ensure that all guest internet access networks, external air gapped networks, and industrial control systems are appropriately segregated from VA networks and meet the Department's information security requirements.

OIT Comments: Concur. The Veterans Health Administration (VHA) and Office of Information & Technology (OI&T) resolved this recommendation. All Industrial Control Systems (ICS) were removed from the Veterans Services Adaptable Network (VSAN) by September 2015 in Orlando. Furthermore, the VSAN was never interconnected to the VA network. The risk was only to the ICS on the VSAN at the time of the investigation. Given there are no ICS systems on the VSAN, now known as Veteran Guest Internet Access (VGIA), there is not a requirement for a full risk assessment; only an airgap Memorandum of Understanding (MOU). The attached airgap MOU and updated airgap MOU support the request to close this recommendation.

In addition, MOU's are in place for all network-based systems at each facility to ensure they are air-gapped from VA OI&T networks and separate from VGIA. VHA nationally will continue to work with OI&T to ensure the airgap MOU process is used and will continue to ensure no ICS systems are connected to a public internet connection as specified in the memo dated May of 2015 also attached.

Status: Completed Target Completion Date: Recommend Closing

For accessibility, the format of the original memo has been modified to fit in this document.

Appendix C Management's Comments – Office of the Under Secretary for Health

Department of Veterans Affairs Memorandum

Date: October 13, 2017

From: Executive in Charge, Office of the Under Secretary for Health

Subj: OIG Draft Report—Review of Alleged Funding and Security Issues of the Veterans Services Adaptable Network at VA Medical Center Orlando, FL (VAIQ 7832089)

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

1. Thank you for the opportunity to review the Office of Inspector General (OIG) draft report, Review of Alleged Funding and Security Issues of the Veterans Services Adaptable Network at VA Medical Center Orlando, FL. The Veterans Health Administration (VHA) concurs with the draft report as written and concurs with the VA Office of Information and Technology's response.

2. If you have any questions, please email Karen Rasmussen, M.D., Director, Management Review Service at VHA10E1DMRSAction@va.gov.

(Original signed by:)

Carolyn M. Clancy, M.D.

Executive in Charge – Office of the Under Secretary for Health

Attachments

For accessibility, the format of the original memo has been modified to fit in this document.

Appendix D OIG Contact and Staff Acknowledgments

Contact	For more information about this report, please contact the Office of Inspector General at (202) 461-4720.
Acknowledgments	Michael Bowman Jerry Charles Rich Wright

Appendix E Report Distribution

VA Distribution

Office of the Secretary
Veterans Health Administration
Veterans Benefits Administration
National Cemetery Administration
Assistant Secretaries
Office of General Counsel
Office of Acquisition, Logistics, and Construction
Board of Veterans' Appeals

Non-VA Distribution

House Committee on Veterans' Affairs
House Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
House Committee on Oversight and Government Reform
Senate Committee on Veterans' Affairs
Senate Appropriations Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Senate Committee on Homeland Security and Governmental Affairs
National Veterans Service Organizations
Government Accountability Office
Office of Management and Budget
U.S. Senate: Bill Nelson, Marco Rubio
U.S. House of Representatives: Gus M. Bilirakis, Vern Buchanan, Kathy Castor, Charlie Crist, Carlos Curbelo, Val Demings, Ron DeSantis, Ted Deutch, Mario Diaz Balart, Neal Dunn, Lois Frankel, Matt Gaetz, Alcee L. Hastings, Al Lawson, Brian Mast, Stephanie Murphy, Bill Posey, Francis Rooney, Tom Rooney, Ileana Ros-Lehtinen, Dennis Ross, John Rutherford , Darren Soto, Debbie Wasserman Schultz, Daniel Webster, Frederica Wilson, Ted Yoho

This report is available on our website at www.va.gov/oig