OFFICE OF THE STATE INSPECTOR GENERAL

Department of Veterans Services Information Technology Security and Procurement

Performance Audit

June 2023

Michael C. Westfall, CPA
State Inspector General

Report No. 2023-PA-007

COMMONWEALTH OF VIRGINIA
Office of the State Inspector General

Michael C. Westfall, CPA
State Inspector General

P.O. Box 1151
Richmond, Virginia 23218

Telephone 804-625-3255
Fax 804-786-2341
www.osig.virginia.gov

June 27, 2023

The Honorable Glenn Youngkin
Governor of Virginia
P.O. Box 1475
Richmond, VA 23219

Dear Governor Youngkin,

The Office of the State Inspector General (OSIG) completed an audit of the Virginia Department of Veterans Services (DVS) Information Technology Security and Procurement. The final report is attached.

OSIG would like to thank Commissioner Daniel Gade and his staff for their cooperation and assistance during this audit. OSIG would also like to thank the staff in the benefits offices and care centers for their cooperation and assistance during the audit.

Sincerely,

Michael C. Westfall, CPA
State Inspector General

CC: The Honorable Jeff Goettman, Chief of Staff to Governor Youngkin
Isabella Warwick, Deputy Chief of Staff to Governor Youngkin
The Honorable Craig Crenshaw, Secretary of Veterans and Defense Affairs
The Honorable Adam P. Ebbin, Senate Chair, General Laws and Technology Committee
The Honorable James A. Leftwich, House Chair, General Laws Committee
Michael Dick, Chairman of the Board of Veterans Services
Daniel Gade, Commissioner, Department of Veterans Services
Steven Combs, Chief Deputy Commissioner, Department of Veterans Services
Staci Henshaw, Auditor of Public Accounts

Department of Veterans Services

What OSIG Found

DVS HAS DEVELOPED A NETWORK COMPLIANCE PLAN TO ADDRESS IT SECURITY CONCERNS

DVS developed a Network Compliance Plan in November of 2022 to address IT infrastructure across the agency. The plan will bring DVS under Virginia Information Technologies Agency (VITA) compliance while also creating and strengthening network integrity at DVS offices. The plan also increases the efficiency and effectiveness of access management.

DVS IS OVERDUE ON OBTAINING VITA-REQUIRED IT SECURITY AUDITS

DVS has not accurately reported their sensitive systems to VITA resulting in VITA being unaware of DVS' sensitive systems requiring Information Technology (IT) security audits. Non-compliance with VITA Security Audit Standard, SEC 502, can result in unauthorized access, data loss, harm to reputation, legal action, and disruptions to critical operations if vulnerabilities in sensitive systems are undetected.

DVS SIGNED A CONTRACT IN VIOLATION OF THE VIRGINIA PUBLIC PROCUREMENT ACT

The DVS Sitter & Barfoot Veterans Care Center signed an IT-related contract that did not comply with the requirements of the Virginia Public Procurement Act (VPPA). The contract was signed without the involvement of DVS' central IT or central procurement functions. DVS officials signed a third-party vendor contract that did not include a dollar value, did not have an end date of service, and managed disputes in a state other than the Commonwealth.

Management concurred with all three of the findings and plans to implement corrective actions from May 31 to December 31, 2023.

June 2023

HIGHLIGHTS

Why OSIG Conducted This Audit

This audit was conducted at the request of the DVS Commissioner to improve the efficiency and effectiveness of DVS' IT security oversight and management.

What OSIG Recommends

- DVS should regularly assess and report their sensitive systems to VITA and have IT security audits performed as required.
- Procurement of IT systems and all contracts involving IT should require prior approval by DVS central IT leadership.
- DVS should adopt a uniform process to ensure that all contracts entered by agency personnel comply with VPPA and Agency Procurement & Surplus Property Manual (APSPM) requirements.
- DVS should ensure that DVS' central IT and central procurement functions have oversight and authority to ensure that procurement issues identified are properly addressed and remediated.

For more information, please contact OSIG at (804) 625-3255 or
www.osig.virginia.gov

TABLE OF CONTENTS

BACKGROUND

The Virginia Department of Veterans Services (DVS) operates more than 40 locations across the Commonwealth providing services to veterans and their families. This includes four veterans care centers, three veteran cemeteries, the Virginia War Memorial, 35 benefits centers, and the central office.

The DVS Information Technology (IT) office has four full-time employees and seven contractors to serve all DVS locations and support the agency's operations. The information systems used within the agency are operated on the Commonwealth and federal networks. DVS is currently undergoing modernization of their systems.

Procurement in central office is reviewed by the Chief Financial Officer (CFO) and Procurement Manager. DVS does not have any internal procurement policies related to IT but is required to follow VITA's IT procurement policies. The DVS offices refer to central office for IT related procurement.

SCOPE

The scope of this performance audit was IT security oversight and management. This included a review of the following areas:

- DVS physical and IT security for applications to include voicemails, spreadsheets, and other data files with sensitive information including Personally Identifiable Information (PII) and Protected Health Information (PHI).
- DVS IT procurement processes from July 1, 2021, through January 31, 2023.

OBJECTIVES

Objectives of this audit were to:

- Ensure the proper storage of PII and PHI on portable devices or at unauthorized locations, through verification of system controls.
- Determine if DVS has sufficient processes in place to allow DVS staff to properly procure IT assets in accordance with VITA requirements.

METHODOLOGY

OSIG conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that OSIG plan and perform the audit to obtain

sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. OSIG believes that the evidence obtained provides reasonable basis for the findings and conclusion based on the audit objectives. Additionally, OSIG applied various methodologies during the audit process to gather and analyze information pertinent to the project scope and to assist with developing and testing the project objectives. The methodologies included the following:

- Conducting interviews of executive management and agency staff.
- Conducting observations/walk-throughs of DVS Benefits Offices and Veterans Care Centers.
- Testing IT physical security controls at DVS Benefits Offices.
- Reviewing procurement policies and procedures.
- Testing of DVS purchasing requests.
- Testing of DVS IT procurements at Veterans Care Centers.
- Testing of DVS small purchase charge card (SPCC) transactions at Veterans Care Centers.

COMMENDATIONS

COMMENDATION #1 - DVS HAS DEVELOPED A NETWORK COMPLIANCE PLAN TO ADDRESS IT SECURITY CONCERNS

DVS developed a Network Compliance Plan in November of 2022 to address IT infrastructure across the agency. The plan will bring DVS under VITA compliance while also creating and strengthening network integrity at DVS offices. The plan also increases the efficiency and effectiveness of access management. DVS is already in the process of implementing their Network Compliance Plan.

COMMENDATION #2 - DVS IS IN THE PROCESS OF PROCURING NEW IT APPLICATIONS TO IMPROVE OPERATIONS

DVS has initiated the process of procuring new IT applications that allows for better integration of services across the DVS offices. DVS is working with VITA to ensure that the applications comply with all VITA requirements, to include application security.

FINDINGS

OSIG provided two other findings to DVS, separately, related to IT security that are not included in this report. DVS management agreed with the conditions observed in the findings and provided OSIG with a corrective action plan.

FINDING #1- DVS IS OVERDUE ON OBTAINING VITA-REQUIRED IT SECURITY AUDITS

Historically, DVS has not accurately reported their sensitive systems to VITA. As a result, VITA was unaware of DVS' sensitive systems requiring IT security audits. Accurately reporting sensitive systems to VITA was further complicated by entities under DVS' authority procuring IT resources and systems without the knowledge of DVS' central IT staff.

VITA Security Audit Standard, SEC 502, requires that, "IT systems that contain sensitive data or reside in a system with a sensitivity of high on any of the criteria of confidentiality, integrity, or availability, shall be assessed at least once every three years or more frequently commensurate with risk." DVS's last system security audits were conducted in 2018.

Non-compliance with VITA Security Audit Standard, SEC 502, can result in unauthorized access, data loss, harm to reputation, legal action, and disruptions to critical operations if vulnerabilities in sensitive systems are undetected. DVS currently has a plan to accomplish the needed audits within the fiscal year. The DVS IT Director has taken steps to address these issues.

Recommendations:

1. DVS should regularly assess and report their sensitive systems to VITA and have IT security audits performed as required by VITA Security Audit Standard, SEC 502.
2. Procurement of IT systems and all contracts involving IT should require prior approval by DVS central IT leadership.

DVS Management Response:

Management agreed with the conditions observed by OSIG and agreed with the recommendations.

Management Corrective Action

DVS will perform Risk Assessments to sensitive systems as required by VITA and regularly perform internal audits. Further DVS will modify the IT procurement process to include DVS central IT leadership approval. The expected completion date is December 31, 2023.

FINDING #2 - DVS SIGNED A CONTRACT IN VIOLATION OF THE VIRGINIA PUBLIC PROCUREMENT ACT

Sitter & Barfoot Veterans Care Center signed an IT-related contract that did not comply with the requirements of the Virginia Public Procurement Act (VPPA). The contract was signed without the involvement of DVS' central IT or central procurement functions. OSIG identified the following concerns:

- DVS officials signed a third-party vendor contract that did not include the required Virginia Public Procurement Act required terms and conditions.
- DVS did not provide evidence of following Commonwealth procurement requirements per the Agency Procurement and Surplus Property Manual (APSPM).
- The contract terms required that disputes are to be governed by and interpreted in accordance with the laws of the State of Tennessee.
- The agreement did not have a dollar value attached.
- The agreement did not have an end date of service.
- The agreement held DVS responsible to purchase a third-party license system if recommended by the contractor.
- The contract required a statement of work to document any specific work agreed upon between DVS and the third-party.

Per VPPA, "all public contracts with nongovernmental contractors for the purchase or lease of goods, or for the purchase of services… shall be awarded after competitive sealed bidding, or competitive negotiation. All state public bodies accepting bids or proposals for contracts shall provide an option to submit bids or proposals through the Commonwealth's statewide electronic procurement system, eVA."

DVS' central IT and central procurement functions had no knowledge of this contract being signed with the third-party contractor or that the contractor was not in eVA. OSIG found other contracts at the Sitter & Barfoot Veterans Care Center that had not been properly procured. DVS' central procurement function was not aware of these until after the agreements had been approved by the care center. Though OSIG did not find a statement of work between DVS and the third-party, services were rendered, and funds committed for IT services performed.

Recommendations:

1. DVS should adopt a uniform process to ensure that all contracts entered into by agency personnel comply with VPPA and APSPM requirements prior to final approval.
2. DVS should ensure that DVS' central IT and central procurement functions have oversight and authority to ensure that procurement issues identified are properly addressed and remediated.

3. DVS should work to identify and remediate any contracts that do not include the standard terms and conditions or are otherwise noncompliant with VPPA requirements.

DVS Management Response:

Management agreed with the conditions observed by OSIG and agreed with the recommendations.

DVS has already adopted the recommended process to review all the agency contracts, by Central Office Procurement staff prior to signature. This will be included in the updated policies that they are currently reviewing. All agency contracts are under review to ensure compliance.

Management Corrective Action

DVS will update their policy to require the review of all future contracts. In addition, all current contracts will be reviewed no later than May 31, 2023.

FINDING #3 - DVS DOES NOT HAVE A POLICY FOR MANAGING IT PROCUREMENT

DVS does not have a procurement policy in place to procure IT resources in an effective, efficient and VITA-compliant manner. Staff at DVS' thirty-five benefit offices, three cemeteries and four care centers have been following undocumented, inconsistent procurement procedures for IT and non-IT resources. Specifically, DVS' care centers have been operating independently of DVS IT's directions regarding procurement.

DVS uses an Internal Purchase Request (IPR) document for requesting and receiving procurement approvals. OSIG found this document was used consistently at benefit offices and cemeteries but did not find evidence that the IPR was used at care centers. OSIG also found that contracts at care centers were entered into without input and oversight from DVS central office procurement and DVS IT procurement. This resulted in at least one contract being signed by a care center that is not in compliance with Virginia's requirements and could allow for inappropriate use of sensitive agency data.

DVS' procurement of IT resources not being documented is due to staff relying on institutional knowledge of the procurement process. Additionally, prior staff did not follow VITA IT procurement requirements due to delays addressing VITA requirements for purchasing IT systems.

DVS is in the process of developing an internal procurement policy. The draft policy includes necessary approval from the agency Information Technology Resource before final approval in

eVA. The draft policy also lays out how IT procurement must be labeled for approval and points to VITA vendor list and policies for any IT related procurement.

Recommendation(s):

1. DVS should continue to finalize and publish this policy for guidance to staff to ensure that procurements are compliant with VITA and other Commonwealth procurement regulations.
2. DVS should ensure that its procurement policy includes the following:
    - Dollar, procurement type, and length of agreement thresholds requiring additional approval.
    - Central office's level of involvement with all types of procurement.
    - Requirements that central office review and approve prior to DVS finalizing the contract.

DVS Management Response:

Management agreed with the conditions observed by OSIG and agreed with the recommendations.

DVS is updating their procurement policies, which will be finalized soon. DVS is awaiting the outcome of this audit in order to ensure they have addressed all issues reported in the audit management comments. The expected completion date is May 31, 2023.

AUDIT RESULTS

This report presents the results of OSIG's audit of DVS IT physical and application security management and oversight, and IT procurement processes. The following testing was performed with immaterial, if any, discrepancies noted:

- DVS security awareness training provided to staff.
- DVS purchasing request process.

Based on the results and findings of the audit test work conducted of DVS, OSIG concluded that internal controls were operating properly except as identified in the report findings.

APPENDIX I – CORRECTIVE ACTION PLAN

FINDING NO.	RECOMMENDATION	CORRECTIVE ACTION	DELIVERABLE	ESTIMATED COMPLETION DATE	RESPONSIBLE POSITION
1	1. DVS should regularly assess and report their sensitive systems to VITA and have IT security audits performed as required by VITA Security Audit Standard, SEC 502. 2. Procurement of IT systems and all contracts involving IT should require prior approval by DVS central IT leadership.	• DVS will perform Risk Assessments to sensitive systems as required by VITA and regularly perform internal audits. • DVS will modify IT procurements process to include DVS central IT leadership approval.	• Risk assessments of sensitive systems • Regular internal audits • Modified IT procurements process	12/31/2023	DVS Chief Technology Officer
2	1. DVS should adopt a uniform process to ensure that all contracts entered into by agency personnel comply with VPPA and APSPM requirements prior to final approval. 2. DVS should ensure that DVS' central IT and central procurement functions have oversight and authority to ensure that procurement issues identified are properly addressed and remediated. 3. DVS should work to identify and remediate any contracts that do not include the standard terms and conditions or are otherwise noncompliant with VPPA requirements.	• Update policy to require review of all future contracts. In addition, all current contracts will be reviewed no later than May 31, 2023.	• Updated policy and review of all current contracts	5/31/2023	DVS Chief Financial Officer

FINDING NO.	RECOMMENDATION	CORRECTIVE ACTION	DELIVERABLE	ESTIMATED COMPLETION DATE	RESPONSIBLE POSITION
3	1. DVS should continue to finalize and publish this policy for guidance to its staff to ensure that procurements are compliant with VITA and other Commonwealth procurement regulations. 2. DVS should ensure that its procurement policy includes the following: • Dollar, procurement type, and length of agreement thresholds requiring additional approval. • Central office's level of involvement with all types of procurement. • Requirements that central office review and approve prior to DVS finalizing the contract.	• Update current policy to include OSIG recommendation	• Updated procurement policy	5/31/2023	DVS Chief Financial Officer