UNIVERSITY OF MARY WASHINGTON

REPORT ON AUDIT FOR THE YEAR ENDED JUNE 30, 2025

Auditor of Public Accounts
Staci A. Henshaw, CPA
www.apa.virginia.gov
(804) 225-3350

AUDIT SUMMARY

We have audited the basic financial statements of University of Mary Washington (University) as of and for the year ended June 30, 2025, and issued our report thereon, dated July 31, 2026. Our report, included in the University's basic financial statements, is available at the Auditor of Public Accounts' website at www.apa.virginia.gov and at the University's website at www.umw.edu. Our audit found:

- the financial statements are presented fairly, in all material respects;

- Six matters involving internal control and its operation requiring management's attention, that also represent instances of noncompliance with applicable laws and regulations that are required to be reported under Government Auditing Standards; however, we do not consider them to be material weaknesses; and

- One additional internal control finding requiring management's attention; however, we do not consider it to be a material weakness.

In the section titled "Internal Control and Compliance Findings and Recommendations" we have included our assessment of the conditions and causes resulting in the internal control and compliance findings identified through our audits as well as recommendations for addressing those finding. Our assessment does not remove management's responsibility to perform a thorough assessment of the conditions and causes of the findings and develop and appropriately implement adequate corrective actions to resolve the findings as required by the Department of Accounts in Topic 10205 – Agency Response to APA Audit of the Commonwealth Accounting Policies and Procedures Manual. Those corrective actions may include additional items beyond our recommendation.

-TABLE OF CONTENTS-

INTERNAL CONTROL AND COMPLIANCE FINDINGS AND RECOMMENDATIONS

Obtain and Retain Authorization for Wage Employee Compensation

Type: Internal Control

Severity: Significant Deficiency

The University of Mary Washington (University) does not have adequate policies and procedures surrounding the authorization of compensation for wage employees which resulted in unsupported or unauthorized compensation for wage employees. For 22 of the 40 (55%) wage employees selected, the University could not provide adequate documentation authorizing the employment or compensation of the wage employee. Of those 22 employees, the University was unable to provide supporting documentation for 11 of the employees' compensation rates, while the remaining 11 employees did not have authorized compensation rates. The lack of adequate policies and procedures resulted in unapproved or unsupported compensation rates utilized to calculate payments to student wage employees for 22 out of 28 paychecks (78.6%) selected.

University policies and procedures over student wage employees, the Student Employment Handbook (handbook), requires the hiring supervisor/department to complete the Student Employment Hire Form (SEMPL Form). The handbook further requires the supervisor/department to provide the completed SEMPL form to the Student Employment Coordinator by email to coordinate the student completion of any necessary documentation. University policies and procedures prohibit the employment of wage employees until the completion of all employment documents, and a work authorization is issued. The Code of Virginia § 42.1-76 through § 42.1-91, known as the Virginia Public Records Act, governs the creation, maintenance, and disposition of public records and states that the Library of Virginia's State Library Board shall issue regulations over the records management, including record retention. The Library of Virginia's record retention schedule over personnel records (Policy GS-103) requires the retention of employee personnel records related to compensation and position history for 50 years.

The University's handbook does not have a procedure for the communication of SEMPL forms to the Student Employment Coordinator, nor does it include retention requirements or procedures for documentation. In addition to the lack of requirements within the handbook, the University departments did not follow established policies and procedures within the handbook and were inconsistent in using SEMPL Forms that required an authorized signature. The lack of procedures and ineffective application of policies and procedures across University departments led to unauthorized and/or unsupported student employee compensation.

Without requiring or maintaining properly authorized SEMPL Forms or other pay authorization documentation, the University increases the risk that the compensation rates or adjustments to compensation for student workers are inappropriate or established by unauthorized individuals. Further, without ensuring proper retention of personnel documents, the University is unable to comply with the requirements of the Virginia Public Records Act, which prevents the University from supporting compensation and may result in penalties.

The University should update its policies and procedures to ensure it includes communication and retention requirements for SEMPL forms. Along with updates to its existing policies and procedures, the University should evaluate its SEMPL Form to ensure it includes all required elements from the policies and procedures to meet the needs of the University. The University should provide adequate communication and training on University policies and procedures to those responsible for completing and submitting employment documentation. The University should further consider whether there are opportunities to improve accountability of departments and/or supervisors for completing the SEMPL Forms in accordance with University policies and procedures.

Improve Offboarding Process

Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not have effective internal controls over the employee termination process. Management does not hold individual departments and supervisors accountable for following its offboarding procedures, resulting in supervisors not completing or submitting offboarding checklists (checklist) in accordance with University policy. Through our testing, we identified the following deficiencies:

- The University departments did not complete off-boarding checklists timely for seven of the 20 (35%) terminated employees selected. For three of these seven employees, the University did not complete an off-boarding checklist as of our review, while the remaining four employees did not have a checklist completed within 24 hours of the employee's termination date.

- The University did not ensure that employees returned University property before the employee's termination date for seven of the 21 (33%) terminated employees selected.

- The University did not complete the checklist to confirm the removal of physical and system access for seven out of 20 (35%) employees selected. Of those seven employees, the University did not remove access timely for three terminated employees selected.

The University's offboarding policies and procedures require supervisors to provide a copy of the offboarding checklist to employees separating from the University and meet with them prior to their termination to discuss and complete the checklist. The checklist includes requirements for the supervisor to initiate collection of University property, removal of physical access, and removal of University system access among other requirements. Once completed, the supervisor must provide the checklist to the Office of Human Resources (Human Resources) within 24 hours of the employee's termination. The University's Information Security Standard (Security Standard) also requires that Human Resources notify system administrators within 24 hours of an employee's termination.

By not completing the checklists in accordance with University policy and the Security Standard, the University risks not recovering University property from terminated employees. Further, failure to complete the checklist may result in unauthorized physical or system access. Not collecting property and removing access in a timely manner may result in unauthorized access or use of University property

or information. Unauthorized access to University information systems may result in the processing of unauthorized system transactions.

The University should ensure adequate policies and procedures are in place to ensure the completion of offboarding checklists and provide training to those responsible for performing the procedures. The University should further consider whether there are opportunities to improve accountability of departments and/or supervisors for completing the offboarding checklists in accordance with University policies and procedures.

Improve Internal Router Security
Type: Internal Control and Compliance
Severity: Significant Deficiency

The University should strengthen certain router security controls to ensure it operates in accordance with its Information Security Program Policy (Policy). We identified opportunities to improve the University's processes for assessing and monitoring the security of certain router infrastructure.

Effective router security assessment and monitoring processes provide management with important information regarding the security posture of critical network infrastructure and help identify vulnerabilities that could affect the confidentiality, integrity, and availability of university systems and data.

We communicated the specific control weaknesses, affected router components, associated security risks, and recommended corrective actions to University management in a separate communication. We excluded that information from the public report under Section 2.2-3705.2 of the Code of Virginia because it describes sensitive information about the University's information technology security controls, security mechanisms, and vulnerabilities.

The University should address router security control weaknesses and implement the corrective actions described in the separate FOIA-exempt communication in accordance with its Policy and applicable industry best practices. Strengthening these controls will help protect the confidentiality, integrity, and availability of the University's information systems and sensitive data.

Improve IT Asset Management Process
Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not document and implement an information technology (IT) asset management policy, procedure, and process in accordance with its Information Security Program Policy. Maintaining an IT asset management process ensures the protection of sensitive information on assets designated for surplus, including destruction and recycling. We communicated the control weaknesses in a separate document marked Freedom of Information Act Exempt (FOIAE) under Section 2.2-3705.2 of the Code of Virginia due to its sensitivity and description of security mechanisms.

The University should improve IT asset management processes as discussed in the communication marked FOIA Exempt in accordance with its Information Security Program Policy and

industry best practices. Improving IT asset management processes will help protect the confidentiality, integrity, and availability of the University's sensitive data.

Improve Security Awareness Training Program

Type: Internal Control and Compliance
Severity: Significant Deficiency

The University does not administer its information security awareness training program in accordance with its Information Technology (IT) Security Awareness and Training Policy (Security Awareness Policy). In addition to the Security Awareness Policy, the University did not comply with their own documented procedures that establish the requirements and scope of the University's information security awareness training program. All users assigned security awareness training completed the training, which included 978 of 1794 users (55%) with access to IT systems. However, the University did not assign security awareness training to 39 of 75 (52%) new hires and 777 of 1719 (45%) existing users, resulting in a total of 816 of 1794 (45%) users with access to IT systems that the University did not assign security awareness training.

The University's Security Awareness Policy requires that the University provide security awareness training annually to all users that have access to its IT systems and after employment for all new hires that have access to its IT systems. Lack of management oversight and a process breakdown resulted in the University not assigning information security awareness training to all users with access to IT systems. The process breakdown occurred due to the manual steps the University follows to add users to their security awareness training platform and subsequently assign users' information security awareness training.

An established information security awareness training program is essential to protecting IT systems and data by ensuring that employees understand their roles and responsibilities in securing sensitive information at the agency. Without assigning security awareness training to all users with access to its IT systems to ensure users complete the training; the University increases the risk that users are not aware of the specific requirements for its IT environment. Additionally, the users may be more susceptible to malicious attempts to compromise sensitive data, such as ransomware, phishing, and social engineering.

The University should strengthen its procedures surrounding the manual steps for assigning IT system users to the information security awareness training platform to ensure all users receive required information security awareness training, including annual training for existing users and new hire training, as required by the University's Security Awareness Policy. Improving the information security awareness training program will help protect the agency from malicious attempts to compromise confidentiality, integrity, and availability of sensitive information.

Comply with Conflict-of-Interest Act Requirements

Type: Internal Control and Compliance

Severity: Significant Deficiency

The University does not ensure compliance with the Conflict-of-Interest Act (COIA) requirements for monitoring, filing, and training. Through our testing, we noted the following instances of noncompliance:

- The University does not maintain an accurate and complete list of employees in positions of trust required to file a Statement of Economic Interest (SOEI) disclosure. The University did not adequately track or identify 16 out of 114 employees (14%) holding positions of trust who are noted in the Commonwealth's human resource and payroll management system as required to file a SOEI disclosure. Additionally, the University's tracking list over filers did not have accurate training dates for eight employees when compared to the database maintained by the Virginia Conflict of Interest and Ethics Advisory Council (Ethics Council).

- The University did not ensure timely submission of SOEI forms in accordance with the Code of Virginia. Four new employees in positions of trust failed to file a SOEI form within two months of their employment start date and six existing employees in a position of trust failed to file prior to the February deadline.

- The University did not ensure that employees completed their conflict-of-interest training in accordance with the Code of Virginia. Twenty-one employees in positions of trust at the University did not complete conflict of interest training timely in accordance with the Code of Virginia. Two employees did not complete the conflict-of-interest training in accordance with the Code of Virginia as of our review.

Pursuant to Code of Virginia § 2.2-3129, agencies shall maintain records indicating specific attendees, each attendee's job title, and dates of their attendance for each orientation course. Code of Virginia §§ 2.2-3114A and 2.2-3117 require employees in a position of trust to file with the Council, as a condition to assuming office or employment, a disclosure statement of their personal interests and thereafter shall file such a statement annually on or before February 1st. Additionally, Code of Virginia § 2.2-3130, requires each state filer to attend an ethics and conflict of interest training course initially within two months after he or she becomes a state filer and thereafter on a biennial basis. Further, the University's COIA procedures require filing by employees in a position of trust prior to the first day of employment and for training to be completed within two months of the hire date.

The University's current process of identifying employees in positions of trust occurs through University-wide emails or a quarterly review that does not adequately identify all employes in positions of trust timely to ensure compliance with the Code of Virginia SOEI disclosure and training requirements. Additionally, the University does not verify the accuracy of its internal training records and ensure agreement with the Ethics Council database. Without appropriately identifying employees in positions of trust and ensuring adequate disclosure and completion of required training, the University could be susceptible to actual or perceived conflicts of interest and may limit its ability to hold its employees accountable for not knowing how to recognize and resolve a conflict of interest. Any actual or perceived

conflicts of interest could impair or appear to impair the objectivity of transactions, contract procurement, and/or fiscal decisions made by employees in positions of trust. Employees and board members could be subject to penalties for inadequate disclosure on their filings, as outlined within § 2.2-3120 through § 2.2-3127 of the Code of Virginia.

The University should improve its identification and monitoring processes over employees in positions of trust to ensure compliance with the Conflict-of-Interest Act. In addition to process improvements, the University should evaluate policies and procedures over enforcement of the COIA to ensure that employees comply with the Code of Virginia. Further, the University should improve the process for maintaining its tracking list over employees in positions of trust to include a cross-check with the Ethics Council database.

Comply with Employment Eligibility Requirements

Type: Internal Control and Compliance
Severity: Significant Deficiency

During fiscal year 2025, the University did not complete Section 2 of the Employment Eligibility Verification (I-9) Form within three business days of the employee's first day of employment. The University uses a mass hiring process for student workers at the beginning of each semester; however, University management did not have sufficient resources to accommodate the increased volume of forms. As a result, University completed ten out of the 25 (40%) I-9 forms and 11 out of 25 (44%) E-Verify cases selected between two and 24 business days late. In addition, the University did not provide the I-9 form for one employee out of the 25 selected; therefore, the form could not be tested for compliance with federal regulations. During the audit period, the University stated that Human Resources staff could not retrieve the I-9 form as it was stored in a building undergoing mold abatement and foundation repairs.

The Immigration Reform and Control Act of 1986 requires employers to complete I-9 Forms to verify both employment eligibility and identity for all employees. The U.S. Citizenship and Immigration Services sets forth federal requirements for completing I-9 Forms in the Handbook for Employers M-274 (Handbook). Section 4.0 of the Handbook requires the employer to complete Section 2 of the I-9 Form within three business days of the date employment begins. The E-Verify User Manual M-775, Chapter 2.2 requires the employer to create a case for each newly hired employee no later than the third business day after he or she starts work for pay. Section 10 of the Handbook requires I-9 Forms to be readily retrievable to support the employee's eligibility and identity. Noncompliance with federal regulations related to employment verification could result in civil and/or criminal penalties and debarment from government contracts.

The University should dedicate additional resources for completing I-9 forms and E-Verify cases during periods of mass hiring to ensure timely completion of the I-9 forms and E-Verify in accordance with federal regulations. For instances in which the E-Verify delay is due to technical problems or employee delays, management should retain supporting documentation for the delay. Management should also properly train employees tasked with completing I-9 Forms to ensure they are familiar with the requirements for completing and retaining I-9 Forms in accordance with federal regulations.

Commonwealth of Virginia

Auditor of Public Accounts

Staci A. Henshaw, CPA
Auditor of Public Accounts

P.O. Box 1295
Richmond, Virginia 23218

July 31, 2026

The Honorable Abigail D. Spanberger
Governor of Virginia

Joint Legislative Audit
and Review Commission

Board of Visitors
University of Mary Washington

Dr. Troy Paino
University of Mary Washington

INDEPENDENT AUDITOR'S REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in Government Auditing Standards, issued by the Comptroller General of the United States, the financial statements of the business-type activities and discretely presented component unit of the **University of Mary Washington** (University) as of and for the year ended June 30, 2025, and the related notes to the financial statements, which collectively comprise the University's basic financial statements and have issued our report thereon dated July 31, 2026. Our report includes a reference to another auditor who audited the financial statements of the component unit of the University, as described in our report on the University's financial statements. The other auditor did not audit the financial statements of the component unit of the University in accordance with Government Auditing Standards, and accordingly, this report does not include reporting on internal control over financial reporting or compliance and other matters associated with the component unit of the University.

Report on Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the University's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the University's internal control. Accordingly, we do not express an opinion on the effectiveness of the University's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented or detected and corrected on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control titled **"**Obtain and Retain Authorization for Wage Employee Compensation," "Improve Offboarding Process," "Improve Internal Router Security," "Improve IT Asset Management Process," "Improve Security Awareness Training Program," "Comply with Conflict-of-Interest Act Requirements," and "Comply with Employment Eligibility Requirements," which are described in the section titled "Internal Control and Compliance Findings and Recommendations," that we consider to be significant deficiencies.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the University's financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed instances of noncompliance or other matters that are required to be reported under Government Auditing Standards and which are described in the section titled "Internal Control and Compliance Findings and Recommendations" in the findings titled "Improve Offboarding Process," "Improve Internal Router Security," "Improve IT Asset Management Process," "Improve Security Awareness Training Program," "Comply with Conflict of Interest Act Requirements," and "Comply with Employment Eligibility Requirements."

The University's Response to Findings

We discussed this report with management on September 10, 2026. Government Auditing Standards require the auditor to perform limited procedures on the University's response to the findings identified in our audit, which is included in the accompanying section titled "University Response." The University's response was not subjected to the other auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with Government Auditing Standards in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Staci A. Henshaw
AUDITOR OF PUBLIC ACCOUNTS

JJR/clj

FINDINGS SUMMARY

Finding Title	Status of Corrective Action*	Fiscal Year First Reported
Obtain and Retain Authorization for Wage Employee Compensation	Ongoing	2025
Improve Offboarding Process	Ongoing	2025
Improve Internal Router Security	Ongoing	2025
Improve IT Asset Management Process	Ongoing	2025
Improve Security Awareness Training Program	Ongoing	2025
Comply with Conflict-of-Interest Act Requirements	Ongoing	2025
Comply with Employment Eligibility Requirements	Ongoing	2025

* A status of **Ongoing** indicates new and/or existing findings that require management's corrective action as of fiscal year end.

University of Mary Washington

Finance
1301 College Avenue
Fredericksburg, VA 22401-5300

September 4, 2026

Staci Henshaw, CPA
Auditor of Public Accounts
P O Box 1295
Richmond, VA 23218

Dear Ms. Henshaw,

Administration at the University of Mary Washington has reviewed the Internal Control and Compliance Findings and Recommendations report provided by the Auditor of Public Accounts for the fiscal year ended June 30, 2025. The University appreciates the effort and work of the APA and has the following response to the report.

Obtain and Retain Authorization for Wage Employee Compensation
The University is updating policies, procedures and forms to address communication and documentation retention requirements related to work authorization and compensation. Training will be provided, as appropriate. The University is committed to ensuring ongoing compliance with employment policies, procedures and documentation requirements.

Improve Offboarding Process
The University has taken steps to address the importance of timely completion of the out-processing checklist. It should be noted that the checklist does not initiate system access removal. There is a separate notification process that takes place prior to the employee's final day of employment. The University is committed to ensuring ongoing compliance with the related policies and procedures.

Improve Internal Router Security
The University has reviewed and updated the scope of its vulnerability scanning program to ensure that all critical infrastructure components, including internal network devices such as routers and firewalls, are explicitly identified and included. This includes coordination with the external scanning provider to validate asset inventories and ensure comprehensive coverage. In addition, the University is strengthening governance over vulnerability management. The University is committed to ensuring comprehensive vulnerability management coverage and will continue to enhance oversight and validation processes to prevent recurrence of this condition.

Improve IT Asset Management Process
Corrective actions are underway to address asset management issues comprehensively. The University is implementing a standardized, end-to-end IT asset lifecycle management process. Controls are being integrated into a broader asset governance framework to ensure ongoing compliance, auditability, and protection of sensitive information throughout the asset disposal lifecycle. The University is committed to remediating this control weakness and establishing a sustainable, verifiable process that ensures full accountability for all IT assets from decommissioning through final disposition.

Improve Security Awareness Training Program
The University has taken corrective action to address both the control gap and the underlying process deficiencies. Specifically, the University has transitioned from a manually driven assignment process to a structured, identity-driven approach that aligns training requirements with user lifecycle events. The University is also aligning its training program with broader identity and access governance improvements to ensure that assignment of required training is consistently enforced as part of the user access lifecycle. The University is committed to maintaining a comprehensive and effective information security awareness training program and will continue to monitor and refine these controls to ensure ongoing compliance with policy and audit expectations.

Comply with Conflict of Interest Act Requirements
The University has revised processes to improve tracking and monitoring of Statement of Economic Interest (SOEI) training and disclosure. In addition, integration of SOEI indicators on positions provides earlier identification of positions of trust and allows for better reporting. The University is committed to ensuring compliance with the Conflict of Interest Act.

Comply with Employment Eligibility Requirements
The University is updating I-9 verification procedures related to our student employees and will provide appropriate training. Additional resources will be assigned to the process during periods of mass hiring. The University is committed to ensuring ongoing compliance with Employment Eligibility Verification requirements.

We appreciate the opportunity to respond and address the findings.

Kind Regards,

Julie R Smith Digitally signed by Julie R Smith
Date: 2026.09.04 16:18:14 -04'00'

Julie Smith
Associate Vice President for Finance and Controller
jsmith23@umw.edu
540-654-1614