

Audit Report

St. Mary's College of Maryland

August 2016



OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

For further information concerning this report contact:

Department of Legislative Services

Office of Legislative Audits

301 West Preston Street, Room 1202

Baltimore, Maryland 21201

Phone: 410-946-5900 · 301-970-5900

Toll Free in Maryland: 1-877-486-9964

Maryland Relay: 711

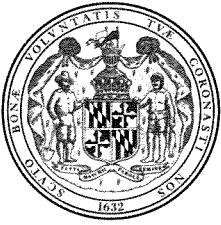
TTY: 410-946-5401 · 301-970-5401

E-mail: OLAWebmaster@ola.state.md.us

Website: www.ola.state.md.us

The Office of Legislative Audits operates a Fraud Hotline to report fraud, waste, or abuse involving State of Maryland government resources. Reports of fraud, waste, or abuse may be communicated anonymously by a toll-free call to 1-877-FRAUD-11, by mail to the Fraud Hotline, c/o Office of Legislative Audits, or through the Office's website.

The Department of Legislative Services does not discriminate on the basis of age, ancestry, color, creed, marital status, national origin, race, religion, gender, gender identity, sexual orientation, or disability in the admission or access to its programs, services, or activities. The Department's Information Officer has been designated to coordinate compliance with the nondiscrimination requirements contained in Section 35.107 of the Department of Justice Regulations. Requests for assistance should be directed to the Information Officer at 410-946-5400 or 410-970-5400.



DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Warren G. Deschenaux
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

August 17, 2016

Senator Guy J. Guzzone, Chair, Joint Audit Committee
Delegate C. William Frick, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have conducted a fiscal compliance audit of St. Mary's College of Maryland (the College) for the period beginning July 1, 2012 and ending August 23, 2015. The College is a public, liberal arts honors college that offers undergraduate and graduate degree programs in various disciplines. The College is governed by a Board of Trustees as authorized by the Education Article, Title 14, Subtitle 4 of the Annotated Code of Maryland.

Our audit disclosed security and control deficiencies over the College's information systems. For example, the College had not established appropriate safeguards to protect sensitive personally identifiable information in a critical database which, in part, contained information about students and employees. Additionally, numerous users were granted unnecessary privileges on their workstations resulting in increased security threats, and certain workstations had not been updated with the latest software releases to protect against known vulnerabilities.

Our audit also disclosed that the College did not ensure the propriety of amounts billed by its food services vendor by routinely obtaining cost documentation that was the basis for payments which totaled approximately \$4.2 million during calendar year 2015.

Finally, the College did not independently review accumulated leave payout calculations, resulting in an overpayment of approximately \$10,000 for one individual retiring from State service.

The College's response to this audit is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by the College.

Respectfully submitted,



Thomas J. Barnickel III, CPA
Legislative Auditor

Table of Contents

Background Information	4
Agency Responsibilities	4
Status of Findings From Preceding Audit Report	4
Findings and Recommendations	5
Information Systems Security and Control	
Finding 1 – Sensitive personally identifiable information applicable to 117,194 unique individuals was not appropriately safeguarded.	5
* Finding 2 – The College’s computers were not adequately secured from malware and the College lacked assurance that malware protection software was fully operational.	6
Finding 3 – Certain database security events were not monitored, and documentation supporting independent reviews of direct changes to critical tables did not exist.	7
Food Services Contract	
* Finding 4 – The College did not ensure the accuracy of amounts invoiced by its food services vendor which totaled \$4.2 million during calendar year 2015.	8
Leave Overpayment	
Finding 5 – The College did not independently review accumulated leave payout calculations, resulting in an overpayment of approximately \$10,000 for one individual retiring from State service.	9
Audit Scope, Objectives, and Methodology	11
Agency Response	Appendix

* Denotes item repeated in full or part from preceding audit report

Background Information

Agency Responsibilities

St. Mary's College of Maryland (the College) is a public, liberal arts honors college that offers undergraduate degree programs in various disciplines and a graduate degree in Masters of Arts in Teaching. The College is governed by a Board of Trustees as authorized by the Education Article, Title 14, Subtitle 4 of the Annotated Code of Maryland. This law provides the Board with broad authority in managing the affairs of the College, and specifies that the Board may not be superseded in its authority by any State agency or office except as expressly provided in law. Furthermore, the law provides for the College to receive State general funds in the form of an annual grant. According to the State's records, fiscal year 2015 revenues totaled approximately \$65.6 million, which included a State general fund appropriation of approximately \$18.2 million. According to the College's records, student enrollment for the Fall 2015 semester totaled 1,773.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the eight findings contained in our preceding audit report dated November 19, 2013. We determined that the College satisfactorily addressed six of the findings. The remaining two findings are repeated in this report.

Findings and Recommendations

Information Systems Security and Control

Background

The St. Mary's College of Maryland's (the College) Office of Information Technology provides information systems support to the College through the operation and maintenance of campus-wide administrative applications, such as the student information and financial system. The Office also operates an integrated administrative and academic computer network that provides connections to a substantial number of servers used for administrative applications and related databases. The campus network also includes separate file servers, Internet connectivity, and firewalls.

Finding 1

Sensitive personally identifiable information applicable to 117,194 unique individuals was not appropriately safeguarded.

Analysis

Sensitive personally identifiable information (PII) was stored in a critical database containing, in part, student and employee information in clear text. Specifically, we noted that, as of January 28, 2016, this database contained sensitive PII for 117,194 unique individuals in clear text. This included the individuals' full names, social security numbers and, in some cases, dates of birth. In addition, we determined that this sensitive PII was not protected by other substantial mitigating controls.

This PII, which is commonly associated with identity theft, should be protected by appropriate information system security controls. Best practices as noted in the University System of Maryland (USM) *Information Technology Security Standards* state that protection measures for confidential data can include the deletion of unneeded confidential information, encryption or other equally secure safeguards; and if encryption is used to protect confidential information, then certain encryption standards must be used.

Recommendation 1

We recommend that the College

- a. perform a complete inventory of its systems and identify all sensitive PII,**
- b. determine if it is necessary to retain this PII and delete all unnecessary PII,**
- c. determine if this sensitive information is properly protected by encryption or other equally secure safeguards, and**

- d. **comply with the aforementioned USM *IT Security Standards* to control and properly secure all sensitive PII.**

Finding 2

The College's computers were not adequately secured from malware, and the College lacked assurance that malware protection software was operational on all of its workstations and servers.

Analysis

The College's computers were not adequately secured from malware, and the College lacked assurance that malware protection software was operational on all of its workstations and servers.

- Although the College had procedures requiring written authorization for users (other than system and network administrators) to have administrative rights on their local workstations, for 36 of 100 workstations tested the users were inappropriately given administrative rights without such written authorizations. As a result, if the workstations used by these 36 employees were infected with malware, the malware would run with administrative rights and expose these workstations to a greater risk of compromise than if the workstations' user accounts operated with only user rights.
- Certain workstations had not been updated with the latest releases for software products that are known to have significant security-related vulnerabilities. Although the vendors for these software products frequently provide software patches to address these vulnerabilities, the College had not updated all of its workstations for these patches. For example, 9 of 10 workstations tested were running older versions of three commonly vulnerable applications which were outdated up to 31 months.
- As of February 22, 2016, the College's malware protection tool reported that the Campus network included 314 computers that did not have malware protection software installed. College personnel advised us that this information was unreliable because it included numerous retired computers that had not been removed from the College's network directory of computers and that certain computers were configured to report to an outdated malware protection tool rather than the current malware protection tool. As a result, the College did not know the number or identity of computers that did not have malware protection software installed. A similar condition was commented upon in our preceding audit report.

Best practices, as noted in the USM *Information Technology Security Standards*, state that standard virus protection programs must be installed, updated, and maintained on all computers.

Recommendation 2

We recommend that the College

- a. ensure that administrative rights on its workstations are restricted to system and network administrators and those employees authorized in writing to have such rights;**
- b. promptly install all critical security-related software updates for commonly vulnerable applications on all of its workstations; and**
- c. ensure, on an ongoing basis, that all of its computers are running current versions of its malware protection software (repeat).**

Finding 3

Certain database security events were not monitored and documentation supporting independent reviews of direct changes to critical tables did not exist.

Analysis

Certain database security events were not monitored and documentation supporting independent reviews of direct changes to critical tables did not exist.

- Although security and audit events for the database supporting the student information and financial system were logged, we were advised that reports of this logged activity were not generated for subsequent review. As a result, improper and/or unauthorized changes to database security and audit settings would not be detected by management.
- Although College personnel advised that independent reviews of reports of direct changes to 42 critical student information and financial system database tables were performed, these reviews were not documented. As a result, there was no assurance that these reviews were performed. Therefore, unauthorized modifications to critical database tables may not be detected by management.

Best practices as noted in the USM *Information Technology Security Standards* require institutions to maintain appropriate audit trails of events and actions related to critical applications and data and further require that these actions be independently reviewed and documented.

Recommendation 3

We recommend that the College

- a. generate reports of security and audit events for the database supporting the student information and financial system; and**
- b. perform periodic independent reviews of these security and audit event reports and direct changes to critical database tables, document these reviews, and retain the documentation for future reference.**

Food Services Contract

Finding 4

The College did not ensure the propriety of amounts invoiced by its food services vendor before payment. Calendar year 2015 invoices totaled \$4.2 million.

Analysis

The College paid its food services vendor without ensuring the propriety of invoices submitted. The food services contract provided for the College to reimburse the vendor that operated its dining services facilities for certain costs incurred (primarily labor costs and the cost of goods sold such as food and beverages) that exceeded the revenue collected by the vendor (such as from catered services). However, the College did not routinely obtain and review detailed documentation to support the invoiced costs. As a result, the propriety of the invoiced costs was not sufficiently verified before payment. Rather, the College's review was generally limited to ensuring that the amounts charged were within the contractor's approved annual budget.

College management advised us that, because of the complexity of the invoices, the College only obtained documentation from the food services vendor for three weekly invoices each year and used that documentation to verify the propriety of amounts billed. For example, in calendar year 2015, the College verified just three invoices totaling \$249,000 of the 52 invoices that the College paid the vendor totaling approximately \$4.2 million. Furthermore, our review of the College's verification of one of these invoices totaling \$47,675 disclosed that there was no documentation supporting charges totaling \$15,200 included on that invoice. For example, the College represented that it had verified labor charges, but the documentation obtained did not support the amount invoiced, and the College could not explain the discrepancy.

In July 2013, the College entered into a two-year contract (with five one-year renewal options), with a base term valued at approximately \$8.7 million for

campus food services management. This contract was awarded to the same vendor that had provided these services since May 2005. A similar condition was commented upon in our preceding audit report.

Recommendation 4

We recommend that the College ensure that charges billed by the food services contractor are adequately supported and verified prior to payment (repeat).

Leave Overpayment

Finding 5

The College did not independently review accumulated leave payout calculations, resulting in an overpayment of approximately \$10,000 for one individual retiring from State service.

Analysis

The College did not have a procedure to require that calculations of accumulated leave payouts for employees leaving State service be independently reviewed for propriety. Our review of two leave payouts totaling \$40,000 disclosed that the College incorrectly calculated a leave payout for one individual who retired from State service, resulting in an overpayment of \$9,924.

Specifically, the College paid this individual \$38,118 for 630 hours of unused annual leave, which included 564 hours of unused leave carried forward from the preceding year. However, State law only allows payments for up to 400 hours of leave from prior years, as well as for leave earned in the current year, which would have resulted in a payout of \$28,194, indicating an overpayment of \$9,924. Although the College is exempt from the aforementioned State law, this individual was employed by another State agency but was assigned to work at the College and, therefore, was subject to this law.

We were advised by College management that it was unaware of the State laws applicable to this individual so it paid the employee for the total leave balance. However, this approach was also not consistent with the College's own policy which was more restrictive than the State law and would have limited the payment to this employee to \$11,497 (resulting in an overpayment of \$26,621).

College management further advised us that it will not attempt to recover this overpayment because the individual could have taken the unused leave prior to retirement. However, the individual did not use the leave and would not have

been able to use all of the leave under State regulations. Specifically, the regulations provide that, once an employee has given notice of resignation, the employee may not use more than 10 days of annual, personal, or compensatory leave, or any combination of those types of leave, between the time notice is given and the effective date of resignation.

In light of these circumstances, we discussed this matter with the Office of the Attorney General. The Office has agreed to consider performing additional follow-up action, including possible recovery of the funds.

Recommendation 5

We recommend that the College

- a. ensure that calculations of accumulated leave payouts are subject to a documented independent review and approval;**
- b. ensure future annual leave payouts are calculated in accordance with State law or College policy, as appropriate; and**
- c. in conjunction with the Office of the Attorney General, take appropriate follow-up actions including pursuing the recovery of the aforementioned overpayment.**

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of St. Mary's College of Maryland (the College) for the period beginning July 1, 2012 and ending August 23, 2015. The audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine the College's financial transactions, records, and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of significance and risk. The areas addressed by the audit included purchases and disbursements, student accounts receivable, cash receipts, information systems security and control, payroll, student financial aid, and corporate purchasing cards. Our audit included certain support services (such as payment processing, payroll processing, maintenance of personnel and accounting records, and related fiscal functions) provided by the College to the Historic St. Mary's City Commission. We also determined the status of the findings included in our preceding audit report.

Our audit did not include an evaluation of internal controls over compliance with federal laws and regulations for federal financial assistance programs and an assessment of the College's compliance with those laws and regulations because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including the College.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspections of documents and records, observations of the College's operations, and tests of transactions. Generally, transactions were selected for testing based on auditor judgment, which primarily considers risk. Unless otherwise specifically indicated, neither statistical nor non-statistical audit sampling was used to select the transactions tested. Therefore, the results of the tests cannot be used to project those results to the entire population from which the test items were selected.

We also performed various data extracts of pertinent information from the State's Financial Management Information System (such as revenue and expenditure data) and the State's Central Payroll Bureau (payroll data), as well as from the contractor administering the State's Corporate Purchasing Card Program (credit card activity). The extracts are performed as part of ongoing internal processes established by the Office of Legislative Audits and were subject to various tests to determine data reliability. We determined that the data extracted from these various sources were sufficiently reliable for the purposes the data were used during this audit. We also extracted data from the College's financial system for the purpose of testing certain areas, such as student accounts receivable and financial aid. We performed various tests of the relevant data and determined that the data were sufficiently reliable for the purposes the data were used during the audit. Finally, we performed other auditing procedures that we considered necessary to achieve our audit objectives. The reliability of data used in this report for background or informational purposes was not assessed.

The College's management is responsible for establishing and maintaining effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including the safeguarding of assets and compliance with applicable laws, rules, and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings related to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect the College's ability to maintain reliable financial records, operate effectively and efficiently, and/or comply with applicable laws, rules, and regulations. Our report also includes findings regarding significant instances of noncompliance with applicable laws, rules, or regulations. Other less significant findings were communicated to the College that did not warrant inclusion in this report.

The response from the College to our findings and recommendations is included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the College regarding the results of our review of its response.

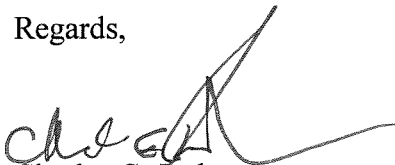
August 16, 2016

Thomas J. Barnickel, III, CPA
Legislative Auditor
Department of Legislative Service
Office of Legislative Audits
Maryland General Assembly
301 West Preston Street, Room 1202
Baltimore, Maryland 21201

Dear Mr. Barnickel:

St. Mary's College of Maryland is in receipt of your correspondence dated July 28, 2016 requesting responses to the audit report comments and recommendations. Per your request, we are pleased to submit our responses to each of the five findings. Please contact me at 240-895-4413, or via email at ccjackson@smcm.edu, with any questions, or if further information is needed.

Regards,



Charles C. Jackson
Vice President for Business and Finance

cc: Tuajuanda C. Jordan, President

St. Mary's College of Maryland
Agency Response to Draft Audit Report
for the Period Beginning July 1, 2012 and Ending August 23, 2015

Finding 1 – Sensitive personally identifiable information applicable to 117,194 unique individuals was not appropriately safeguarded.

Response: The College agrees with this finding. We have taken steps to mask certain personally identifiable information in the database for users that do not require that information to perform their job duties. The College expects to have all recommendations implemented by January 2017.

Finding 2 – The College's computers were not adequately secured from malware and the College lacked assurance that malware protection software was fully operational.

Response: The College agrees with this finding. Work has begun on all recommendations ensuring limited and documented access for user administrative rights, applying critical security related updates for commonly vulnerable applications to all workstations, and ensuring all computers are running current versions of malware protection software. The College expects to have all recommendations implemented by November 2016.

Finding 3 – Certain database security events were not monitored, and documentation supporting independent reviews of direct changes to critical tables did not exist.

Response: The College agrees with this finding and has implemented the recommendations to generate reports of security and audit events, provide independent reviews of the reports, and document the reviews.

Finding 4 – The College did not ensure the accuracy of amounts invoiced by its food services vendor which totaled \$4.2 million during calendar year 2015.

Response: The College agrees to perform additional verification of charges billed by the food service vendor. The College and OLA have agreed on specific procedures which will be implemented by October 2016. The major points of the agreed upon procedure is that the College will verify direct labor charges on a bi-weekly basis and will randomly select a limited number of significant cost of goods sold items each week for verification.

Finding 5 – The College did not independently review accumulated leave payout calculations, resulting in an overpayment of approximately \$10,000 for one individual retiring from State service.

Response: The College agrees that future annual leave payouts are to be calculated in accordance with College policy. The College will implement procedures to ensure that payout of accrued leave does not exceed the number of allowed hours.

Further, the College has contacted the Office of Attorney General and will coordinate any additional follow-up action on this issue as they deem appropriate.

August 16, 2016

AUDIT TEAM

Heather A. Warriner, CPA
Audit Manager

Richard L. Carter, CISA
Stephen P. Jersey, CPA, CISA
Information Systems Audit Managers

Marissa L. Eby, CPA
Senior Auditor

Michael K. Bliss, CISA
Edwin L. Paul, CPA, CISA
Information Systems Senior Auditors

Matusala Y. Abishe
Amanda M. Jones
Staff Auditors

Steven D. Bryant
Robert H. Dean
Edward O. Kendall
Information Systems Staff Auditors