Audit Report

University System of Maryland
Frostburg State University

April 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.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Warren G. Deschenaux
Executive Director

Thomas J. Barnickel III, CPA
Legislative Auditor

April 19, 2016

Senator Guy J. Guzzone, Co-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 the University System of Maryland (USM) – Frostburg State University (FSU) for the period beginning June 4, 2012 and ending June 30, 2015. FSU is a comprehensive public institution of USM and operates under the jurisdiction of the USM's Board of Regents. FSU offers an array of undergraduate and graduate degrees.

Our audit disclosed security and control deficiencies over FSU's information systems. For example, capabilities assigned to individuals on FSU's financial management systems were not adequately restricted, allowing certain individuals to have incompatible duties over student accounts and financial aid. FSU also did not establish appropriate safeguards to protect sensitive personally identifiable information in two databases, and numerous workstations were not properly maintained and secured.

The USM Office's response to this audit, on behalf of FSU, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during the course of this audit by FSU.

Respectfully submitted,

Thomas J. Barnickel III, CPA
Legislative Auditor

301 West Preston Street · Room 1202 · Baltimore, Maryland 21201
410-946-5900/301-970-5900 · Fax 410-946-5999/301-970-5999
Toll Free in Maryland 877-486-9964 · Fraud Hotline 877-FRAUD-11

Table of Contents

Background Information

Agency Responsibilities

Frostburg State University (FSU) is a comprehensive public institution of the University System of Maryland (USM) and operates under the jurisdiction of the System's Board of Regents. FSU offers an array of undergraduate and graduate degrees with an emphasis on arts, humanities, business, applied technologies, education, environmental sciences, human services, and social and behavioral sciences. Student enrollment for the Fall 2015 semester totaled 5,756 students, including 4,961 undergraduate students and 795 graduate students. FSU's budget is funded by unrestricted revenues, such as tuition and fees and a State general fund appropriation, and by restricted revenues, such as federal grants and contracts. According to the State's accounting records, FSU's revenues for fiscal year 2015 totaled approximately $114.6 million, including a State general fund appropriation of approximately $37.4 million.

Former FSU Official's Leave Usage

FSU and USM's Internal Audit Unit conducted an investigation into possible irregularities in leave reporting. In particular, the investigation examined the propriety of 30 days of sick leave taken by a former FSU official just prior to the official's departure from FSU in 2015. Reporting sick leave rather than annual leave effectively increased the official's final payment for unused annual leave. At the conclusion of the investigation, the USM Chancellor advised the former official, in an October 2015 letter, that the net amount of sick leave for the 30 days in question was $20,044.

As required by a Governor's Executive Order (*Standards of Conduct for Executive Branch Employees and Reporting of Misconduct*), in October 2015 the Chancellor advised the Office of the Attorney General's Criminal Division of the possible irregularities. This matter was also forwarded to the Governor's Chief Counsel.

USM advised us that FSU received payment of $20,044 on April 18, 2016 and that it does not anticipate taking any further action.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the four findings contained in our preceding audit report dated August 21, 2013. We determined that FSU satisfactorily addressed these findings.

Findings and Recommendations

Information Systems Security and Control

Background

Frostburg State University's (FSU) Office of Networking and Telecommunications and Office of Information Technology provide technical information systems support to FSU through the operation and maintenance of campus-wide administrative applications, such as the human resources system, the student administration system, and the financial system. The Office of Information Technology also operates an integrated administrative and academic computer network, which provides connections to multiple servers used for administrative applications and related databases. The campus network also has connections to the Internet, the Maryland Research and Education Network, and certain University System of Maryland (USM) institutions and includes a firewall, other network traffic filtering devices, and an extensive campus wireless network.

Finding 1
FSU did not ensure that capabilities assigned to individuals on the financial management systems were adequately restricted.

Analysis

FSU did not ensure that capabilities assigned to individuals on its financial management systems were adequately restricted to prevent improper student account and financial aid transactions. Our review of system capabilities assigned to 142 active users disclosed that some users were assigned unnecessary or inappropriate system capabilities.

- Our review of nine critical functions related to student accounts determined that three system users were assigned unnecessary or inappropriate access to one or more of those functions. For example, one of the users with the capability to process non-cash credits was responsible for reviewing and approving these non-cash credits. According to FSU records, non-cash credits processed during fiscal year 2015 totaled approximately $3.9 million.

- Our review of 15 critical functions related to student financial aid determined that 6 system users were assigned unnecessary or inappropriate access to one or more of those functions. For example, these 6 users could modify student financial data used to determine if a student is eligible for federal aid and also indicate that the information had been verified. The 6 users also had the

capability to create and modify student financial aid budgets, which establish a maximum amount a student can receive in aid, without supervisory review.

- FSU had not established adequate controls over the termination of user accounts. Specifically, user accounts for 6 individuals who were previously employed by FSU remained active for periods of 1 to 16 months after the individuals left FSU employment. In addition, for one other account, an existing employee received a new account while unnecessarily retaining access to the old account.

USM's *Information Technology Security Standards* specify that institutions are responsible for ensuring that access rights reflect employee status, including changes in employee status. In addition, institutions must segregate various functions, such as processing and authorizing business transactions, to ensure the appropriate separation of duties for system users or implement compensating controls to mitigate the risk.

Recommendation 1
We recommend that FSU

a. restrict user access capabilities for critical functions to those employees who require such capabilities for their job duties, including those noted above, in a manner that ensures a proper segregation of duties and independent review and approval of critical transactions; and

b. establish procedures to ensure that all user accounts are terminated timely.

Finding 2
Procedures for maintaining and securing numerous FSU workstations were not sufficient.

Analysis
Procedures for maintaining and securing numerous FSU workstations were not sufficient.

- Certain workstations were configured with users having administrative rights. Administrative rights are the highest permission level that can be granted and allow users to install software and change configuration settings. Our test of ten workstations disclosed that eight employees' user accounts were inappropriately defined with administrative rights rather than with user rights. We were advised by FSU personnel that faculty and staff are generally given

administrative rights on their workstations. As a result, if the workstations used by accounts with administrative rights 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 computers tested 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, FSU had not updated all of its computers for these patches. For example, of 13 computers tested for one of these software products, we noted that 7 computers were running older versions of this software that had not been updated for periods ranging from 2 to 15 months.

- The malware protection software used to protect FSU workstations was not properly configured to limit users' capabilities. Specifically, users of all eight workstations tested could disable malware protection software features that would render the software unable to protect against malware threats.

- Although FSU used an enterprise-wide management tool to administer malware protection software on its computers, FSU did not use the management capabilities of this tool to verify that the malware protection software and related definition files were up-to-date on its computers. In this regard, FSU personnel advised that regular reviews of the management tool's dashboard and reports were not performed. Specifically, 10 of 11 computers tested did not have a current version of the malware protection software installed and 2 of these 10 computers had outdated malware protection signatures which detect malware and prevent it from attacking the computers.

The USM *Information Technology Security Standards* state that institutions must install software to protect systems from malicious programs such as viruses, trojans, and worms. The software should be configured to update signatures regularly.

Recommendation 2
We recommend that FSU

a. ensure that administrator rights on workstations are restricted to network administrators;
b. promptly install all critical security-related software updates on its computers;

c. configure its malware protection software so that users cannot disable the settings which allow users to override and modify default security controls established by management; and

d. use its malware protection enterprise-wide management tool to regularly confirm that all computers are configured with anti-malware software that is operating properly, up-to-date and has current anti-malware signatures. These regular reviews should be documented and retained for future reference.

Finding 3
Sensitive personally identifiable information was not appropriately safeguarded.

Analysis

Sensitive personally identifiable information (PII) was stored in two critical databases in clear text. Specifically, we noted that, as of August 18, 2015, these two databases contained sensitive PII for 131,488 and 134,042 unique individuals in clear text. This included the individuals' full names, dates of birth, addresses, and social security numbers. 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. The 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 the USM encryption standards must be used.

Recommendation 3

We recommend that FSU:

a. perform an 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 4
Access and monitoring controls over two databases and applications were not sufficient to protect critical data.

Analysis
Access and monitoring controls over two databases and applications were not sufficient to protect critical data.

- Access to critical roles, tools, and permission lists used by the financial and student administration applications were not properly restricted. For example, we noted that four accounts were improperly assigned the financial application's administrator role as the related individuals did not require this capability to perform their job duties. As a result of this role assignment, these four accounts had unnecessary, full access to all of the financial application's menus, pages, and interfaces along with unnecessary use of critical administrative tools. The USM *IT Security Standards* state that institutions must implement and document processes to ensure that access rights reflect employee status.

- FSU did not log changes to the financial application's security settings relating to password controls, procurement cards, and critical security options. In addition, for the student administration application, FSU did not generate reports of logged changes to critical password settings. Furthermore, although critical student administration system database security events were properly logged, reports generated from the logged events were configured to exclude almost all of the critical logged security events. As a result, numerous significant security events were not reviewed for propriety. The USM IT Security Council *Guide for Security Event Logging* requires each institution to maintain appropriate audit trails of events and actions related to critical applications and data.

Recommendation 4
We recommend that the FSU

a. implement controls over the financial and student information system applications which properly restrict access to critical roles, tools, and permission lists;
b. log changes to critical application security settings;
c. generate reports of logged changes to critical application settings and regularly review these reports; and
d. configure the reports of logged database security events to include all significant security events.

Audit Scope, Objectives, and Methodology

We have conducted a fiscal compliance audit of the University System of Maryland (USM) – Frostburg State University (FSU) for the period beginning June 4, 2012 and ending June 30, 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 FSU'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 cash receipts, student accounts receivable, purchases and disbursements, student financial aid, payroll, and information technology systems. We also determined the status of the findings contained in our preceding audit report.

Our audit did not include certain support services provided to FSU by the USM Office. These support services (for example bond financing) are included within the scope of our audit of the USM Office. In addition, 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 FSU'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 components of USM.

To accomplish our audit objectives, our audit procedures included inquiries of appropriate personnel, inspection of documents and records, and observations of FSU'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 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 FSU's financial systems 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.

FSU'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 relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect FSU'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 FSU that did not warrant inclusion in this report.

The response from the USM Office, on behalf of FSU, 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 USM Office regarding the results of our review of its response.

APPENDIX

OFFICE OF THE CHANCELLOR

April 4, 2016

Mr. Thomas J. Barnickel III, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, MD 21201

Re: University System of Maryland –
Frostburg State University
Period of Audit: June 4, 2012 through
June 30, 2015

Dear Mr. Barnickel:

I have enclosed the University System of Maryland's responses to your draft report covering the examination of the accounts and records of the University System of Maryland – Frostburg State University. Our comments refer to the individual items in the report.

Sincerely Yours,

Robert L. Caret
Chancellor

Enclosures

cc:

Dr. Thomas L. Bowling, Ph.D., President, FSU
Mr. David C. Rose, Vice President for Administration and Finance, FSU
Mr. James L. Shea, Chair, University System of Maryland Board of Regents
Mr. Robert L. Page, Associate Vice Chancellor for Financial Affairs, USM Office
Mr. David Mosca, Director of Internal Audit, USM Office

1807 University of Maryland, Baltimore

1856 University of Maryland, College Park

1865 Bowie State University

1866 Towson University

1886 University of Maryland Eastern Shore

1898 Frostburg State University

1900 Coppin State University

1925 Salisbury University

1925 University of Baltimore

1925 University of Maryland Center for Environmental Science

1947 University of Maryland University College

1966 University of Maryland, Baltimore County

RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
FROSTBURG STATE UNIVERSITY
JUNE 4, 2012 TO JUNE 30, 2015

Information Systems Security and Control

Finding 1
FSU did not ensure that capabilities assigned to individuals on the financial management systems were adequately restricted.

Recommendation 1
We recommend that FSU

a. restrict user access capabilities for critical functions to those employees who require such capabilities for their job duties, including those noted above, in a manner that ensures a proper segregation of duties and independent review and approval of critical transactions; and

b. establish procedures to ensure that all user accounts are terminated timely.

University response

a. FSU has completed this recommendation effective March 2016.
b. FSU will restrict access and establish procedures to ensure all accounts are terminated timely. We plan to complete this recommendation by July 2016.

Finding 2
Procedures for maintaining and securing numerous FSU workstations were not sufficient.

Recommendation 2
We recommend that FSU

a. ensure that administrator rights on workstations are restricted to network administrators;

b. promptly install all critical security-related software updates on its computers;

c. configure its malware protection software so that users cannot disable the settings which allow users to override and modify default security controls established by management; and

d. use its malware protection enterprise-wide management tool to regularly confirm that all computers are configured with anti-malware software that is operating properly, up-to-date and has current anti-malware signatures. These regular reviews should be documented and retained for future reference.

RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
FROSTBURG STATE UNIVERSITY
JUNE 4, 2012 TO JUNE 30, 2015

University response

a. FSU will restrict administrator rights on workstations. We expect to be completed by June 18.
b. FSU has completed this recommendation effective January 2016.
c. FSU will complete this recommendation by May 2016.
d. FSU has completed this recommendation effective December 2015.

Finding 3
Sensitive personally identifiable information was not appropriately safeguarded.

Recommendation 3
We recommend that FSU:

a. perform an 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.

University response

FSU is in the process of strengthening its PII controls, and will fully complete all four recommendations by June 2018.

Finding 4
Access and monitoring controls over two databases and applications were not sufficient to protect critical data.

Recommendation 4
We recommend that the FSU

a. implement controls over the financial and student information system applications which properly restrict access to critical roles, tools, and permission lists;
b. log changes to critical application security settings;
c. generate reports of logged changes to critical application settings and regularly review these reports; and

RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
FROSTBURG STATE UNIVERSITY
JUNE 4, 2012 TO JUNE 30, 2015

d. configure the reports of logged database security events to include all significant security events.

University response

a. FSU has completed this recommendation effective September 2015.
b. FSU is preparing application code changes to meet this recommendation with an expected completion date of July 2016.
c. FSU will begin generation and review of these reports by July 2016.
d. FSU has completed this recommendation effective January 2016.

AUDIT TEAM

William R. Smith, CPA
Audit Manager

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

Evan E. Naugle
Senior Auditor

Eric Alexander, CPA, CISA
Christopher D. Jackson, CISA
Information Systems Senior Auditors

Wesley M. Elder, CPA
Christopher J. Fowler
Staff Auditors

Steven D. Bryant
Matthew D. Walbert
Information Systems Staff Auditors