

Audit Report

**University System of Maryland
Frostburg State University**

March 2007



OFFICE OF LEGISLATIVE AUDITS
DEPARTMENT OF LEGISLATIVE SERVICES
MARYLAND GENERAL ASSEMBLY

-
- This report and any related follow-up correspondence are available to the public through the Office of Legislative Audits at 301 West Preston Street, Room 1202, Baltimore, Maryland 21201. The office may be contacted by telephone at 410-946-5900, 301-970-5900, or 1-877-486-9964.
 - Electronic copies of our audit reports can be viewed or downloaded from our website at <http://www.ola.state.md.us>.
 - Alternate formats may be requested through the Maryland Relay Service at 1-800-735-2258.
 - The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at 410-946-5400 or 301-970-5400.
-



Karl S. Aro
Executive Director

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Bruce A. Myers, CPA
Legislative Auditor

March 20, 2007

Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Senator Nathaniel J. McFadden, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the University System of Maryland - Frostburg State University (FSU) for the period beginning July 1, 2002 and ending June 30, 2006.

Our audit disclosed that FSU's information systems were not adequately secured. For example, key administrative systems were not adequately protected from both internal and external exposures.

We also noted other internal control and recordkeeping deficiencies in the areas of purchasing, financial aid, procurement of goods and services, and equipment.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

Executive Summary	5
Background Information	7
Agency Responsibilities	7
Current Status of Findings From Preceding Audit Report	7
Findings and Recommendations	9
Information Systems Security and Control	
* Finding 1 – FSU’s Computer Network Was Not Adequately Secured	9
Finding 2 – Critical Systems Were Not Adequately Monitored and Controlled	10
Finding 3 – Network Account Controls and Backup Procedures Were Inadequate	11
Purchasing Transactions	
Finding 4 – Adequate Internal Control Was Not Established Over Certain Purchasing Transactions	12
Student Records	
Finding 5 – Proper Internal Control Had Not Been Established Over Student Records	12
Student Financial Aid	
Finding 6 – Reconciliations of Financial Aid Applied to Student Accounts With Federal Financial Aid Authorizations Were Not Always Performed	13
Procurement of Goods and Services	
Finding 7 – Questionable Purchases Were Made From One Vendor and Certain Services Were Procured Without Competitive Bids or Written Contracts	14
Equipment	
* Finding 8 – An Independent Control Account Was Not Maintained	15
Audit Scope, Objectives, and Methodology	17
Agency Response	Appendix

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

Executive Summary

Legislative Audit Report on University System of Maryland Frostburg State University (FSU) March 2007

- **FSU's information systems were not adequately secured. For example, key administrative systems were not adequately protected from both internal and external exposures.**

FSU should take the recommended corrective actions to improve security over its information systems.

- **Proper internal control was not established over the processing of certain purchasing transactions.**

Available security features should be used to establish independent online approval requirements for all critical purchasing transactions.

- **FSU did not adequately control and verify changes to critical student records including student grades and student residency status.**

FSU should adequately control and verify changes to critical student records.

- **FSU did not always perform reconciliations to ensure the proper amounts were recorded in the student accounts receivable records.**

FSU should periodically reconcile financial aid applied to student accounts with the related federal financial aid authorizations.

- **FSU made questionable purchases from one vendor and certain services were procured without competitive bids or written contracts.**

FSU should refer the matter concerning the questionable purchases to the Office of the Attorney General – Criminal Investigations Unit and, if determined appropriate, to the State Ethics Commission for review. FSU should also ensure that it is in compliance with established policies when procuring goods and services.

Background Information

Agency Responsibilities

Frostburg State University (FSU) is a comprehensive public institution of the University System of Maryland and operates under the jurisdiction of the System's Board of Regents. FSU offers an array of baccalaureate and master's 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 2006 semester totaled 4,910, including 4,252 undergraduate students and 658 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 2006 totaled approximately \$79 million, including a State general fund appropriation of approximately \$26 million.

Current Status of Findings From Preceding Audit Report

We reviewed the current status of the nine items from our preceding audit report dated January 24, 2003. We determined that FSU satisfactorily addressed seven of these findings. The remaining two findings are repeated in this report.

Findings and Recommendations

Information Systems Security and Control

Background

FSU's Office of Technology Services provides information systems support to FSU through the operation and maintenance of campus-wide administrative applications, such as the human resources/student administration and financial systems. The Office 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 includes separate email and file servers, Internet connectivity, a firewall and other network traffic filtering devices, and an extensive campus wireless network. FSU also maintains a website that functions as an entry point to many of its services.

Finding 1

FSU's computer network was not adequately secured.

Analysis

Key administrative systems (such as the financial and human resources/student administration application systems) were not adequately protected from both internal and external exposures as follows:

- Traffic from the Internet and untrusted portions of FSU's network (such as computer labs and third party organizations located on campus) could access critical administrative computers without being adequately filtered. A similar condition was commented upon in our preceding audit report.
- Numerous publicly accessible servers were located on the internal network rather than in a separate network zone to minimize security risks. These servers, which could potentially be compromised, exposed the internal network to attack from external sources. A similar condition was commented upon in our preceding audit report.
- Intrusion detection/prevention systems were not used to help protect critical portions of the FSU network. Intrusion/detection prevention systems gather and analyze network traffic to identify and/or to prevent network security breaches and attacks, and alert network administrators of these situations.

Recommendation 1

We again recommend that FSU assess risks from exposures to its computer network and implement appropriate security measures. Specifically, we recommend that FSU properly filter traffic from the Internet and untrusted portions of its network. We also recommend that FSU place all publicly accessible servers in a separate network zone to minimize security risks. Furthermore, we recommend that FSU implement intrusion detection/prevention systems for the critical portions of its network and that it monitor these systems and document its monitoring efforts.

Finding 2

Critical systems were not adequately monitored and controlled.

Analysis

Critical systems were not adequately monitored and controlled. Specifically, we noted the following conditions:

- Audit logging of application security events for FSU's financial and human resources/student administration applications was not enabled. In addition, many significant security events for the server hosting the human resources/student administration application were not logged. These security events include individual changes to system user access rights, roles, and permissions.
- Audit logging of database security events for the human resources/student administration database was also not enabled. This database includes security features which control access at the database level. The lack of logging and review of database security events could result in unauthorized or inappropriate changes to critical data which could go undetected.

As a result of these conditions, FSU was not in compliance with University System of Maryland's (USM) *Guidelines in Response to the State's IT Security Policy* dated April 2005, which requires that appropriate audit trails of events and actions related to critical applications and data be maintained, and that these logged actions and events be reviewed, and that the reviews be documented.

Recommendation 2

We recommend that FSU enable logging of critical security events for its key servers, applications and databases, and that reviews of the logs be performed, documented, and retained for subsequent verification.

Finding 3

Network account controls and backup procedures were inadequate.

Analysis

Network account controls and backup procedures were inadequate. Specifically, we noted the following conditions:

- Certain user account settings over critical systems were inadequate. For network user accounts, the account lockout feature was not used as required by the USM *Guidelines in Response to the State IT Security Policy*. In addition, numerous inactive non-student accounts defined to the network for at least 60 days had either never been used or had not been used for the 60 days that preceded our testing.
- FSU stored copies of backup files for its critical applications in a building adjacent to the facility housing the original files. With such close proximity, a disaster affecting both buildings could destroy both the original and backup data.

Recommendation 3

We recommend that FSU implement a network account lockout provision in accordance with the aforementioned USM *Guidelines* and that inactive accounts be disabled after 60 days of inactivity. We also recommend that FSU store backup copies of its critical files at an off-site, secure, environmentally controlled location.

Purchasing Transactions

Finding 4

Adequate internal control was not established over the processing of certain purchasing transactions.

Analysis

FSU did not fully use the available security features of its automated purchasing and accounts payable system to establish adequate internal control over certain purchasing transactions. Specifically, two employees could both initiate and approve purchase orders without being subject to independent online approval. In addition, these two employees could also receive the related goods or services, and one of the two employees had the ability to modify vendor data (for example, change a vendor's mailing address). Consequently, unauthorized purchases could be processed that may not be readily detected.

During fiscal years 2004 to 2006, purchase orders initiated and approved by the same employee totaled approximately \$280,000. According to the State's records, disbursement transmittals processed by FSU during fiscal year 2005 totaled approximately \$19.4 million.

Recommendation 4

We recommend that FSU use the available security features of its automated purchasing and accounts payable system by establishing independent online approval requirements for all purchasing transactions.

Student Records

Finding 5

Adequate internal control had not been established over certain FSU student records.

Analysis

FSU had not established adequate internal control over certain student records. Specifically, we noted that changes made to student grades and student residency status were not reviewed and approved by supervisory personnel. In this regard, output reports of changes to student grades and student residency status were not generated and verified to related source documents by supervisory personnel to ensure the propriety of such changes. Additionally, seven employees had the

ability to modify certain critical student data (such as student grades and student residency status) even though their job responsibilities did not require such access. According to FSU records, 515 grade changes and 31 residency status changes were processed during fiscal year 2006.

As a result of these conditions, unauthorized changes could be made to critical student records that may not be readily detected by FSU management.

Recommendation 5

We recommend that FSU generate output reports of changes made to student grades and student residency status and that, at least on a test basis, supervisory personnel verify and document changes made to related input documents. We also recommend that the ability to modify critical student data be limited to only those employees whose job responsibilities require such capability.

Student Financial Aid

Finding 6

Reconciliations of financial aid applied to student accounts with the related federal financial aid awards were not always performed.

Analysis

FSU did not always reconcile financial aid applied to student accounts with the related federal financial aid awards. Specifically, FSU did not perform such reconciliations for six of the seven types of federal financial aid (for example, Perkins Loans, Stafford Loans) to ensure that the proper amounts of financial aid were recorded in the student accounts receivable records. According to its records, FSU disbursed approximately \$20 million in federal financial aid to students during the 2005-2006 academic year.

Recommendation 6

We recommend that FSU periodically (such as monthly) reconcile financial aid applied to student accounts with the related federal financial aid authorizations, and that any resulting differences be investigated and resolved.

Procurement of Goods and Services

Finding 7

Questionable purchases were made from one vendor and certain services were procured without competitive bids or written contracts.

Analysis

FSU made questionable purchases from one vendor during fiscal years 2004 and 2005 and certain services were procured without competitive bids or written contracts. Specifically, FSU purchased computer accessories (such as wireless internet cards and printer ink cartridges) totaling approximately \$21,200 primarily for resale at the FSU Bookstore without obtaining competitive bids or entering into a campus-wide blanket contract. The company from which the items were purchased was owned by an individual who, at the time of the purchases, had a relationship with a family member of a former FSU senior management official.

The propriety of the aforementioned purchases totaling \$21,200 appears questionable since FSU personnel may not have acted impartially. Accordingly, we believe that this matter should be referred to the Office of the Attorney General – Criminal Investigations Division (CID) for its consideration since it is primarily responsible for investigating possible criminal conduct within State government and has prosecutorial authority. In addition, this situation potentially could be a violation of State ethics laws.

Additionally, FSU procured photocopier services, totaling approximately \$339,000, from another vendor during fiscal years 2004 to 2006 without soliciting competitive bids or entering into a campus-wide blanket contract. Rather, the services were procured by various FSU departments using corporate purchasing cards. FSU's *Procurement Policies and Procedures Manual* requires that procurements over \$5,000 be competitively bid and supported by written contracts and/or purchase orders to help ensure that the goods and services were obtained at the lowest available price.

Recommendation 7

We recommend that FSU refer the aforementioned questionable purchases to CID for its review. Pending the outcome of this review, we recommend that FSU determine if this matter should be referred to the State Ethics Commission for further review. Additionally, we recommend that FSU

comply with established procurement policies by soliciting competitive bids for procurements over \$5,000 and preparing written contracts and/or purchase orders when procuring goods and services.

Equipment

Finding 8

An independent control account was not maintained.

Analysis

FSU did not maintain an independent equipment control account. In this regard, FSU used the general ledger equipment account maintained in its automated accounting system as the equipment control account. However, the general ledger account was automatically updated using the transactions (such as purchases and disposals) entered in the automated detail equipment records. Consequently, the control account simply reflects the data recorded in the detail records rather than serving as an independent summary which can be reconciled to the detail records to help ensure that transactions are accurately recorded. A similar condition was commented upon in our preceding audit report.

The University System of Maryland's *Policy for Capitalization and Inventory Control* requires that an equipment control account be maintained and periodically reconciled to the aggregate balance of the detail records. According to FSU's records, the book value of its equipment, as of June 30, 2006, totaled approximately \$16.9 million.

Recommendation 8

We again recommend that FSU maintain an equipment control account independent of the detail records. We also again recommend that the control account be periodically reconciled with the aggregate balance of the detail records, and that any resulting differences be investigated and resolved.

Audit Scope, Objectives, and Methodology

We have audited the University System of Maryland (USM) – Frostburg State University (FSU) for the period beginning July 1, 2002 and ending June 30, 2006. The audit was conducted in accordance with generally accepted government auditing standards.

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. We also determined the current status of the findings included in our preceding audit report.

In planning and conducting our audit, we focused on the major financial-related areas of operations based on assessments of materiality and risk. Our audit procedures included inquiries of appropriate personnel, inspections of documents and records, and observations of FSU's operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives. Data provided in this report for background or informational purposes were deemed reasonable, but were not independently verified.

Our audit did not include certain support services (such as bond financing) provided to FSU by the USM Office. These support services are included within the scope of our audits of the USM Office. In addition, we did not audit FSU's federal financial assistance programs for compliance with federal 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.

Our audit scope was limited with respect to FSU's cash transactions because the Office of the State Treasurer was unable to reconcile the State's main bank accounts during the audit period. Due to this condition, we were unable to determine, with reasonable assurance, that all FSU cash transactions were accounted for and properly recorded on the related State accounting records as well as the banks' records.

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 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 the 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 USM regarding the results of our review of its response.

APPENDIX



OFFICE OF THE CHANCELLOR

March 16, 2007

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building
301 West Preston Street
Baltimore, MD 21201

**RE: University System of Maryland –
Frostburg State University
Audit Period: July 2, 2002 –
June 30, 2006**

Dear Mr. Myers:

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

Sincerely,

A handwritten signature in black ink that reads "W. E. Kirwan".

William E. Kirwan
Chancellor

Enclosure

WEK:mpk

cc: Dr. Jonathan Gibraltar
Mr. David Rose
Mr. Joseph F. Vivona
Mr. Robert L. Page
Mr. David Mosca
Mr. Clifford M. Kendall

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

1985
University of Maryland
Biotechnology Institute

Findings and Recommendations

Information Systems Security and Control

Finding 1

FSU's computer network was not adequately secured.

Recommendation 1

We again recommend that FSU assess risks from exposures to its computer network and implement appropriate security measures. Specifically, we recommend that FSU properly filter traffic from the Internet and untrusted portions of its network. We also recommend that FSU place all publicly accessible servers in a separate network zone to minimize security risks. Furthermore, we recommend that FSU implement intrusion detection/prevention systems for the critical portions of its network and that it monitor these systems and document its monitoring efforts.

Response

FSU has assessed risks from exposures to computer network and implemented appropriate security measures, except for the 3 student lab networks. These networks will be segmented by the campus firewall no later than June 1, 2007. Traffic is now being filtered from the Internet and un-trusted portions of the FSU network. Publicly accessible servers will be placed in a separate network zone. This process should be completed by April 2007. A new intrusion detection appliance was implemented on March 1, 2007.

Finding 2

Critical systems were not adequately monitored and controlled.

Recommendation 2

We recommend that FSU enable logging of critical security events for its key servers, applications and databases, and that reviews of the logs be performed, documented, and retained for subsequent verification.

Response

FSU plans to implement the use of a tool that can be used to search the event logs of several different computers for specific events. This tool can be configured to search the logs in a very detailed fashion. These reports will be reviewed and retained electronically by mid – April 2007.

Finding 3

Network account controls and backup procedures were inadequate.

Recommendation 3

We recommend that FSU implement a network account lockout provision in accordance with the aforementioned USM *Guidelines* and that inactive accounts be disabled after 60 days of inactivity. We also recommend that FSU store backup copies of its critical files at an off-site, secure, environmentally controlled location.

Response

A procedure has been implemented to identify accounts that have not been used for 60+ days. Once identified, those accounts are disabled. Back-up tapes are now being stored in a safe located in the University Police Department building.

Purchasing Transactions**Finding 4**

Adequate internal control was not established over the processing of certain purchasing transactions.

Recommendation 4

We recommend that FSU use the available security features of its automated purchasing and accounts payable system by establishing independent online approval requirements for all purchasing transactions.

Response

The University has removed the ability to initiate purchase orders and the vendor modification abilities from the employees cited. The security has been modified to prohibit accounts payable control group update capability from clerks entering vouchers.

Student Records

Finding 5

Adequate internal control had not been established over certain FSU student records.

Recommendation 5

We recommend that FSU generate output reports of changes made to student grades and student residency status and that, at least on a test basis, supervisory personnel verify and document changes made to related input documents. We also recommend that the ability to modify critical student data be limited to only those employees whose job responsibilities require such capability.

Response

Non-cash credits are independently verified upon posting by a Billing Office supervisor that is not entering the transaction. The ability to modify critical student data has been removed from the employees in the Billing Office and Registrar Office whose job responsibilities do not require access to perform their job duties. Monthly reports are being generated to verify changes to student grades and student residency status on a test basis by supervisory personnel.

Student Financial Aid

Finding 6

Reconciliations of financial aid applied to student accounts with the related federal financial aid awards were not always performed.

Recommendation 6

We recommend that FSU periodically (such as monthly) reconcile financial aid applied to student accounts with the related federal financial aid authorizations, and that any resulting differences be investigated and resolved.

Response

The Financial Aid Office will continue to periodically reconcile financial aid applied to student accounts with the related federal financial aid authorizations, and resulting differences will be investigated and resolved. Effective immediately the Financial Aid Office will attach the related federal financial aid authorizations to the reconciliations.

Procurement of Goods and Services

Finding 7

Questionable purchases were made from one vendor and certain services were procured without competitive bids or written contracts.

Recommendation 7

We recommend that FSU refer the aforementioned questionable purchases to CID for its review. Pending the outcome of this review, we recommend that FSU determine if this matter should be referred to the State Ethics Commission for further review. Additionally, we recommend that FSU comply with established procurement policies by soliciting competitive bids for procurements over \$5,000 and preparing written contracts and/or purchase orders when procuring goods and services.

Response

The University will continue to stringently endeavor to comply with procurement policies for areas not excluded from the policies. The questionable purchases noted have been referred to the Office of Attorney General for their review.

Equipment

Finding 8

An independent control account was not maintained.

Recommendation 8

We again recommend that FSU maintain an equipment control account independent of the detail records. We also again recommend that the control account be periodically reconciled with the aggregate balance of the detail records, and that any resulting differences be investigated and resolved.

Response

The FSU Accountant for Asset Management has established a separate account in spreadsheet format stating the balances of the equipment purchases, disposals and final totals for each month. This account will then be reconciled with the detail records from Asset Management. Periodically this summary will be reviewed and confirmed by someone other than the Asset Management Accountant. In addition, the supervisor will review and approve the reconciliation.

AUDIT TEAM

Mark A. Ermer, CPA

Audit Manager

Stephen P. Jersey, CPA, CISA

A. Jerome Sokol, CPA

Information Systems Audit Managers

Lisa M. Pawlowski, CFE

Senior Auditor

R. Brendan Coffey, CPA

Edwin L. Paul, CPA

Information Systems Senior Auditors

Deanna P. Leedy

Kelly A. Morgan

Staff Auditors