Audit Report

# University System of Maryland
# University of Maryland Eastern Shore

January 2008

**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.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Bruce A. Myers, CPA
Legislative Auditor

January 24, 2008

Senator Verna L. Jones, Co-Chair, Joint Audit Committee
Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the University System of Maryland – University of Maryland Eastern Shore (UMES) for the period beginning September 20, 2004 and ending May 31, 2007.

Our audit disclosed that procedures and controls for the UMES' information systems need to be improved. For example, the computer network was not adequately secured and controls on its firewall need improvement. Also, UMES did not have an information technology disaster recovery plan.

We also noted other internal control and recordkeeping deficiencies in the areas of student accounts receivable and equipment.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

# Table of Contents



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

# Background Information

## Agency Responsibilities

The University of Maryland Eastern Shore (UMES) is a comprehensive public institution of the University System of Maryland and operates under the jurisdiction of the System's Board of Regents. UMES offers an array of baccalaureate programs in both traditional arts and sciences, and in applied professional fields, as well as select professionally-oriented graduate programs and doctoral programs. Student enrollment for the Spring 2007 semester totaled 3,779, including 3,355 undergraduate students and 424 graduate students. UMES' 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, UMES' revenues for fiscal year 2007 totaled approximately $104 million, including a State general fund appropriation of approximately $28.6 million.

## Current Status of Findings From Preceding Audit Report

Our audit included a review to determine the current status of the 16 findings contained in our preceding audit report dated August 22, 2005. We determined that UMES satisfactorily addressed 14 of these findings. The remaining 2 findings have been combined into one finding and are repeated in this report.

# Findings and Recommendations

## Information Systems Security and Control

### Background

The University of Maryland Eastern Shore's (UMES) Administrative Computing, Information Technology, and Academic Computing units provide information technology support to UMES through the operation and maintenance of campus-wide administrative applications, such as the Student Administration system. These units also operate an integrated administrative and academic computer network, which provides connections to multiple servers used for administrative and academic purposes. The campus network also includes separate email and file servers, Internet connectivity, and a firewall. In addition, UMES connects to the University of Maryland Academic Telecommunications System network to send and receive data to and from other University System of Maryland institutions.

**Finding 1**
**UMES' computer network was not adequately secured and controls on its firewall need improvement.**

### Analysis

Adequate security measures had not been established to protect UMES' critical network devices and administrative systems from external and internal threats. Specifically, we noted the following conditions:

- Numerous publicly accessible servers were located on the internal network rather than in a separate network zone to minimize security risks. These publicly accessible servers, which could potentially be compromised, exposed the internal network to attack from external sources. The State of Maryland Department of Budget and Management's *Information Technology Security Policy and Standards* stipulates that all publicly accessible servers be placed in a neutral network zone.

- Key administrative systems were not adequately protected from untrusted portions of the UMES network. Specifically, numerous computer labs spread throughout the campus had unnecessary network level access to critical campus administrative resources.

- Firewall rules allowed numerous unnecessary connections to portions of the UMES' internal network, placing various network devices at risk. For example, unnecessary access to the entire UMES internal network was allowed from the Internet over several ports.

Similar conditions were commented upon in our prior audit report.

**Recommendation 1**
**We again recommend that UMES improve security over its network and firewall. Specifically, we made detailed recommendations, which if implemented, should provide for adequate security over its network.**

**Finding 2**
**Controls over critical network devices need improvement.**

**Analysis**
Controls over critical network devices need improvement. Specifically, we noted the following conditions:

- Individuals could gain unnecessary, administrative access to a critical core network device by using a default password for the device's remote management service. Also, the same service did not use a secure communications protocol. Furthermore, the network device's operating software included two default accounts which were not used but were not disabled and password controls were inadequate.

- Network personnel were not sent alerts for certain significant security events identified by the UMES firewall. Also, we were advised that the log files for the UMES' firewall and intrusion detection system were regularly reviewed; however, these reviews were not documented. Accordingly, assurance did not exist that adequate monitoring procedures were performed to detect and address network attacks.

**Recommendation 2**
**We recommend that administrative access to critical network devices be limited to only those individuals requiring such access and that adequate password controls be established for accessing these devices. We further recommend that remote management services which access and monitor critical network devices use only secure communications protocols. In addition, we recommend that alerts be sent to network administrators for**

**significant security events detected by the UMES firewall. Finally, we recommend that logs for all critical network devices be reviewed on a regular basis and that these reviews be documented and retained for reference purposes.**

**Finding 3**
**Controls over a critical UMES application database and program changes need improvement.**

**Analysis**
Controls over the UMES student administration application database and production program changes, for all applications, need improvement. Specifically, we noted the following conditions:

- A default administrative database account had unnecessary but full access to the student administration application database. Since this account includes local server administrators by default, anyone who is granted or obtains local administrator privileges on the database server would have full administrative access to this database and could perform unauthorized modifications to critical data.

- Production program changes were implemented without generating a report comparing the modified and original versions of the computer programs. Such comparative reports allow supervisory information systems staff to review and approve specific changes to program code. As a result, there was a lack of assurance that the programs moved into production accurately reflected only the changes that should have occurred.

**Recommendation 3**
**We recommend that access to all critical components of the UMES student administration database be limited to personnel whose job duties require such capabilities. We also recommend that information systems personnel, independent of the program change process, perform comparisons between original and modified versions of computer programs, and that supervisory information systems personnel review and approve the reports of program code differences generated by this comparison and document such reviews.**

**Finding 4**
**UMES did not have an information technology disaster recovery plan.**

**Analysis**
UMES did not have an information technology disaster recovery plan for recovering its computing operations from disaster scenarios (for example, a fire). Key requirements in a recovery plan address recovery strategies involving alternate sites, network connectivity and restoring applications, as well as rules and responsibilities of designated critical personnel, application inventories prioritized for recovery, and periodic disaster recovery plan testing. In accordance with the Department of Budget and Management's *IT Disaster Recovery Guidelines*, a complete information systems disaster recovery plan should, at a minimum, address the aforementioned items. Finally, without a complete disaster recovery plan, a disaster could cause significant delays (for an undetermined period of time) in restoring operations above and beyond the expected delays that would exist in a planned recovery scenario.

**Recommendation 4**
**We recommend that, in accordance with the aforementioned *IT Disaster Recovery Guidelines*, UMES develop and implement a comprehensive information systems disaster recovery plan that covers UMES' computing operations. We also recommend that, at a minimum, the plan address the items noted above.**

## Student Accounts Receivable

**Finding 5**
**Internal controls over the processing of certain non-cash credit adjustments were not adequate.**

**Analysis**
Adequate controls had not been established over the processing of certain non-cash credits. Independent verifications of non-cash credits related to housing and board were not always documented. Under these conditions, improper non-cash credit adjustments could be recorded to student accounts without detection. According to UMES' records, housing and board related non-cash credits for the fall 2006 semester totaled approximately $1.1 million.

**Recommendation 5**
**We recommend that an employee independent of the non-cash credit adjustment processing and approval procedures verify output reports of recorded adjustments with related, authorized source documents and that this verification be documented.**

**Finding 6**
**Adequate internal controls had not been established over certain UMES student records.**

**Analysis**
UMES had not established adequate internal control over certain student records. Specifically, changes made to student residency status were not adequately reviewed and approved by supervisory personnel. Although output reports of changes to student residency status were generated, UMES personnel did not verify the changes to related source documents to ensure the propriety of such changes. According to UMES records, 38 residency status changes were processed during the fall 2006 semester, and the residency status was changed from out-of-state to in-state in 28 of these cases. Any improper change of residency from out-of-state to in-state would reduce the amount of tuition collected by UMES. As a result of this condition, unauthorized changes could be made to critical student records that may not be readily detected by UMES management.

**Recommendation 6**
**We recommend that changes to residency status be verified by reviewing supporting documentation and that this verification be documented.**

## Equipment

**Finding 7**
**Inventory records were not always properly maintained.**

**Analysis**
UMES did not adequately maintain its detail equipment records. As of July 1, 2007, the value of equipment as recorded in UMES records, totaled $14.9 million. Our test of 10 acquisitions, totaling approximately $520,000, purchased during fiscal years 2006 and 2007, disclosed that 3 of the purchases (including a video

editing machine and kitchen equipment), totaling approximately $56,300, were not recorded in the equipment records as required by the University System of Maryland's *Policy for Capitalization and Inventory Control*.

**Recommendation 7**
**We recommend that UMES ensure that all equipment is properly recorded in its detail records.**

# Audit Scope, Objectives, and Methodology

We have audited the University System of Maryland (USM) – University of Maryland Eastern Shore (UMES) for the period beginning September 20, 2004 and ending May 31, 2007. 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 UMES' 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 UMES' 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 provided to UMES by the USM Office (such as endowment accounting) and by the University of Maryland, College Park (such as processing vendor payment transmittals and payroll). These support services are included within the scope of our audits of the USM Office and the University of Maryland, College Park, respectively. In addition, we did not audit UMES' 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 UMES' cash transactions because the Office of the State Treasurer was unable to reconcile the State's main bank accounts during a portion of the audit period. Due to this condition, we were unable to determine, with reasonable assurance, that all UMES' cash transactions prior to July 1, 2005 were accounted for and properly recorded on the related State accounting records as well as the banks' records.

UMES' 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 UMES' 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 UMES that did not warrant inclusion in this report.

The response from the USM Office, on behalf of UMES, 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

January 22, 2008

Mr. Bruce A. Myers, CPA
Legislative Auditor
Office of Legislative Audits
State Office Building, Room 1202
301 West Preston Street
Baltimore, MD 21201

RE: University System of Maryland –
University of Maryland Eastern Shore
Audit Period: September 20, 2004 and
ending May 31, 2007

Dear Mr. Myers:

I have enclosed the University System of Maryland's reponses to your draft report covering the examination of the accounts and records of the University of Maryland Eastern Shore. Our comments refer to the individual items in the report.

Sincerely,

William E. Kirwan
Chancellor

WEK:mk
Enclosures

cc: Dr. Thelma B. Thompson, President, UMES
Mr. Clifford M. Kendall, Chair, Board of Regents
Mr. Kevin M. O'Keefe, Chair, MHEC
Dr. James E. Lyons, Sr., Secretary of Higher Education, MHEC
Mr. Robert Page, Comptroller, 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
1985 University of Maryland Biotechnology Institute

# University of Maryland Eastern Shore
## Audit Responses
## Period of Audit: September 20, 2004 – May 31, 2007
## Findings and Recommendations

## Information Systems Security and Control

**Finding 1**
**UMES' computer network was not adequately secured and controls on its firewall need improvement.**

**Recommendation 1**
**We again recommend that UMES improve security over its network and firewall. Specifically, we made detailed recommendations, which if implemented, should provide for adequate security over its network.**

***Response***
**UMES will implement security measures for the network and firewall that will increase the overall security for the campus infrastructure.**

**Finding 2**
**Controls over critical network devices need improvement.**

**Recommendation 2**
**We recommend that administrative access to critical network devices be limited to only those individuals requiring such access and that adequate password controls be established for accessing these devices. We further recommend that remote management services which access and monitor critical network devices use only secure communications protocols. In addition, we recommend that alerts be sent to network administrators for significant security events detected by the UMES firewall. Finally, we recommend that logs for all critical network devices be reviewed on a regular basis and that these reviews be documented and retained for reference purposes.**

***Response***

**UMES has implemented new password controls over its network devices and has started monitoring alerts from the firewall. We will also start reviewing and signing off on all network device and firewall logs by March 31, 2008.**

**Finding 3**

**Controls over a critical UMES application database and program changes need improvement.**

**Recommendation 3**

**We recommend that access to all critical components of the UMES student administration database be limited to personnel whose job duties require such capabilities. We also recommend that information systems personnel, independent of the program change process, perform comparisons between original and modified versions of computer programs, and that supervisory information systems personnel review and approve the reports of program code differences generated by this comparison and document such reviews.**

***Response***

**UMES has limited access to the PeopleSoft database to include only the required job titles. UMES will also implement the proper change controls in order to ensure the integrity of the software development lifecycle.**

**Finding 4**

**UMES did not have an information technology disaster recovery plan.**

**Recommendation 4**

**We recommend that, in accordance with the aforementioned *IT Disaster Recovery Guidelines*, UMES develop and implement a comprehensive information systems disaster recovery plan that covers UMES' computing operations. We also recommend that, at a minimum, the plan address the items noted above.**

***Response***

**UMES has created a DR committee that meets on a regular basis. This committee will draft and have approved a complete disaster recovery plan by June 30, 2008.**

## Student Accounts Receivable

**Finding 5**
**Internal controls over the processing of certain non-cash credit adjustments were not adequate.**

**Recommendation 5**
**We recommend that an employee independent of the non-cash credit adjustment processing and approval procedures verify output reports of recorded adjustments with related, authorized source documents and that this verification be documented.**

***Response***
**UMES agrees that an employee independent of the housing and board adjustment process and approval procedures, verify on a test basis, the output reports of recorded adjustments with related authorized source documents. The administrative assistant will perform this verification and document it. This change is effective immediately.**

**Finding 6**
**Adequate internal controls had not been established over certain UMES student records.**

**Recommendation 6**
**We recommend that changes to residency status be verified by reviewing supporting documentation and that this verification be documented.**

***Response***
**UMES fully agrees with this recommendation. Effective immediately, changes to residency status will be verified and documented by reviewing, on a test basis, supporting documentation.**

## Equipment

**Finding 7**
**Inventory records were not always properly maintained.**

**Recommendation 7**
**We recommend that UMES ensure that all equipment is properly recorded in its detail records.**

***Response***
**UMES fully agrees that these items were not tagged and recorded in our inventory program. Although our program is designed to identify all equipment subcodes and report them to the inventory accountant to record and tag, it had not been programmed to identify vehicles. The program will be modified to identify all equipment subcodes, as well as vehicles purchased subcodes. In addition to the program that generates a report of equipment purchases, the procurement office supplying a copy of the equipment purchase orders to the inventory accountant, the daily visits to the central receiving office by the inventory accountant, another step will be added to our Accounts Payable review on invoices done by the General Ledger Accountant. Each invoice will be reviewed for the item purchased, subcode used and dollar amount before it is sent to College Park for payment processing. For each invoice that meets potential equipment purchases of $500 or greater, the General Ledger Accountant will make a coy of the invoice and give it to the Inventory Accountant. If it is an incorrect subcode, then a journal voucher would be done that day to reclassify to the proper account. This effort will be fully implemented by June 30, 2008.**

## AUDIT TEAM

**Edward L. Shulder, CPA**
Audit Manager

**Stephen P. Jersey, CPA, CISA**
Information Systems Audit Manager

**Catherine M. Easter**
Senior Auditor

**R. Brendan Coffey, CPA**
**Edwin L. Paul, CPA**
Information Systems Senior Auditors

**R. Frank Abel, CPA, CFE**
**Nichole M. Becker**
**Ken H. Johanning, CFE**
Staff Auditors