

Audit Report

University System of Maryland Office

January 2009



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

January 7, 2009

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 Office for the period beginning January 13, 2005 and ending January 31, 2008. The Office develops system-wide policies and procedures; monitors academic, financial, and administrative performance; and provides management information for planning and decision-making to the 13 institutions and 2 regional higher education centers of the University System of Maryland.

Our audit disclosed that, in July 2005, the Office, with the consent of the System's Board of Regents, transferred approximately \$197 million in endowment funds to the University of Maryland Foundation (UMF). The University System of Maryland (USM) entered into an agreement which provided that the Foundation invest the funds on its behalf. Although the agreement contained certain safeguards related to these funds, our audit disclosed that the Office did not adhere to certain of these requirements. For example, the agreement provided that UMF should invest the funds in accordance with the investment policies adopted by its Investment Committee and by the System's Board of Regents; however, as of August 28, 2008, such policies had not been developed.

We also noted that controls over critical University of Maryland Academic Telecommunications System (UMATS) management servers and network devices were inadequate. In addition, the Office's internal computer network was not adequately protected from security risks related to wireless connections, and sensitive personal and financial information for thousands of prospective USM students was unnecessarily stored on a publicly accessible server. The Office also did not have a comprehensive information technology disaster recovery plan.

Finally, the Office had not established adequate internal controls over cash receipts and equipment.

An Executive Summary of our findings can be found on page 5. The Office'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 Office.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

Executive Summary	5
Background Information	7
Agency Responsibilities	7
Audit of the System’s Basic Financial Statements	7
Status of Findings From Preceding Audit Report	7
Findings and Recommendations	9
Transfer of Endowment Funds	
Finding 1 – Certain Significant Provisions Related to the Transfer of Endowment Funds Were Not Adhered to	9
Cash Receipts	
* Finding 2 – Cash Receipts Were Not Adequately Controlled	11
University of Maryland Academic Telecommunications System	
* Finding 3 – Controls on Critical Management Servers Were Inadequate	12
* Finding 4 – Administration and Monitoring Controls for Critical Network Devices Were Inadequate	13
Finding 5 – The Internal Computer Network Was Not Adequately Protected from Security Risks Related to Wireless Connections	14
Finding 6 – Sensitive Personal and Financial Information for Prospective Students Was Stored on a Publicly Accessible Server	15
Finding 7 – A Complete Information Technology Disaster Recovery Plan Did Not Exist	15
Equipment	
Finding 8 – Controls Over Equipment at Two Locations Were Inadequate	16
Audit Scope, Objectives, and Methodology	19
Agency Response	Appendix

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

Executive Summary

Legislative Audit Report on University System of Maryland Office January 2009

- **Certain significant provisions of an agreement to transfer \$197 million in endowment funds to the University of Maryland Foundation (UMF) for investment were not adhered to. For example, investment policies were not adopted by the Office for use by the UMF, and the University System of Maryland (USM) was not identified as the third-party beneficiary in the contract.**

The Office should adopt investment policies and ensure that the UMF is investing endowment funds in accordance with those policies. The Office should also ensure that the USM is identified as a third-party beneficiary on UMF endowment investments.

- **Adequate accountability and control had not been established to ensure that certain collections were restrictively endorsed and recorded immediately upon receipt, and were otherwise controlled. At one location, the same employee that received the cash receipts also recorded the amounts in the accounts receivable records, and there were no independent verifications performed to ensure that the collections were deposited.**

The Office should ensure that all checks are immediately restrictively endorsed and deposited, and that employee duties are appropriately separated.

- **Controls over critical University of Maryland Academic Telecommunications System (UMATS) management servers and network devices were not adequate. For example, unnecessary services were enabled on a critical server, fiber optic transmission devices were not adequately restricted and secured by passwords, and security event monitoring was inadequate.**

The Office should take the recommended actions to establish adequate controls over critical management servers and network devices.

- **The internal computer network was not adequately protected from security risks related to wireless connections.**

The Office should adjust its network to require that wireless connections by employees be subject to user authentication and encryption, and that wireless connections by anyone else be restricted to the Internet.

- **Sensitive personal and financial information for thousands of prospective USM students was unnecessarily stored on a publicly accessible server.**

The Office should remove sensitive personal and financial data from the publicly accessible server or encrypt the data and store it on an internal server.

- **A comprehensive information technology disaster recovery plan did not exist.**

The Office should develop and implement a comprehensive plan that addresses the requirements of the Department of Budget and Management's *Information Technology Disaster Recovery Guidelines*.

Background Information

Agency Responsibilities

The University System of Maryland Office develops system-wide policies and procedures; monitors academic, financial, and administrative performance; and provides management information for planning and decision-making to the 13 institutions and 2 regional higher education centers of the University System of Maryland. The Office oversees the development and management of the University System of Maryland's two regional higher education centers: the Universities at Shady Grove and the University System of Maryland at Hagerstown. The Office also serves as the staff to the Board of Regents.

In addition, the Office serves as the host institution for an operating unit that supports the University of Maryland Academic Telecommunications System (UMATS). The UMATs network provides statewide telecommunications, such as Internet access and interactive video network, to all USM institutions.

According to the State's records, total Office expenditures were approximately \$27.5 million during fiscal year 2008.

Audit of the System's Basic Financial Statements

An independent accounting firm is engaged by the Office for the purpose of expressing an opinion on the System's financial statements each year. In the related audit reports for the fiscal years ended June 30, 2005, June 30, 2006, and June 30, 2007, the firm stated that the basic financial statements presented fairly, in all material respects, the financial position of the System, and the respective changes in financial position and cash flows for the years then ended, in conformity with accounting principles generally accepted in the United States.

Status of Findings From Preceding Audit Report

We reviewed the status of the nine findings included in our preceding audit report dated September 12, 2005. We determined that the Office satisfactorily addressed seven of these findings. The remaining two findings are repeated in this report and appear as three findings.

Findings and Recommendations

Transfer of Endowment Funds

Finding 1

Certain significant contract provisions related to the transfer of approximately \$197 million in endowment funds by the Office to the University of Maryland Foundation for investment were not adhered to.

Analysis

Certain significant contract provisions related to the transfer of approximately \$197 million in endowment funds by the Office in July 2005 to the University of Maryland Foundation (UMF) for investment were not adhered to. Specifically, on July 1, 2005, the University System of Maryland (USM) entered into an agreement with the UMF and, in accordance with the Board of Regents' approval, authorized the Office to transfer \$197 million in endowment funds to the UMF to be invested on its behalf. The funds transferred represented all monies in an endowment of the USM known as the Common Trust Fund (CTF). The CTF generally comprises restricted funds received from donors by the Office and various USM institutions. Under the agreement, which was deemed by legal counsel to the General Assembly to be permissible under State law, assets of the CTF and the UMF are commingled and are invested. Earnings or losses are allocated based on the proportion of assets invested. The agreement is for a five-year term with continuous, automatic two-year renewal periods. According to the records of the Office, the CTF was valued at approximately \$235 million and \$208 million as of June 30, 2008 and September 30, 2008, respectively. During fiscal years 2006, 2007, and 2008, the Office paid approximately \$1.6 million in management fees to the UMF. Our review disclosed the following conditions:

- Although the aforementioned agreement (dated July 1, 2005) provides that the UMF shall invest the CTF in accordance with the investment policies adopted by UMF's Investment Committee and the System's Board of Regents, we were advised by Office management that, as of August 28, 2008, such policies had not been developed. In this regard, State law enacted July 1, 2004, exempted the Office from certain requirements related to the procurement of services for managers of the investment of endowment assets, subject to policies adopted by the Board of Regents. The law also required that, by September 1, 2004, the Board was to report to the State Comptroller and the State Treasurer on the management and investment policies and procedures that the Board had adopted to implement the law. However, as previously mentioned, such policies have not been established. Such policies are needed

so that the Board's investment strategies and goals, including appropriate risks and safeguards, are clearly defined and implemented.

- The CTF funds are commingled with UMF endowment funds as allowed by the agreement. The agreement also states that the UMF shall use its best efforts with respect to future contracts between it and the investment custodian and manager(s) to include a provision specifying that the USM is a third-party beneficiary under the contract; this provision would provide the USM with a direct cause of action against the custodian and manager(s) in the event of a default under the contract. However, we were advised by Office management that, as of August 28, 2008, the USM had not been named as a third-party beneficiary under such contracts.
- State law requires that, on or before November 1st of each year, the Board submit to the Governor, the State Comptroller, the State Treasurer, and the General Assembly, an annual investment performance report comparing the various components of the Office's gift and endowment investment portfolio to appropriate benchmarks. As of April 2008, these reports had not been prepared and submitted for fiscal years 2006 and 2007. Subsequent to our request, the fiscal year 2006 and 2007 investment performance reports were prepared and submitted in May 2008.

Recommendation 1

We recommend that the Office adopt investment policies as required by the aforementioned agreement and by State law, and provide the policies to the State Comptroller and State Treasurer, as required. We also recommend that the Office ensure that UMF is investing the CTF in accordance with the policies established. We further recommend that, where possible and appropriate, the Office take steps to include in this and future contracts a provision specifying the USM as a third-party beneficiary on UMF endowment investments. Finally, we recommend that future annual investment performance reports be prepared and submitted timely as required by law.

Cash Receipts

Finding 2

Cash receipts were not adequately controlled.

Analysis

Collections received by the Office were not properly accounted for and controlled. The Finance Office initially received and processed a majority of the \$3.1 million in cash receipts received during fiscal year 2008. These receipts also included collections initially received from other Office units which were forwarded to the Finance Office for further processing. Our review disclosed the following conditions:

- Certain checks initially received through the mail by other Office units were not restrictively endorsed “for deposit only” or immediately recorded until after they were transferred to the Finance Office for further processing. In addition, checks initially received by the Finance Office on certain days of the week were not recorded until after the deposit was made. Similar conditions regarding the lack of immediate restrictive endorsement and initial recordation were commented upon in our two preceding audit reports.
- At one unit location, with collections totaling approximately \$507,000 during fiscal year 2008, the same employee routinely received cash receipts and was also involved in recording the amounts in the accounts receivable records. This condition was noted with respect to a different unit in our preceding audit report. This employee was also responsible for verifying that collections received were subsequently transferred intact to the University of Maryland, College Park for further processing and deposit.

As a result of these conditions, errors or irregularities could occur without detection.

Recommendation 2

We again recommend that all checks be restrictively endorsed “for deposit only” and recorded immediately upon receipt. We also again recommend that an employee independent of the cash receipts function update the accounts receivable records. Furthermore, we recommend that an employee independent of the cash receipts function verify that all recorded collections are subsequently deposited. We advised the Office on establishing the necessary separation of duties using existing personnel.

University of Maryland Academic Telecommunications System

Background

The Office is the host institution for an operating unit which supports the University of Maryland Academic Telecommunications System (UMATS). The UMATS network provides statewide telecommunications to the 13 University System of Maryland (USM) institutions and other related entities. For example, UMATS provides connectivity for Internet and research activity, access to the System institutions' online library systems, and access to related entities. The network also enables distance learning, where students at the various System institutions take classes from other System institutions offering the classes. The UMATS network connections transfer class-related video, audio, and data content. For administrative purposes, the UMATS network provides System institutions with a connection to the State Financial Management Information System (FMIS). The UMATS network includes high-speed communications lines that connect to routers and supporting network management servers located onsite at the various USM institutions and related entities.

Finding 3

Controls on critical UMATS management servers were inadequate.

Analysis

The UMATS network includes five management servers which are used for controlling network operations. Our examination of two of these servers disclosed that security controls over system services, network access, software maintenance, and security event monitoring were inadequate. Specifically, we noted the following conditions:

- Several unnecessary services, including an insecure connection protocol, were enabled on one critical UMATS server, and adequate network traffic filtering did not exist to protect the server from internal or external attacks. Unnecessary installed services can be used to take advantage of known vulnerabilities to maliciously compromise a computer system.
- Quarterly software vulnerability assessments were not performed for either UMATS network management server reviewed, in accordance with USM requirements. We performed vulnerability scans of these UMATS management servers, and detected 19 instances of vulnerabilities that the scanning tool identified as high or medium security vulnerabilities. As a result of these software vulnerabilities, these servers were not adequately

secured from exposures that could result in the loss of data integrity, the interruption of key services, and the improper use of these servers. We provided the Office with the detailed results of our scan.

- Security event monitoring of one UMATS management server was inadequate. Various security events were logged on the server and Office personnel advised us that they performed regular reviews of the logged information. However, adequate documentation did not exist to substantiate that these reviews were performed. A similar condition was commented upon in our preceding audit report.

Recommendation 3

We recommend that the Office only enable necessary services on all of its UMATS management servers. We also recommend that adequate network traffic filters be implemented to properly limit network level connections to these servers. Furthermore, we recommend that the Office perform quarterly vulnerability assessments of critical servers in accordance with USM requirements, perform timely follow-up reviews of the results of its vulnerability assessments, independently confirm all high risk vulnerabilities, and initiate corrective actions for all confirmed vulnerabilities. Finally, we again recommend that the Office perform regular reviews of management servers' security logs and that these reviews be documented for future reference.

Finding 4

Administration and monitoring controls for critical UMATS network devices were inadequate.

Analysis

The UMATS network backbone includes several high-speed traffic fiber optic transmission devices and core network routing devices which transmit and distribute traffic throughout the network. Our examination of one fiber optic device and one routing device disclosed that administration and monitoring controls were inadequate. Specifically, we noted the following conditions:

- The fiber optic device was improperly accessible from the Internet rather than being restricted to network administrators. Also, password settings (minimum password length, history, and age) for administrative accounts on this device did not comply with the requirements of the *USM Guidelines in Response to the State's IT Security Policy*. Furthermore, the device's log files were stored on the device itself and were not recorded on a separate logging server, which

subjected the log files to being overwritten when filled, and allowed intruders to modify the log files before they could be used to assist in the review of an attack.

- Security event monitoring for the fiber optic device and the routing device was inadequate. Although various security events were logged for these devices, Office personnel stated that they did not regularly review these logs. They advised us that they only reviewed the logs in the event that operating problems occurred. A similar condition was commented upon in our prior audit report.

Recommendation 4

We recommend that network level access to critical network traffic transmission devices be limited to personnel requiring such access and that password controls on these devices comply with the requirements of the USM *Guidelines in Response to the State's IT Security Policy*. We also recommend that security events for these devices be logged to a separate logging server. Furthermore, we again recommend that logs for all critical network devices be reviewed on a regular basis and that these reviews be documented and retained for future reference.

Finding 5

The Office's internal computer network was not adequately protected from security risks related to wireless connections.

Analysis

The Office's internal computer network, including UMATS management servers, was not adequately protected from security risks related to wireless connections. Specifically, connections made through wireless access points within the Office headquarters building could access the entire internal network without user authentication or encryption. As a result, anyone in the immediate vicinity of the Office headquarters building using a wireless network access device could gain access to the internal Office network or could intercept wireless network traffic associated with an Office wireless connection.

Recommendation 5

We recommend that the Office adjust its network to require that wireless connections by employees be subject to user authentication and encryption, and that wireless connections by anyone else be restricted to the Internet.

Finding 6

Sensitive personal and financial information for prospective USM students was unnecessarily stored on a publicly accessible server.

Analysis

Sensitive personal and financial information for certain prospective USM students was unnecessarily stored on a publicly accessible web server. The Office operated a web server to provide a website used by prospective students applying to several USM institutions. We determined that student names, social security numbers and, in some cases, credit card numbers were stored in plain text on the web server. According to the Office's records, more than 53,000 social security numbers and approximately 21,000 credit card numbers (with associated data such as cardholder names, card types, and card expiration dates), were stored on the server, dating back to 2004. Such information could be accessible to unauthorized individuals if the related server was compromised.

This sensitive personal and financial information residing on the server is commonly sought for use in identity theft. Accordingly, appropriate security controls need to exist to ensure that this information is safeguarded and is not improperly disclosed. The *USM Guidelines in Response to the State's IT Security Policy* stipulates that institutions must establish and document the safeguards against disclosure of nonpublic information (such as credit card and social security numbers).

Recommendation 6

We recommend that the Office remove the described sensitive personal and financial data from the publicly accessible server. If the information must be retained, we recommend that it be stored on an internal server that is not publicly accessible and that it be encrypted.

Finding 7

A complete information technology disaster recovery plan did not exist.

Analysis

The Office did not have a complete information technology disaster recovery plan for recovering the UMATS network from disaster scenarios (for example, a fire at a core network location). Although the Office had developed a UMATS disaster recovery plan, the plan was incomplete as it did not fully address certain elements, such as those contained in the State of Maryland Department of Budget and Management's *Information Technology Disaster Recovery Guidelines*.

Specifically, the inventory of critical core UMATS network devices was incomplete, and procurement data, which would help expedite the replacement of equipment, was missing. Also, the plan had not been tested.

Without a complete disaster recovery plan, a disaster could cause significant delays (for an undetermined period) in restoring operations above and beyond the expected delays that would exist in a planned recovery scenario.

Recommendation 7

We recommend that the Office develop and implement a complete information systems disaster recovery plan that covers all of the Office's critical functions, including the items noted above.

Equipment

Finding 8

Controls and accountability over equipment at the Office and one regional higher education center were inadequate.

Analysis

Controls and accountability over the Office's equipment, as well as the equipment at one regional higher education center, were inadequate. According to the Office's records, its equipment totaled \$5.3 million as of June 30, 2008, which included \$3.4 million of equipment for the Office and \$1.9 million of equipment for the regional centers. For example, we noted the following conditions:

- The Office did not properly record certain equipment acquisitions on its detail records. Specifically, our test of 24 equipment items totaling \$347,000 (acquired during the period from March 2007 through August 2007) disclosed that, as of May 2008, the Office had not established a detail record for 18 of the items totaling \$321,000.
- During the last physical inventory count at the Office, which was conducted in April 2006, approximately \$406,000 worth of equipment items from one department could not be located. However, there was no documented investigation regarding the missing items even though, based on verbal approval by an accounting manager, the items were removed from the equipment records. In this regard, the Office's equipment policies did not address the investigation of missing items and the process to remove them

from inventory. To ensure accountability and control over equipment, missing items should be adequately investigated and any required adjustments to the inventory records for such items should be approved by someone at an appropriate level.

- The Office's records for equipment items located at one regional higher education center, which reflected total equipment valued at \$1 million as of June 30, 2008, were incomplete. For example, our test of 55 items costing approximately \$278,000, which were purchased in April 2007 for this center, disclosed that none of the items were tagged nor were the items recorded in the Office's detail records as of June 2008. In addition, a physical inventory at this regional center had not been conducted since at least 2001.

The USM *Policy for Capitalization and Inventory Control* requires that physical inventories be conducted and reconciled with the related detail records at least once every two to three years depending on the value of the equipment. The *Policy* further requires each institution to establish its own formal policies governing the control of equipment.

Recommendation 8

We recommend that the Office properly record all equipment acquisitions in the equipment detail records and ensure that equipment is tagged. In addition, we recommend that the Office amend its policy to address the investigation of missing items and authorization to remove them from inventory. Finally, we recommend that the Office comply with the requirements of the aforementioned USM *Policy* and its own equipment policies.

Audit Scope, Objectives, and Methodology

We have audited the University System of Maryland Office for the period beginning January 13, 2005 and ending January 31, 2008. 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 State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine the Office's financial transactions, records and internal control, and to evaluate its compliance with applicable State laws, rules, and regulations. We also determined the status of the findings contained 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 the Office'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 included support services (that is, endowment accounting, bond financing) provided by the Office on a centralized basis for other units of the University System of Maryland. Our audit did not include certain support services provided to the Office by the University of Maryland, College Park. These support services (such as purchasing, processing vendor payments) are included within the scope of our audits of the University of Maryland, College Park.

Our audit scope was limited with respect to the Office's 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 of the Office's 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.

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

The Office's response 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 Office regarding the results of our review of its response.

APPENDIX



OFFICE OF THE CHANCELLOR

January 5, 2009

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

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

RE: University System of Maryland
Office

Audit Period: January 13, 2005 –
January 31, 2008

Dear Mr. Myers:

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

Sincerely,

WE Kirwan
William E. Kirwan
Chancellor

WEK:mk
Enclosures

cc: Mr. Clifford M. Kendall, Chairman, Board of Regents
Mr. Kevin M. O'Keefe, Chairman, MHEC
James E. Lyons, Sr. Ph.D., Secretary of Higher Education, MHEC
Mr. Robert Page, Comptroller, USM Office

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
UNIVERSITY SYSTEM OF MARYLAND OFFICE
JANUARY 13, 2005 – JANUARY 31, 2008**

Transfer of Endowment Funds

Finding 1

Certain significant contract provisions related to the transfer of approximately \$197 million in endowment funds by the Office to the University of Maryland Foundation for investment were not adhered to.

Recommendation 1

We recommend that the Office adopt investment policies as required by the aforementioned agreement and by State law, and provide the policies to the State Comptroller and State Treasurer, as required. We also recommend that the Office ensure that UMF is investing the CTF in accordance with the policies established. We further recommend that, where possible and appropriate, the Office take steps to include in this and future contracts a provision specifying the USM as a third-party beneficiary on UMF endowment investments. Finally, we recommend that future annual investment performance reports be prepared and submitted timely as required by law.

Response:

The System Office agrees with the recommendation.

Discussions on the necessary components of the Investment Policy have been initiated, and it is expected that a policy will be submitted to the Board of Regents for their consideration at the April 2009 or July 2009 meeting. The approved policy will be provided to the State Comptroller and State Treasurer, as required.

The University System of Maryland Foundation will be requested to comply with the provisions of the contract requiring that the System be specified as a third-party beneficiary on USMF investments arrangements.

Future annual investment reports will be prepared and submitted timely as required by law.

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
UNIVERSITY SYSTEM OF MARYLAND OFFICE
JANUARY 13, 2005 – JANUARY 31, 2008**

Cash Receipts

Finding 2

Cash receipts were not adequately controlled.

Recommendation 2

We again recommend that all checks be restrictively endorsed “for deposit only” and recorded immediately upon receipt. We also again recommend that an employee independent of the cash receipts function update the accounts receivable records. Furthermore, we recommend that an employee independent of the cash receipts function verify that all recorded collections are subsequently deposited. We advised the Office on establishing the necessary separation of duties using existing personnel.

Response

The System Office agrees with the recommendation. All checks will be restrictively endorsed and logged upon receipt. The cash receipts function will be handled by the administrative person in the Office of Financial Affairs. The Comptroller will periodically verify that recorded collections are subsequently deposited.

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
UNIVERSITY SYSTEM OF MARYLAND OFFICE
JANUARY 13, 2005 – JANUARY 31, 2008**

University of Maryland Academic Telecommunications System

Finding 3

Controls on critical UMATS management servers were inadequate.

Recommendation 3

We recommend that the Office only enable necessary services on all of its UMATS management servers. We also recommend that adequate network traffic filters be implemented to properly limit network level connections to these servers. Furthermore, we recommend that the Office perform quarterly vulnerability assessments of critical servers in accordance with USM requirements, perform timely follow-up reviews of the results of its vulnerability assessments, independently confirm all high risk vulnerabilities, and initiate corrective actions for all confirmed vulnerabilities. Finally, we again recommend that the Office perform regular reviews of management servers' security logs and that these reviews be documented for future reference.

Response

UMATS will close all unnecessary services on all of our management servers. Services which are necessary will be limited to only those IP addresses which need the service. The management servers will be added to the quarterly scans already being done of other server machines, and the UMATS staff will review and remediate any findings. An automated procedure will be created to document the review of the security logs from these servers. These changes will be implemented by July 1st, 2009.

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
UNIVERSITY SYSTEM OF MARYLAND OFFICE
JANUARY 13, 2005 – JANUARY 31, 2008**

Finding 4

Administration and monitoring controls for critical UMATS network devices were inadequate.

Recommendation 4

We recommend that network level access to critical network traffic transmission devices be limited to personnel requiring such access and that password controls on these devices comply with the requirements of the USM *Guidelines in Response to the State's IT Security Policy*. We also recommend that security events for these devices be logged to a separate logging server. Furthermore, we again recommend that logs for all critical network devices be reviewed on a regular basis and that these reviews be documented and retained for future reference.

Response

UMATS will restrict access to these critical network devices to the UMATS support unit. The password recommendations will be implemented. The device logs will be sent to a management server. As the device logs can be very large, a program to extract unexpected and security related messages will be written, and these reports will be reviewed by the UMATS staff. An electronic signoff procedure will be created to document the review of these logs. These changes will be implemented by July 1st, 2009.

Finding 5

The Office's internal computer network was not adequately protected from security risks related to wireless connections.

Recommendation 5

We recommend that the Office adjust its network to require that wireless connections by employees be subject to user authentication and encryption, and that wireless connections by anyone else be restricted to the Internet.

Response

The System Office agrees with the recommendation. Two separate wireless networks will be created; one that requires authentication, which will have access to internal servers, and one for guests and visitors to the building, which will not require authentication but will only have outbound internet access. The expected timetable for completion is by the end of the first quarter 2009.

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
UNIVERSITY SYSTEM OF MARYLAND OFFICE
JANUARY 13, 2005 – JANUARY 31, 2008**

Finding 6

Sensitive personal and financial information for prospective USM students was unnecessarily stored on a publicly accessible server.

Recommendation 6

We recommend that the Office remove the described sensitive personal and financial data from the publicly accessible server. If the information must be retained, we recommend that it be stored on an internal server that is not publicly accessible and that it be encrypted.

Response

The System Office agrees with the recommendation. The plan is to split the functionality of the application server into two systems, the web portion of which will be publicly accessible, and the storage / database portion of which will not. The expected timetable for completion is by the end of the first quarter 2009.

Finding 7

A complete information technology disaster recovery plan did not exist.

Recommendation 7

We recommend that the Office develop and implement a complete information systems disaster recovery plan that covers all of the Office's critical functions, including the items noted above.

Response

UMATS will update the disaster recovery plan by April 1st, 2009. The plan will be updated and tested using a simulated disaster at least annually, and the analysis kept on file.

**RESPONSE TO LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND
UNIVERSITY SYSTEM OF MARYLAND OFFICE
JANUARY 13, 2005 – JANUARY 31, 2008**

Equipment

Finding 8

Controls and accountability over equipment at the Office and one regional higher education center were inadequate.

Recommendation 8

We recommend that the Office properly record all equipment acquisitions in the equipment detail records and ensure that equipment is tagged. In addition, we recommend that the Office amend its policy to address the investigation of missing items and authorization to remove them from inventory. Finally, we recommend that the Office comply with the requirements of the aforementioned USM *Policy* and its own equipment policies.

Response

The System Office agrees with the recommendation. The current System Office policy on equipment control and inventory practices will be reviewed and updated to adequately address the resolution of exceptions in the periodic inventory process and the appropriate record-keeping for the inventory. The System Office will continue to improve in complying with the requirements of the USM and System Office policies.

AUDIT TEAM

Phyllis M. Clancy, CPA
Audit Manager

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

James M. Fowler
Senior Auditor

R. Brendan Coffey, CPA
Information Systems Senior Auditor

Catherine M. Clarke
Roger E. Jaynes, III
Tracy D. Ross
Staff Auditors

David J. Burger
Information Systems Staff Auditor