Audit Report

University System of Maryland
University of Maryland University College

June 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.

DEPARTMENT OF LEGISLATIVE SERVICES
OFFICE OF LEGISLATIVE AUDITS
MARYLAND GENERAL ASSEMBLY

Karl S. Aro
Executive Director

Bruce A. Myers, CPA
Legislative Auditor

June 12, 2009

Delegate Steven J. DeBoy, Sr., Co-Chair, Joint Audit Committee
Senator Verna L. Jones, 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 University College (UMUC) for the period beginning July 1, 2005 and ending July 31, 2008. UMUC offers degree and non-credit educational programs to part-time students who prefer not to enroll in more traditional full-time programs.

Our audit disclosed information system security and control deficiencies in UMUC's network that includes the student administration, human resources, and financial information systems, as well as its online education application. Online educational courses serve students around the world and account for a significant portion of UMUC's revenues. For example, our audit disclosed that UMUC did not perform required periodic reviews of the appropriateness of user access capabilities for its accounting, personnel, and student records systems and that certain account and password controls were inadequate, including for the online education application. In addition, security reports were not generated for certain critical applications, proper controls were not established over computer program changes, and the internal computer network was not sufficiently secured from both internal and external sources.

The University System of Maryland Office's response to this audit, on behalf of UMUC, is included as an appendix to this report. We wish to acknowledge the cooperation extended to us during our audit by UMUC.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor

Table of Contents

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

Executive Summary

Legislative Audit Report on University System of Maryland
University of Maryland University College (UMUC)
June 2009

- **UMUC did not perform periodic reviews of user access capabilities for the student administration, human resources, and financial information systems. Based on our limited review, we identified 13 employees who had the ability to change student grades who did not require such capability to perform their job duties.**

  UMUC should perform a documented periodic review of user access capabilities and make necessary corrections when inappropriate access is identified.

- **Access controls over the student administration, human resources, and financial information systems were not adequate. For example, numerous users had unnecessary access that would allow them to modify application security and make improper changes to the related databases.**

  UMUC should take the recommended actions to establish appropriate access controls for these systems.

- **Proper controls had not been implemented at the application, database, and operating systems levels. Specifically, account and password controls on the student administration, human resources, financial information, and online education application systems were inadequate. Certain security-related reports were not generated and adequate control procedures were not in place to ensure that only management authorized computer programs were placed in production.**

  UMUC should establish proper controls over user accounts and passwords for these applications, databases, and operating systems. UMUC should also regularly generate security events reports for review, appropriately segregate program change control procedures, and ensure all program changes are authorized.

- **Other internal control deficiencies were noted with respect to information systems security. For example, UMUC's disaster recovery plan was incomplete and outdated, and the internal computer network was not sufficiently secured.**

  UMUC should update and maintain its disaster recovery plan on a current basis and take other recommended corrective actions to improve its information systems controls.

- **An employee allegedly used a UMUC corporate purchasing card for personal gain. Computer and electronic equipment (such as, laptop computers, digital music players, and digital video cameras) were delivered to the employee's home address.**

  UMUC should consult with the Office of the Attorney General to determine what actions should be taken regarding this matter.

Background Information

Agency Responsibilities

The University of Maryland University College (UMUC) offers degree and non-credit educational programs to part-time students who prefer not to enroll in more traditional full-time programs. UMUC comprises three major divisions: the Statewide Division, the Asian Division, and the European Division. These three divisions offer educational programs at a number of locations primarily throughout the State of Maryland, as well as in numerous foreign countries. The Statewide Division also administers educational and training programs for adults, and maintains a residential conference center that includes conference rooms, guest accommodations, dining facilities, and an auditorium. UMUC's main administrative office and residential conference center are located in College Park, Maryland. The Asian Division is headquartered in Tokyo, Japan and the European Division is headquartered in Heidelberg, Germany.

For fiscal year 2008, UMUC's enrollment totaled approximately 87,600 students. UMUC's budget is funded by unrestricted revenues, such as tuition and student fees, a State general fund appropriation, and restricted revenues, such as federal grants. According to the State's accounting records, fiscal year 2008 revenues totaled approximately $281 million, which included a State general fund appropriation of approximately $24.7 million.

Status of Findings From Preceding Audit Report

Our audit included a review to determine the status of the 10 findings contained in our preceding audit report dated March 2, 2006. We determined that UMUC satisfactorily addressed nine of these findings. The remaining finding is repeated in this report.

Findings and Recommendations

Information Systems Security and Control

Background

The University of Maryland University College (UMUC) maintains an internal network that includes various servers used for student and financial applications. Other key resources include servers supporting online education courses, UMUC's e-mail and website, student and employee activities, and three separate connections to the Internet. Information systems are integral to the UMUC online education function and provide an interactive classroom experience to its students and faculty. Online education services range from supplementing traditional classroom sessions to complete course delivery, allow instructors to deliver materials, and allow students to submit related class work and interact with classmates and instructors. The online education application maintains and uses critical data, such as student assignment folders and faculty grade books used by instructors to record student grades both for individual assignments and for overall course performance. Online educational courses serve students around the world and account for a significant portion of UMUC's revenues. For example, we were advised that approximately 85 percent of UMUC's fiscal year 2008 stateside credit hours were taken through online courses, with a revenue value of approximately $132 million. In addition, UMUC operates student administration, human resources, and financial information systems.

Finding 1
UMUC did not perform periodic reviews of user access capabilities for the student administration, human resources, and financial information systems.

Analysis

UMUC did not perform periodic reviews of user access capabilities for the student administration, human resources, and financial information systems. In this regard, UMUC only reviewed employee access capabilities when an employee transferred to a new position within UMUC or when an employee terminated employment. Consequently, UMUC lacked assurance that inappropriate access would be detected. Based on our limited review, we identified 13 employees who had the ability to change student grades who did not require such capability to perform their job duties.

The University System of Maryland's (USM) *Guidelines in Response to the State's IT Security Policy* dated March 2008 requires that a documented review of employees' access privileges be conducted at least annually.

Recommendation 1
We recommend UMUC

a. perform a documented periodic review of user access capabilities for the student administration, human resources, and financial information systems and make necessary corrections when inappropriate access is identified, including for the 13 employees noted above; and

b. for any users found to have inappropriate access, conduct a review to determine if the user performed any critical system operations that were incompatible with his or her job functions and take any necessary corrective actions.

Finding 2
Deficiencies in access controls over the student administration, human resources, and financial information systems could allow unauthorized changes to the applications and related databases.

Analysis
Access controls over the student administration, human resources, and financial information systems were not adequate. Specifically, we noted the following conditions:

- Default passwords were not changed for three default accounts used for the student administration and human resources applications. Since the default accounts and passwords were provided by the vendor when the systems were purchased and are known to the public they could be used to obtain unauthorized modification access to these applications.

- Numerous user accounts were assigned unnecessary access to an application maintenance tool that could be used to modify all three systems' application security settings and make unauthorized changes to the information in the related databases.

- Two user accounts had unnecessary modification access to the student administration and human resources systems' user profiles, roles, and permissions. Accordingly, these two accounts could make improper changes to user profiles, roles, and permissions and the related system data.

Recommendation 2
We recommend that UMUC

a. change the default passwords for all default critical application system accounts;

b. limit access to the aforementioned application maintenance tool to personnel whose job duties require use of this tool; and

c. restrict modification access to critical applications' user profiles, roles, and permissions to personnel whose job duties require such access.

Finding 3
Account and password controls at the application, database, and operating system levels were inadequate.

Analysis

Account and password controls on the student administration, human resources, financial information, and online education application systems were inadequate. In addition, account and password controls were inadequate at the database level for the student administration, human resources, and financial information systems and at the operating system levels for these three systems and for the online education application system. In this regard, we noted several instances where password length, complexity, aging, history, and account lockout were not enabled. We also noted instances where database and network administrators did not have their own accounts and used shared accounts thereby precluding individual accountability for their actions. In addition, identical account and password information existed on production and non-production versions of the same critical applications and databases, which increased security exposures. Finally, we identified 66 unused active application system accounts which were no longer needed and had been unused for periods from one to more than four years.

Accordingly, defined control settings for accounts and passwords did not comply with the USM *Guidelines in Response to the State's IT Security Policy* dated March 2008.

Recommendation 3

We recommend that adequate security be established over user accounts and passwords for UMUC's applications, databases, and operating systems. We made detailed recommendations to UMUC which, if implemented, should provide the necessary security.

Finding 4
Monitoring of security-related activity was inadequate for critical applications, and proper controls were not established over program changes.

Analysis
Monitoring and program change controls over critical systems were inadequate. Specifically, we noted the following conditions:

- Security-related reports were not generated for the student administration, human resources, and financial information applications. In addition, for the online education application servers' operating systems, we were advised that only limited security-related activity was reported and only cursory reviews were made of the security reports. Furthermore, these reviews were not documented. As a result of these conditions, unauthorized or inappropriate activities, affecting the integrity of application data and operating system security settings, could go undetected.

- Adequate control procedures did not exist to ensure that only management-authorized computer programs had been placed into production. For the online education application system, one individual had complete control over the production program change control process. In addition, for the student administration, human resources, and financial information systems, several individuals could modify programs and then migrate these programs into production thereby bypassing the supervisory review process which is required by the change management procedures. In addition, new and changed production program activity for the student administration, human resources, and financial information systems was not reviewed to ensure that new programs and changes were authorized. As a result of these conditions, improper or erroneous program changes could be placed into production status without management's awareness or authorization.

Recommendation 4
We recommend that UMUC

a. regularly generate reports of security events for its critical applications, perform timely reviews and investigations of these reports, and document these efforts; and

b. appropriately segregate program change control procedures and perform independent, routine reviews of new and changed production programs to ensure that all program changes were authorized.

Finding 5
UMUC's disaster recovery plan was incomplete and outdated.

Analysis
UMUC's disaster recovery plan, which was last updated in September 2004, was incomplete and outdated. The plan did not include the following critical elements specified by the Department of Budget and Management's (DBM) *Information Technology (IT) Disaster Recovery Guidelines*:

- Current listing of hardware and software components
- Plan for restoring network connectivity
- Application inventories prioritized for recovery
- Current roles and responsibilities of critical personnel

In addition, the plan had not been fully tested. Without a complete and current 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 5
We recommend that UMUC update, and maintain on a current basis, a disaster recovery plan to comply with all relevant elements of DBM's *Information Technology (IT) Disaster Recovery Guidelines*.

Finding 6
The internal computer network was not sufficiently secured.

Analysis
Critical systems were not adequately protected from both internal and external exposures. Specifically, we noted the following conditions:

- Critical network devices were not configured to adequately secure the internal network from untrusted network segments (for example, student computer labs and a wireless network). Proper network security control should employ a "least privilege" security strategy, giving individuals only the level of network access needed to perform assigned tasks.

- Several widely accessible servers were located on the internal network rather than in a separate network zone to minimize security risks. These widely accessible servers, which could potentially be compromised, exposed the internal network to attack from external sources.

- Intrusion detection systems were not properly used to protect critical portions of the network. Specifically, while the network included an intrusion detection system, its placement did not protect critical portions of the internal network from threats originating from untrusted network sources. Also, the intrusion detection system was not configured to automatically alert support staff regarding critical security conditions detected and the most current intrusion detection signatures were not installed on the system. Intrusion detection systems gather and analyze network traffic to identify network security breaches and attacks, and alert network administrators of these situations.

- UMUC's quarterly vulnerability assessments of its critical systems did not include numerous critical servers, and documentation of efforts made to research and resolve reported vulnerabilities did not exist.

Recommendation 6
We recommend that controls be established to adequately secure UMUC's internal network. We made detailed recommendations which, if implemented, should provide for the necessary controls.

Finding 7
Security within UMUC's online education application was not adequate to protect critical data.

Analysis
Adequate security did not exist over certain portions of the critical data within the online education application. Specifically, password information for the application's student and faculty accounts was not adequately protected. For login authentication purposes, application users (including the general public via the guest account) were granted necessary read access to the portion of the database storing user accounts; furthermore, application users could view user accounts other than their own. Because of an application weakness and how the host application server was configured, application users could obtain the encrypted passwords for any student or faculty account. In this regard, software is readily available over the Internet that can crack these encrypted passwords. Therefore, student assignment folders and faculty grade books were at risk of disclosure and compromise from the general public. This control weakness was magnified because of the weak password controls mentioned in audit finding 3.

This same condition was commented upon in our preceding audit report.

Recommendation 7
We again recommend that UMUC enable available security features for the online education application to prevent the display of the encrypted user passwords.

Corporate Purchasing Cards

Finding 8
An employee allegedly used a UMUC corporate purchasing card for personal gain.

Analysis
Our review of corporate purchasing card transactions made during the audit period disclosed that, during August and September 2005, an employee used a UMUC credit card to purchase computer and electronic equipment costing approximately $8,800 (such as laptop computers, digital music players, and digital video cameras) that was delivered to the employee's home address. As a result of this review, we tested 10 additional credit card purchases made by this employee, totaling $16,600. The related documentation disclosed that, while the invoices for the items purchased stated that the items were delivered to UMUC, four equipment items (that is, a flat screen television, a laptop, and two digital cameras) costing $2,800 could not be physically located. Furthermore, these four equipment items were not included in UMUC's equipment inventory records.

UMUC was not aware of these employee purchases until we brought this matter to its attention and was not able to readily locate the documentation related to these purchases. UMUC officials advised us that these purchases were not discovered because the employee's supervisor had not reviewed and approved the credit card statements, as required by the Comptroller of the Treasury's *Corporate Purchasing Card Program Policy and Procedures Manual* and by UMUC's existing procedures. The employee resigned from UMUC in October 2005, and the employee's supervisor resigned in June 2006. During the employee's employment at UMUC from May 2004 to October 2005, the employee used the credit card to make purchases totaling approximately $523,900, which were mainly computer and electronic in nature.

UMUC has referred this matter to the Office of the Attorney General - Educational Affairs Division, in accordance with the USM Board of Regents policy on reporting suspected or known fiscal irregularities.

Recommendation 8

We recommend that UMUC

a. consult with the Office of the Attorney General to determine what actions (including determining the extent of questionable purchases and pursuing reimbursement), should be taken at this time regarding this matter;

b. ensure that all cardholder credit card statements are subject to supervisory review and approval, as required.

Audit Scope, Objectives, and Methodology

We have audited the University System of Maryland (USM) – University of Maryland University College (UMUC) for the period beginning July 1, 2005 and ending July 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 the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine the UMUC'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 UMUC'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.

With respect to UMUC's Asian and European Divisions, our audit did not include an evaluation of financial transactions, records, and internal controls and an assessment of compliance with State laws, rules, and regulations. These divisions, which accounted for approximately 8 percent and 10 percent of UMUC's fiscal year 2008 revenues, respectively, are reviewed on a triennial basis by the USM internal auditors.

In addition, our audit did not include certain support services provided to UMUC by the USM Office (such as endowment accounting and bond financing) 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. Furthermore, our audit did not include an evaluation of internal controls for federal financial assistance programs and an assessment of UMUC's compliance with federal laws and regulations pertaining to those programs

because the State of Maryland engages an independent accounting firm to annually audit such programs administered by State agencies, including the components of USM.

UMUC'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.

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

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

APPENDIX

OFFICE OF THE CHANCELLOR

June 10, 2009

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 University College
Period of Audit: July 5, 2005 through July 31, 2008

Dear Mr. Myers:

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

Sincerely,

WE Kirwan

William E. Kirwan
Chancellor

Enclosure

WEK:mpk

cc: Dr. Susan C. Aldridge, President, UMUC
Mr. Clifford M. Kendall, Chairman, Board of Regents, USM
Mr. Robert Page, Comptroller, USM
Mr. Kevin M. O'Keefe, Chair, MHEC
Dr. James E. Lyons, Sr., Secretory of Higher Education, MHEC
Mr. David Mosca, Director of Internal Audit, USM

RESPONSE TO THE LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND – UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE
FOR THE PERIOD JULY 5, 2005 - JULY 31, 2008

Finding 1
UMUC did not perform periodic reviews of user access capabilities for the student administration, human resources, and financial information systems.

Recommendation 1
We recommend UMUC

a. perform a documented periodic review of user access capabilities for the student administration, human resources, and financial information systems and make necessary corrections when inappropriate access is identified, including for the 13 employees noted above; and
b. for any users found to have inappropriate access, conduct a review to determine if the user performed any critical system operations that were incompatible with his or her job functions and take any necessary corrective actions.

UMUC Response

UMUC agrees with these recommendations. In accordance with the USM Guidelines in Response to the State's IT Security Policy dated March 2008, a documented review of employee's access privileges will be conducted periodically and corrections made as necessary. In support of this, UMUC has adopted new policies to revoke and re-approve access for job changes within the university. Corrections have been made for the 13 aforementioned employees' access. For any users with inappropriate access identified, UMUC will use reasonable efforts when available to conduct a review of critical system operations.

Finding 2
Deficiencies in access controls over the student administration, human resources, and financial information systems could allow unauthorized changes to the applications and related databases.

Recommendation 2
We recommend that UMUC

a. change the default passwords for all default critical application system accounts;
b. limit access to the aforementioned application maintenance tool to personnel whose job duties require use of this tool; and

c. restrict modification access to critical applications' user profiles, roles, and permissions to personnel whose job duties require such access.

UMUC Response

UMUC agrees with the recommendations. The default passwords for default critical application system accounts have been changed and will continue to be changed with future software system upgrades. A review of the aforementioned application maintenance tool will be conducted by March 31, 2010, and access limited appropriately to job duties. UMUC will continue to review and restrict modification access as appropriate to personnel job duties.

Finding 3
Account and password controls at the application, database, and operating system levels were inadequate.

Recommendation 3
We recommend that adequate security be established over user accounts and passwords for UMUC's applications, databases, and operating systems. We made detailed recommendations to UMUC which, if implemented, should provide the necessary security.

UMUC Response

UMUC agrees with the recommendations. The detailed recommendations will be addressed individually to comply with the USM Guidelines in Response to the State's IT Security Policy document. Implementation of many of these recommendations has already been completed. Other more technically involved recommendations are being reviewed and analyzed. It is expected all individual recommendations to be addressed by July 1, 2010, as some will require research and testing of new operational procedures and enforcement means.

Finding 4
Monitoring of security-related activity was inadequate for critical applications, and proper controls were not established over program changes.

Recommendation 4
We recommend that UMUC

a. regularly generate reports of security events for its critical applications, perform timely reviews and investigations of these reports, and document these efforts; and

b. appropriately segregate program change control procedures and perform independent, routine reviews of new and changed production programs to ensure that all program changes were authorized.

UMUC Response

UMUC agrees with the recommendations. UMUC will expand its present security event generation and documented review process for critical applications. Evaluations to determine the technical feasibility to implement such solutions for certain application systems will be conducted and are expected to be completed by December 31, 2010. UMUC currently has policies, procedures, and change control software in place to restrict changes to production programs. The change control software will be evaluated to determine if it can provide further restrictions as recommended. If unable to do so, additional independent, routine reviews will be performed to validate authorization for new and changed production programs. This assessment and implementation is expected to be completed by December 31, 2010.

Finding 5
UMUC's disaster recovery plan was incomplete and outdated.

Recommendation 5
We recommend that UMUC update, and maintain on a current basis, a disaster recovery plan to comply with all relevant elements of DBM's *Information Technology (IT) Disaster Recovery Guidelines*.

UMUC Response

UMUC agrees with the recommendation. UMUC has been actively undergoing an updated disaster recovery project since 2007 including the purchase of information technology hardware to protect mission-critical applications (including Peoplesoft and WebTycho), contracting a remote disaster recovery site for space and services, and the

implementation and testing of these applications in the remote disaster recovery environment. These activities were being conducted during the audit period and have been completed as of May 2009. The remaining DBM Disaster Recovery guidelines will be completed by December 31, 2010.

Finding 6
The internal computer network was not sufficiently secured.

Recommendation 6
We recommend that controls be established to adequately secure UMUC's internal network. We made detailed recommendations which, if implemented, should provide for the necessary controls.

UMUC Response

UMUC agrees with the recommendations. Implementation of many of these recommendations has already been completed. Others more technically involved recommendations are being reviewed and analyzed. It is expected all individual recommendations to be addressed by December 31, 2010, as some will require significant planning, testing, and deployment efforts.

Finding 7
Security within UMUC's online education application was not adequate to protect critical data.

Recommendation 7
We again recommend that UMUC enable available security features for the online education application to prevent the display of the encrypted user passwords.

UMUC Response

UMUC agrees with this recommendation and implemented changes in September 2008 to address the security vulnerability discovered.

RESPONSE TO THE LEGISLATIVE AUDIT REPORT
UNIVERSITY SYSTEM OF MARYLAND – UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE
FOR THE PERIOD JULY 5, 2005 - JULY 31, 2008

Finding 8
An employee allegedly used a UMUC corporate purchasing card for personal gain.

Recommendation 8
We recommend that UMUC

a. consult with the Office of the Attorney General to determine what actions (including determining the extent of questionable purchases and pursuing reimbursement), should be taken at this time regarding this matter;
b. ensure that all cardholder credit card statements are subject to supervisory review and approval, as required.

UMUC Response

UMUC agrees with the recommendations and has been working with USM's Office of Internal Audit and the Attorney General's Office on this matter. In addition, all cardholders and approvers have been re-trained stressing the importance of the approval process, and new steps have been added to ensure all supervisors approve purchasing card transactions.

AUDIT TEAM

Matthew L. Streett, CPA, CFE
Audit Manager

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

W. Thomas Sides
Senior Auditor

Omar A. Gonzalez, CPA
Albert E. Schmidt, CPA
Information Systems Senior Auditors

Catherine M. Clarke
Kingsley M. Ndi
Jacquelyn M. Tindall
Staff Auditors

Amanda L. Trythall
Information Systems Staff Auditor