

THE UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Received by the Regents
March 20, 2008

Item for Information

Subject: Report of University Internal Audits
December 1, 2007 – January 31, 2008

Background:

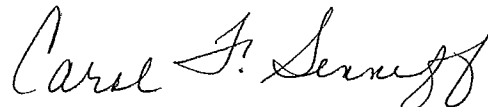
This is the report of the Office of University Audits activities for the period **December 1, 2007 through January 31, 2008**. The summaries of audits contained in this report were previously reported to members of the Regents' Finance, Audit and Investment Committee and included in discussions at Committee meetings.

Included in this report:

- Summaries of each audit report issued during the period, including Management's Plan to enhance specific control processes discussed with the audit client and presented in the report.
- Summaries of follow-up review reports issued during the period, including the actions taken by Management. Follow-up reviews are designed to give assurance that Management's Plan for corrective action has been implemented and controls are working appropriately.
- A report on the status of follow-up reviews as of **January 31, 2008**.

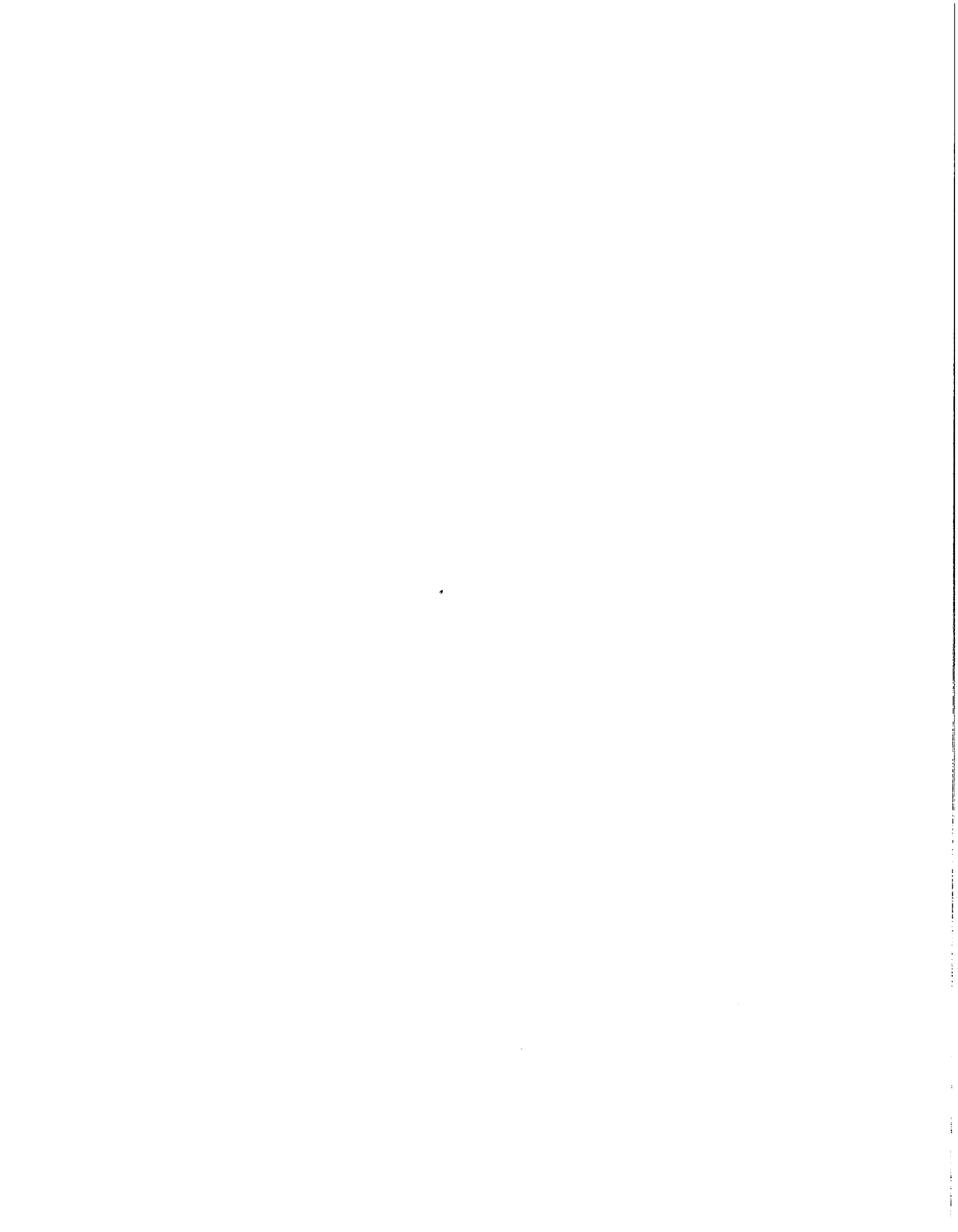
If you have any questions or would like additional information, please contact me at 647-7500 or by e-mail at csenneff@umich.edu.

Respectfully submitted,



Carol F. Senneff, Executive Director
University Audits

Attachment: February, 2008 Report



University Audits
December 2007 and January 2008 – Summary of Reports Issued

ORIGINAL REPORTS

Campus

University Human Resources Family and Medical Leave Act
Issued December 17, 2007

#2007-403

University Audits completed a review of processes related to the Family and Medical Leave Act of 1993 (FMLA). The U.S. Department of Labor's (DOL) Employment Standards Administration, Wage and Hour Division administers and enforces FMLA for all private, state, and local government employees. FMLA allows eligible employees up to twelve weeks of job-protected leave per year, provides for the employee's pre-existing group health insurance coverage, and restores the employee to the same or an equivalent position at the conclusion of the designated leave. The University employs over 38,000 people; FMLA applies to all employees with at least one year of service who worked at least 1,250 hours in the previous twelve months. It is not possible to determine the volume of FMLA qualifying absences because current procedures only require unpaid absences to be recorded in the University's system.

The following grid explains the responsibility for FMLA administration at the University:

Employee Type	Responsible Department
Ann Arbor Campus Bargained For	University Human Resources (UHR)
Ann Arbor Campus Non-Bargained For	Employee's Department
Health System Bargained For	UHR
Health System Non-Bargained For	Employee's Department
Flint Campus	Flint-HR
Dearborn Campus	Dearborn-HR

The objective of this audit was to evaluate the adequacy of policies and procedures to assure compliance with FMLA across the University's campuses for staff appointees.

Audit procedures included interviews with various staff from the following areas: UHR, Payroll Office, Human Resource Records and Information Services (HRRIS), Office of General Counsel, Risk Management Services, Flint HR, Dearborn HR, U-M Health System (UMHS) HR, and five individual departments from the Ann Arbor campus and Health System. University Audits distributed a survey to a representative sample of departments across the Ann Arbor campus and Health System to help assess the unit-level understanding of FMLA. In addition, analysis of Human Resource Management System data sets, as well as a review of FMLA and leave documentation for a sample of employees, was performed to verify compliance with FMLA for all campuses.

Based on the audit work performed, the University appears to be providing employees with the intended benefits of the Family and Medical Leave Act. University Audits did not observe any issues of non-compliance. The University's commitment to providing high-quality and comprehensive health benefits for its employees reduces the risk of non-compliance. Detailed observations and recommendations to help ensure that FMLA absences are processed and tracked consistently, University-wide, were provided to UHR. UHR has agreed to:

- Train employees responsible for answering questions related to FMLA and send a reminder with links to available FMLA resources to unit-level employees.
- Update relevant online SPG sections to include a statement regarding FMLA and links to available resources.
- Send employees a written notification that clearly explains the reasons their request for an FMLA absence has been denied and details their right to file a dispute.

UHR is working with other central units to assess the risk associated with record keeping and explore options for recording all FMLA absences in the University's Human Resources Management System. University Audits will follow-up during the fourth quarter of fiscal year 2008 to verify that all process improvements are implemented and working accordingly.

Ross School of Business Multidisciplinary Action Projects

#2007-103

Issued January 10, 2008

The Ross School of Business School (RSB) Multidisciplinary Action Projects (MAP) is a part of the MBA core curriculum. The MAP program involves teams of 4-6 students who are placed in company environments and guided by faculty advisers in order to learn how to integrate business disciplines and provide actionable recommendations to address organizational challenges. MAP projects cover a range of business issues and can be domestic, international, corporate, entrepreneurial, or nonprofit. Sponsors generally reimburse student, project-related expenses. Since 1992, Ross students have completed more than 1,180 MAP projects for more than 600 organizations around the world.

The MAP Office is responsible for reviewing and selecting project proposals, assigning students and faculty to projects, preparing students for international travel, obtaining student travel advances and reconciling expense reports, and invoicing international sponsors for expense reimbursement. For domestic projects, the students work directly with the sponsors for expense reimbursement.

Primary audit objectives were to:

- Assess the adequacy of processes to manage international travel issues
- Confirm that expenses from Expendable Restricted Funds are adequately managed and comply with University guidelines
- Evaluate the process to invoice and obtain timely reimbursement from sponsors
- Verify that travel advances are used appropriately and reconciled within 30 days
- Determine whether the MAP Program is evaluated on a regular basis to confirm that program goals are being achieved effectively and efficiently
- Verify that potential conflicts of interests related to the project selection and assignment of students and faculty are adequately managed

Control Issues:

1. **International Travel Registration** - The MAP Office does not have procedures to ensure that students register international travel with the International Travel Oversight Committee (ITOC). The U-M International Travel Guidelines require this registration. This requirement is included in the checklist provided to students; however, only one of ten students sampled registered their international travel with the ITOC. The MAP

Office is aware of the dates and locations where the students travel, as well as emergency contact information; however, ensuring this information is also with the ITOC will help guarantee that students can be contacted while overseas in the event of an emergency.

Management Plan - MAP Management will ensure that all international travel information is registered with the ITOC. Rather than having each student individually provide information to the ITOC, which they are already providing to MAP, Management will work with the ITOC to determine if it is possible to send a spreadsheet with all required details. Otherwise, the MAP Office will register each team prior to travel.

2. Procurement - Detailed testing, to verify timeliness of reconciliations and consistency with University and MAP guidelines, for a sample of expense reports and P-Card purchases revealed the following exceptions in some cases:
 - Non-itemized meal receipts, as required by MAP Office guidelines
 - Missing support documentation for conversion rates, as required by MAP Office guidelines
 - Lack of appropriate signature authority for expense reports
 - P-Card statements significantly above total credit limit
 - Individual P-Card transaction limits exceeded
 - P-Card statement approver not the designated approver
 - Travel advances not reconciled within 30 days

Management Plan - On occasion, expense reports are delayed so that the MAP Office can work with students to resolve any errors prior to submitting to Accounts Payable. University Audits has made Management aware of Procurement Services' willingness to discuss Controlled Value Cards as an option for our program. The temporary, limited credit cards would make the process for reconciling expenses more efficient and automatically convert expenses to U.S. Dollars. MAP Management will re-evaluate their expense guidelines, change them as necessary, and provide students with additional guidance regarding appropriate receipts for reimbursement. Map Management will request a temporary increase to the Assistant Director's P-Card to address business needs. Back-up approvers will be added to P-Cards where deemed necessary. P-Card approvers will take the online approver training offered by Procurement Services.

3. Expendable Restricted Funds - There is no process to verify the appropriateness of expendable restricted funds expenditures. The MAP Office did not have agreements for the gifts assigned to the MAP program; however, agreements were obtained from the RSB Development Office. Although MAP expenses appear to be appropriate, it is difficult to confirm consistency with restrictions due to the vague language in existing, original documentation. To determine whether expenditures made from gifts are permissible, it is imperative to review agreement provisions.

Management Plan - MAP management will work with the RSB Development Office to create a document summarizing the donor intentions for each of the restricted funds assigned to the MAP Program. This document will be used to ensure that all funds are being used appropriately when reconciling the MAP Office Statement of Activity. This process will be included in the documented procedures.

4. Documented Procedures: MAP Office operational procedures are not formally documented. Documented procedures provide a standard source of information for training; job aids and checklists can assist staff in performing daily duties consistently.

Procedures should include timeframes for meeting critical deadlines, as well as a process for reviewing and updating procedures to keep them current. Key operational processes include, but are not limited to:

- Reviewing proposals and selecting projects, including selection criteria at each phase of the selection process
- Assigning students and faculty to projects, including the process to run the algorithm program used to place students on project teams based on preferences and required criterion
- Preparing students for international travel
- Coordinating the expense reimbursement process for international projects
- Reviewing travel advance expenses
- Evaluating the program against goals or established metrics

Management Plan - Key guidelines for the MAP Office operations will be documented at a high-level to ensure the program maintains flexibility. Guidelines will include a reference to the RSB COC/COI statement(s) where applicable. Criterion for selecting MAP projects for each phase of the process will be documented; however, these will also be at a high-level since it is largely based on experience and judgment.

Based on the audit work completed, the MAP Office has adequate procedures to review and select projects, prepare students for international travel, and evaluate and improve the program annually. University Audits will conduct a follow-up review in the first quarter of fiscal year 2009 to assess progress on action plans.

Transportation Services
Issued January 28, 2008

#2007-101

Parking and Transportation Services provides University faculty, staff, students, patients and visitors with safe, reliable, clean, and efficient parking and transportation services. Transportation Fleet Services administers and maintains the fleet of University vehicles. All University vehicles, including those obtained by departments as gifts or under research grants, must be purchased, leased, and disposed of by Fleet Services.

University Audits examined the following processes to evaluate the adequacy and effectiveness of internal controls governing Transportation Services:

- Fleet management
- Inventory management
- Purchasing
- Billing
- Administrative procedures

Control Issues:

1. **Controls over Physical Access** - The main entry into the area where Transportation Services vehicles are located (the SC 10 lot) is secured via an electronic gate. The gate is operated by electronic switch, which is secured in a locked box located on the side of the gate. According to a sign posted at the gate, the Transportation Services area is accessible weekdays from 6:00 am until 12:30 am. A second electronic gate secures a smaller entrance located on the south side of the garage. The second gate is not equipped with an outside electronic switch; the gate must be opened from inside the Transportation Services area. During the audit, the main gate was observed to be open after operating hours. It does not appear that the gates are consistently

secured as intended. Physical security controls are less effective when applied inconsistently, which allows opportunity for unauthorized individuals to access the Transportation Services area.

Bus drivers and many Plant Operations staff have keys to the gate to obtain access to Transportation Services after operating hours. However, no formal key inventory is maintained within Transportation Services. Additionally, lost key procedures are not formally documented. Improperly maintained inventory of keys increases the risk of unauthorized access to the gated area. Without appropriate security controls, automobiles, trucks, and buses stored in this area are more susceptible to vandalism and theft.

Management Plan - A comprehensive security plan involving several different occupants and users of the SC 10 lot is in progress, with plans to install automated gate controls. This plan also includes consideration of surveillance camera installation for monitoring of the area. An interim policy has been established to ensure both gates are closed when Parking and Transportation Services supervision is not occupying the building.

2. FASTER User Access Levels - Transportation Services uses FASTER system software by CCG Systems to perform daily fleet management tasks, including parts and equipment inventory maintenance, work order entry, and billing. Review of a sample of user access levels revealed that several Transportation Services employees have access to update, add, and delete information within the Work Orders tables. Some of these roles are not necessary for the employees' specific job responsibilities. As work orders are used to record and bill maintenance and repair activities, staff access to these tables should be limited to the lowest level required to complete their responsibilities.

Management Plan - Transportation Services took prompt action to review and correct access levels during the audit; however, a similar review and evaluation will be necessary as part of the new system implementation. Therefore, University Audits will evaluate user access levels again during the follow-up review, but in the new MAXIMUS system after implementation.

3. Commercial Driver's License Testing - U-M has been a third party test organization for commercial driver's licenses since 1989. As required by the State of Michigan, the University must offer these testing services to the general public. The two individuals who perform skills testing, both retirees from Transportation Services, test non U-M affiliated persons on their personal time at the U-M test site. A fee is charged for testing to the non-affiliated individuals. Fees, which are published on University letterhead, are collected by the individual testers and are not remitted to the University. A receipt is issued to the individual remitting the payment on University letterhead, even though the University has not received the funds.

We suggest that management consult with the Office of the General Counsel to develop an appropriate business arrangement with the individuals administering the skills testing for commercial driver's licenses. The arrangement should eliminate the process of issuing University receipts for funds not collected.

Management Plan - Management will confer with the Office of the General Counsel to establish appropriate procedures for receipt of testing fees and payment of examiners.

4. Vehicle Inventory Monitoring Procedures - Vehicle inventory monitoring procedures are not formally documented within Transportation Services. The FASTER fleet management system is used to track all vehicles. Physical observation of each vehicle is performed at least annually by way of vehicle maintenance, which is also tracked in the FASTER system. The vehicle listing, from the FASTER system, is compared to an annual inventory report from the Asset

Management module of M-Pathways Financials & Physical Resources system. Discrepancies are investigated and resolved, as appropriate; however, evidence of the review is not retained.

Inventory monitoring limits the possibility of inaccurate reporting, discrepancies between systems, and undetected vehicle theft or loss. Without appropriately documented procedures, it is difficult to ascertain if monitoring procedures are sufficient. Additionally, inventory monitoring may not be completed appropriately if the employee with knowledge of the reconciliation process is absent.

Management Plan - Management will document inventory monitoring procedures and implement a process whereby vehicle lists are verified to ensure consistent information is contained in both FASTER and M-Pathways Asset Management module. This process will include documentation of inventory reviews.

5. Fuel Inspection Upon Delivery - Due to high delivery volume, fuel vendors have keys to fuel tanks at service stations located at Transportation Services on Kipke Road and Baxter Road for delivery of fuel. Transportation Services staff do not verify the delivery of gas, specifically to the unmanned service station on Baxter Road. In addition, fuel is not tested once delivered. Verification of shipment and proactive testing of fuel could identify incorrect fuel type or tainted fuel before pumps or vehicles are affected.

Management Plan - Management will install an electronic tank monitoring system at the Baxter Road service station with the ability to report fuel delivery amounts. Fuel specifications have been updated to reflect minimum acceptable quality of fuels, including testing standards. Two fuel testing vendors have been identified for periodic testing.

6. Gross Pay Register Review Process - The financial clerk responsible for time entry reviews the Gross Pay Register to ensure payroll was processed according to time entered. Management does not regularly review the Gross Pay Register. Regular payroll monitoring by employees independent of the timekeeping function could alert management to payroll issues, irregularities, and possible fraud.

Management Plan - Management will establish and document a procedure for verifying payroll to the Gross Pay Register. An employee independent of the timekeeping function will perform this verification. Management will perform regular reviews of the Gross Pay Register and retain a record of the Gross Pay Register review with the Statement of Account.

7. Use and Reimbursement of Imprest Cash Fund - The imprest cash fund is used to pay individuals not employed by the University of Michigan for services provided to Transportation Services. Reimbursement of the imprest cash fund is obtained through the Cashier's Office using the Petty Cash Form.

SPG 201.86, Independent Consultants, describes the procedure for requesting payment for services of an independent consultant. As indicated in the Standard Practice Guide, the form G-2 should be used for payments to independent consultants. (Forms G and G-2 will soon be replaced by the PeoplePay module.) Guidelines for reimbursement of imprest cash funds are included in SPG 501.2-1, Imprest Cash Funds. According to the SPG, non-PO vouchers must be prepared and submitted to the Accounts Payable Office for imprest cash fund reimbursement.

Internal Audit recommends the following:

- Review imprest cash usage and reimbursement procedures

- Develop and document formal procedures in accordance with applicable Standard Practice Guide sections. Specifically, the use of forms G for payment to independent consultants for services, and obtain reimbursement of the imprest cash fund via Accounts Payable
- Ensure procedures include guidance for usage of the forms G replacement, PeoplePay

Management Plan - The current practice was previously allowed as an exemption to the policy due to the infrequency of occurrence and the difficulty and cost of contracting some services, especially that of auction drivers, elsewhere. Individuals reimbursed with these funds are auction drivers, typically U-M retirees, who would likely refrain from providing this valuable service rather than deal with the implications of this small stipend. Management will contact Financial Operations, the Office of Contract Administration, and Human Resources to obtain documentation of the exception.

8. Formal Policies and Procedures - Procedures are not formally documented for operational processes including vehicle, fuel management, inventory management, maintenance, vehicle disposal, billing, and purchasing. Although informal procedures exist for some processes, specific guidance is not provided for key decisions, such as parameters for vehicle disposal. Documented procedures provide a standard source of information for training. Job aids and checklists can assist staff in performing daily duties consistently.

Management Plan – Transportation Services management will develop a procedure manual for key processes, including vehicle management, fuel management, inventory management, maintenance standards, vehicle disposition, and purchasing.

University Audits will conduct a follow-up review in the first quarter of fiscal year 2009 to assess progress on action plans.

I-9 Employment Verification Process

#2007-823

Issued January 29, 2008

At the request of the Senior Director of Human Resource Records and Information Services (HRRIS), University Audits conducted a review of the I-9 Employment Eligibility Verification process.

The I-9 eLearning course became available to University employees two years ago. The objective of this audit was to assess the effectiveness of the I-9 verification process since the implementation of the on-line training. Data for employees hired since the inception of the eLearning Course was provided by HRRIS for analysis.

Control Issue:

Analysis of the sample data provided by HRRIS identified areas for potential improvement, primarily related to timeliness and file maintenance. Details of these observations were provided to HRRIS management for their review. Additionally, a collaborative meeting was conducted with University Audits, Academic Human Resources, and HRRIS aimed at identifying solutions.

The eLearning Course is a valuable tool and should be taken by all employees with I-9 verification responsibility. We recommend that University Human Resources (UHR) work with appropriate University resources to identify individuals who can serve as Unit Compliance Officers responsible for the I-9 verification process in their units.

Management Plan - They are working with the Office of the General Counsel and the International Center to institute the concept of an "I-9 Compliance Officer" in each unit. The I-9 Compliance Officers

(ICOs) will be asked to remain current on new regulations and requirements, regularly audit the I-9s generated by their unit staff, and provide feedback and suggestions for additional training when necessary. An e-mail group for ICOs will be developed and maintained by UHR to facilitate better communication with UHR, the International Center, and the Office of the General Counsel.

In addition, HRRIS is currently investigating possible system and process enhancements to:

- Further develop the eLearning Course tutorial module's ability to register staff and track course completion. ICOs would be responsible for identifying and monitoring training for the appropriate staff
- Implement the Employment Eligibility Verification System (EEVS) should its use become federally mandated
- Develop and implement continuous monitoring mechanisms to help identify individuals/units that would benefit from additional training
- Automate file maintenance processes

Finally, they are working in consultation with the Office of the General Counsel to verify the proper retention period for I-9 documentation in accord with federal regulations. Once the retention period has been clearly defined, Standard Practice Guide section 201.46 Personnel Records – Collection, Retention, and Release will be modified to include the specific detail.

University Audits will review progress made on identifying and training employees with I-9 verification responsibility during the first quarter of fiscal year 2009.

Health System

University of Michigan Health System Human Resources Fiscal Responsibilities

#2008-209

Issued January 21, 2008

University of Michigan Health System Human Resources (UMHS HR) administers a full range of personnel services, including recruitment, employment, and salary administration to non-faculty staff at U-M Hospitals and Health Centers (UMHHC). In addition, it provides certain human resource support services for non-faculty staff at the U-M Medical School, University Health Services, and Michigan Health Corporation. UMHS HR's mission is to deliver innovative human resource services that recognize, value, and enhance both the employees and the University of Michigan Health System.

The Chief Human Resource Officer-UMHS proactively requested this audit be completed to review department processes and procedures, and identify opportunities for improvement.

The objective of this audit was to assess whether UMHS HR has adequate procedures and practices to monitor and control the following fiscal processes:

- Procurement (P-Card, Purchase Orders, and Non Purchase Order Vouchers)
- Cash and Cash Equivalents Handling
- Payroll and Form G Controls
- Conflict of Interest/Commitment Management

University Audits and UMHS HR staff cooperated to identify opportunities to improve internal controls governing payroll and other key processes.

A review of P-Card expenditures and other procurement activity revealed that purchases are supported with adequate documentation, expenditures are for University-related business, and P-

Card Statements are properly reconciled and approved. There is minimal access to cash and cash equivalents.

Opportunities for improvement include strengthening controls to ensure:

- Time reports are properly completed, authorized, and managed
- Time reporting codes are not changed without proper authorization
- Payroll verifications and reconciliations are performed timely, and properly reviewed and documented
- Attendance, including employee leaves of absence, is properly monitored, documented, and managed

Management can also strengthen the internal control structure by ensuring that:

- P-Card holders do not allow other individuals to purchase goods or services on their P-Cards
- Conflicts of interest/commitment forms are completed and adequately managed
- Key business processes are documented and communicated to the appropriate staff members

Detailed observations and action plans are contained in a separate Management Advisory memorandum. University Audits will perform a follow-up review during the first quarter of fiscal year 2009 to assess progress of action plan implementation.

Information Technology

Medical Center Information Technology (MCIT) Arbor Lakes Computing Facility #2008-307
Issued December 20, 2007

The Arbor Lakes Computing Facility (ALCF) is owned by Medical Center Information Technology (MCIT) and managed by MCIT's Technical & Operations Services (TOS) team. The facility was brought online in the spring of 2006. It is located on the ground floor of Building 2 of the Arbor Lakes complex.

ALCF primarily houses MCIT and Michigan Administrative Information Systems (MAIS) computing equipment. It is currently serving as a mirrored computing site to the Taubman Machine Room and an alternate machine room for a number of other units throughout U-M.

While the TOS team manages the facility, they do not manage the individual systems within the room. Departments and groups that own servers housed in ALCF are responsible for their management. TOS has a standard agreement for all entities housing equipment within ALCF.

There are a number of critical applications housed at ALCF including CareWeb, the MAIS purchasing and payroll systems, and CareLink, the Health System order entry system.

Three units provide security for ALCF.

- Hospital Security, the first responder for ALCF, provides support from two locations a) from their main security office at U-M Hospital, and b) from their location across the street from Arbor Lakes at the East Ann Arbor Medical Center.
- Information Technology Central Services (ITCS), the primary steward of Arbor Lakes, has an on-site, contracted, security staff available 24 x 7.
- The Department of Public Safety (DPS) provides on-call security response, as well.

Alarms for the Machine Room are monitored by TOS, Building Automation Services (BAS), Hospital Security, and DPS. TOS and BAS both monitor all environmental alarms, the uninterruptible power supply, and the generator. BAS also monitors the ventilation system, cold water pumps, and a number of other building and environmental related points. Hospital Security monitors exterior cameras, and the internal and external door alarms. DPS monitors the fire alarm system.

The long-term goal for this facility is to serve as an unmanned, backup machine room to the new facility that MCIT is currently planning. Until that time, it is a fully-manned production environment.

This audit included an examination of security and physical access related to ALCF, and an examination of the configuration, utilities, and environmental processes within the room. Support and facility systems directly impacting ALCF were also reviewed. This audit does not address logical access to the systems housed in ALCF, or the security of the systems themselves.

The objectives of this audit were to ensure the ALCF and its supporting systems were appropriately controlled and safeguarded against failure. University Audits:

- Reviewed and tested the physical protection of the Machine Room
- Reviewed environmental support systems
- Reviewed and tested monitoring systems
- Reviewed systems, policies, and procedures in place related to the Machine Room's power supply systems
- Reviewed and tested emergency response procedures and agreements

Generator Plaza Security

Control Issues:

- Motion Detectors - On July 31, 2007, University Audits performed a test of the physical access controls over the MCIT Machine Room generator plaza (an outdoor, restricted access, in-ground space housing Machine Room support equipment) behind Arbor Lakes Building 2. Upon gaining entry to the plaza, it was noted that there were no motion sensors in place.

Management Plan - MCIT submitted a capital request to accomplish this on May 24, 2007. We have set-up agreements with UMHHC Security Systems Project Manager for the monitoring of these detectors. The motion detectors will turn on the lights in the generator plaza area, as well as alerting UMHHC Security. We will investigate the possibility of having the alarm report to the TOS monitoring room as well.

- Generator Access - Inside the generator plaza there is a large diesel engine that serves as a power generator for the Machine Room in case of an outage. The generator is covered by a shed type structure with doors along two of the four sides. These doors were found unlocked and easy to access. An individual with access to the generator and malicious intent could disable it. In the event of a power outage, a disabled generator would require systems in ALCF to be shutdown, causing an extended service outage.

Management Plan - All access panels to the generator housing and fuel tank have been secured with keyed pad locks. Keys are kept in a key box within the TOS monitoring room.

Auditor's Comments: This issue was resolved during the course of the audit. We have verified that the doors are now locked. **This issue is closed.**

- Water Pump Valves - There are water pumps located in the generator plaza. These pumps feed cold water to the cooling system for the Machine Room. Valves on intake and output pipes are easily accessible and not properly secured. A closed valve could cause the Machine Room to overheat potentially leading to system loss and service outages.

Management Plan – Management agrees with this assessment. A capital request will be entered to secure the valves.

Machine Room Security

Control Issues:

- Loading Dock Doors - There are two sets of loading dock doors that lead directly into the Machine Room from outside. The doors are hollow, and close into each other, with no center support or reinforcement. The inherent weakness of the door, combined with lack of proper reinforcement, provides a potentially easy break in point. There are contact alarms on the doors that are monitored by U-M Hospitals and Health Centers (UMHHC) Facility Control Center (FCC). A contact alarm senses when the door is in contact with the doorframe. When contact is broken, the alarm is triggered. According to procedure, there is no response to these alarms between 8:00 am and 5:00 pm. Physical access to the Machine Room increases the risk of hacking, and adds a risk of theft or destruction of property.

Management Plan – Management agrees with University Audits' assessment. They will contact UMHHC Security to change monitoring times to 24 x 7. TOS Manager will also investigate the possibility of having the alarm enunciate in the TOS Monitoring Room. A capital request will be put in to have the doors replaced and the mullion installed.

- Computer Room Access Lists - A list of individuals with access to the Machine Room is maintained by UMHHC Security in conjunction with MCIT, Orders Management Project (OMP), and Michigan Administrative Information Services (MAIS). All updates to the list come from MCIT, OMP, or MAIS, and go to UMHHC Security. UMHHC Security then distributes the updated list back to the other three groups. While this serves as an informal review, there is no formal review process in place for the access list. An individual on the access list who should not have access poses a risk to the security of the Machine Room.

Management Plan - The Manager III / MCIT-ISO-TOS, who is responsible for the access lists from MCIT's side, will set up a monthly meeting with other involved parties to review the lists.

- Unauthorized Access - Physical access to a computer greatly increases the ease and speed with which an unauthorized person can compromise that computer. As part of a test of physical access, a University Audits staff member was able to gain unauthorized access to the Machine Room using social engineering techniques. Social engineering is the act of posing as an authorized person, and relying on people's good will and desire to help in order to obtain access to information that the individual is not authorized to have. In this case Audits obtained a contractor's logo shirt, and posed as a service technician from that company. Gaps in policy and failure to follow procedures allowed this unauthorized access.

Management Plan - MCIT and the TOS group have made some procedural changes to prevent unauthorized access from occurring again. Call Center staff no longer have access to the Machine Room. This will keep an untrained staff member from inadvertently allowing someone inappropriate access. All TOS staff now have access to the Machine Room and are responsible for controlling access to it.

Management also strengthened existing procedures and reiterated their existence and importance with their staff members. TOS staff will check for Remedy tickets for all vendors requesting access. If an appropriate ticket is not available in the Remedy ticketing system, staff have been instructed to contact the U-M account manager associated with the vendor to ensure that the visit was expected. If appropriate access cannot be verified, the vendor will not be allowed into the Machine Room.

These changes took place immediately after we were informed of Audits' access.

Auditor's Comments: This issue was addressed during the audit. **This issue is closed.**

- Unlocked Server Cabinets - As part of an access controls test, a University Audits staff member entered the Machine Room using social engineering techniques. It was noted during this exercise that server cabinets were left unlocked. While controlled access to the Machine Room does mitigate risk relating to physical access to the servers, locked cabinets provide an added layer of security in case an unauthorized person manages to enter the room.

Management Plan - The cabinets and servers in the Machine Room are the property of the individual groups managing them, not ALCF. TOS management will send a memo to all groups with equipment in the room suggesting that cabinets should be locked. It will also be noted that groups not locking their cabinets are accepting the risk of doing so. We will add a copy of the memo into the Machine Room documentation so future groups bringing equipment in will get a copy.

- Video Monitoring - There are a number of cameras in the ALCF Machine Room and the generator plaza monitoring these facilities at all times. The video feed from the cameras in the generator plaza are sent to both the TOS and the FCC for monitoring. The feed from the cameras within the Machine Room goes only to the TOS. Although live feeds are rarely monitored, the feeds to FCC are recorded. In addition, the TOS is not staffed 24 x 7, and monitoring the camera feeds is not part of any staff member's regular duties. The feeds from within the Machine Room to the TOS are not recorded, and none of the cameras are equipped with motion sensors to alert monitoring staff of activity. Failure to monitor and/or record the video feeds from the cameras renders them ineffective.

Management Plan - MCIT is in the process of implementing sensor grid technology to our monitoring cameras. This will allow us to alert staff in the TOS monitoring room when there is motion within a camera's field of view. They are also implementing a recording solution tied to the sensor grid technology. Video from any camera sensing motion will be stored from 10 seconds before the motion, to 10 seconds after.

Safety

- Lack of Disaster Recovery Plan - A thorough disaster recovery plan is a necessity in any area that deals with critical business applications. A number of mission critical application servers, including MAIS payroll, CareWeb, and CareLink are housed at

ALCF. Quick recovery from any outage is imperative. There is currently no formalized Disaster Recovery Plan in place for the Machine Room.

Management Plan - MCIT will develop and fully test a Disaster Recovery Plan for the Arbor Lakes Computing Facility, focusing on all mission-critical applications.

- Arbor Lakes Complex Fire Safety - The Machine Room and its supporting areas in Building 2 are controlled by MCIT. The rest of Building 2 and the Arbor Lakes complex are controlled by ITCS. Because the Machine Room is part of the Arbor Lakes complex, it depends on not only its own safety measures, but also on those of the facilities around it. A fire elsewhere in Building 2 could cause great harm in the Machine Room. The lack of any automated fire suppression systems in other parts of Building 2, and Arbor Lakes as a whole, creates greater risk for the Machine Room.

Management Plan - Arbor Lakes Facilities will setup a meeting with MCIT, the U-M Fire Marshall, and other interested parties to discuss improving fire safety at the Arbor Lakes complex, especially in close proximity to the Machine Room.

- Fire Panel Upgrades - The Simplex (third party vendor) fire panel installed for the ALCF Machine Room has the capability to use a "direct line" to communicate with a monitoring facility. The direct line allows for a detailed report to be passed on to monitoring staff. This technology is currently in use at the East Ann Arbor facility, and is reporting to the UMHHC FCC. The Machine Room was originally designed to report over a direct line to FCC. Currently, the fire alarms are reporting to DPS through the building's MOSCAD (Motorola Supervisory Control and Data Acquisition) system. While this does alert first responders, it only informs them that there is a problem. A detailed report would tell them what the problem is, and where it is occurring. Detailed reports would lead to faster, more accurate responses.

Management Plan - A Capital Request has been opened to complete the work required for direct monitoring of ALCF fire alarm panel from UMHHC FCC. An investigation has been started that will ascertain the scope of the work required and an estimate of the costs. After the investigation has been issued and the budget approved construction documents will be issued. Until the investigation work scope is completed, modifications to the fire alarm panel will be made so the panel can be monitored off-site by Simplex.

- Battery Room Spill Guard - Safety is always a vital concern when hazardous materials are in use. The backup batteries for the Machine Room are wet cell, acid batteries. Because of the acid, these batteries are a potential safety hazard. The batteries are serviced by Zone Maintenance. An emergency shower is in place in case of an accident. There is no spill guard in front of the door to keep acid from spilling into the hallway in the event of an accident.

Management Plan - The IT Mgr Healthcare for the TOS will submit a capital request to have a spill guard installed.

- Safety Shower Test Requirements - A safety shower is provided in the UPS battery storage room that supports the Machine Room. Testing requirements for both UMHHC Safety Management Services and Campus OSEH state that safety showers must be tested annually. Weekly testing is also suggested (to prevent water stagnation), but not required. This test must be recorded either on a tag on the shower, or on a log nearby. Michigan Occupational Safety and Health recommends that maintenance perform other

specific monthly and annual tests as well. There is currently no regular testing performed on the safety shower.

Management Plan – Management will contact Zone Maintenance to have the monthly and annual testing started. They will also speak with Zone Maintenance about performing the weekly testing for the TOS group. A log will be created to be kept near the shower to log these tests.

The Arbor Lakes Computing Facility poses a number of unique challenges. It is a UMHHC administered room within a Campus owned building. Arbor Lakes Building 2 was remodeled to accommodate the Machine Room. The space is not ideal. During the construction project, the project manager left. These challenges, coupled with communications problems, are the source for many of the audit issues.

Communication will continue to be key to ALCF's role as a shared computing facility housing critical applications because of the number of units impacted by the facility. University Audits observed communication breakdowns in a number of areas. Documents reviewed during the audit showed that most of these problems occurred during the construction of the facility. Many of the groups involved with ALCF continue to feel their effect. It would be beneficial to all parties involved if a standing committee met on a regular basis to discuss matters concerning ALCF. Members of this group should include MCIT, UMHHC Facilities, Campus Facilities, UMHHC Security, and DPS. Other groups, such as OSEH and Zone Maintenance, could be included, as necessary.

At the request of MCIT, University Audits performed a review of the enunciation of, and response to, fire alarms originating in ALCF. The alarms are reporting, but not as originally designed. Despite this, UMHHC Security and DPS both respond to the calls to ensure the safety of those working at Arbor Lakes. The processes of who responds and how needs to be clarified. Efforts have been made by Campus Facilities, Hospital Facilities, UMHHC Security, MCIT, and ITCOM to resolve this issue. University Audits is pleased with the cooperation and urgency all groups are showing in resolving this issue.

University Audits found that controls within the Machine Room are well monitored by MCIT. MCIT needs to increase monitoring and recording of video from the cameras in the Machine Room. Both TOS and Building Automation Services (BAS) are doing an excellent job monitoring the environmentals within the Machine Room. BAS is also monitoring the environmentals in support rooms. TOS also has a robust system in place to look for abnormal behavior among MCIT servers in the Machine Room.

The power setup for ALCF is well designed and implemented. All power is routed through the uninterrupted power supply, ensuring it is well conditioned. There is enough battery power to give the generator time to power up or bring the servers down safely in the event of generator failure. The system is entirely automated and monitored from within TOS monitoring.

A formal follow-up to the outstanding issues will be conducted during the fourth quarter of fiscal year 2008.

Healthcare

FOLLOW-UP REPORTS

Recreational Sports Business Office Internal Control Review

#2007-813

Original Report issued February 20, 2007

Follow-up Report issued December 18, 2007

During the original audit, testing procedures were limited to the business office at the Intramural Sports Recreation Building; however, REC Sports management applied their corrective actions to the business offices at all three recreation buildings (North Campus Recreation Building, Central Campus Recreation Building and Intramural Sports Recreation Building), as well as the Outdoor Adventures Rental Center. As part of follow-up, University Audits performed detailed testing at all four locations where business is conducted to verify that updated procedures effectively improve controls over the following processes:

- Cash Handling
- Credit Card Processing
- System Back-up and Recovery
- Imprest Cash Fund Management
- Time Report Authorization
- Inventory Tracking
- P-Card Processing

REC Sports has adequately addressed all concerns raised during the audit. See summaries below for additional information. **This audit is closed.**

Cash Handling Controls

REC Sports staff completed the training for the new depository procedures. For all four business locations:

- Revenue is reconciled daily and reviewed by a second individual prior to depositing
- Deposits are being made according to agreements with the Treasurer's Office
- Access to cash has been reviewed and limited as necessary

Team fees, locker sales, and continuing memberships are being reconciled to source documentation on specific high-volume dates. The senior accounting clerk reconciles the Statement of Activity monthly. Cash handling and reconciliation procedures are documented.

Credit Card Processing

Credit card refunds are now being reviewed and approved prior to processing. Each time a refund is processed, an email is sent to notify the business manager. The business manager reviews the online Fifth-Third credit card statements for refund activity and verifies appropriateness with the approver for a sample of refunds once per month. Procedures ensure that refunds are processed to the same credit card used for the original purchase. Hard-copy documentation with complete credit card numbers is adequately secured and shredded appropriately. Credit card refund procedures are documented.

System Back-up and Recovery Procedures

The Disaster Recovery Plan has been updated to include more specific information and cover all of the REC Sports systems. Procedures for the use and maintenance of the membership editor and breakdown systems are documented.

Imprest Cash Fund Management

The funds from the internal petty cash account have been deposited into an appropriate REC Sports account; a reminder not to maintain such funds was sent to all REC Sports staff. The balances of all REC Sports imprest cash funds are now consistent with Accounts Payable records. Controls over imprest cash funds appear to be adequate. Cash is adequately secured and reconciled daily.

Time Report Authorization

A document listing the authorized signers for time reports by employee was provided to the time administrator to help ensure appropriateness. All time reports reviewed during follow-up were signed by the appropriate higher authority.

Inventory Tracking

REC Sports acquired a new Point of Sale (POS) system to track and account for their equipment room sales. The first count of inventory for all equipment rooms was performed in October 2007. Inventory counts and reconciliations to reports generated by the POS system will be performed quarterly. Inventory reconciliations for the rental equipment at Outdoor Adventures Rental Center are also performed quarterly. Guest passes are being controlled centrally; individual sales are tracked at each location. All inventory procedures are adequately segregated and documented.

P-Card Processing

REC Sports management reviewed and reduced P-Card credit and transaction limits as necessary. P-Card statement reconciliations and approvals are performed monthly by appropriate individuals. Overall, P-Card transactions sampled were consistent with University guidelines; REC Sports management agreed to enforce the requirement for complete itemized hotel bills for all lodging expenses to verify expenses are appropriate and charged to the right account.

Office of the Provost and Executive Vice President for Academic Affairs Fiscal

Responsibilities

#2007-201

Original Report issued July 16, 2007

Follow-up Report issued December 19, 2007

Management has implemented several positive changes as detailed below:

Academic Administrative Search Expense

University Audits recommended fiscal controls over academic administrative searches be improved to include the establishment of a budget for each search. Additionally, all parties involved in a search should comply with University travel, hosting, and alcohol policies. The Office of the Provost has made significant improvements in this area. Detailed budgets are now established for each search. These budgets are approved by the chief of staff. All search expenses are reviewed in detail with a periodic comparison to budgeted amounts. Consulting contracts now contain specific language regarding meal limitations and alcohol purchases.

Statement of Activity Reconciliation

Statement of Activity reconciliations were being performed by a person who made most of the purchases for the office without any review by an independent person. A newly hired financial specialist has begun to perform reconciliations of the Statements of Activity. He does not make purchases for the office. Additionally, Statements of Activity are now being reviewed by the chief of staff.

Lack of Documentation of Policies and Procedures

University Audits recommended detailed policies and procedures should be documented for key office functions. The chief of staff provided several office policies and procedures. The staff will continue with their efforts to document all critical functions.

Management has taken appropriate corrective action on all audit recommendations. **This audit is now closed.**

Plant Operations Zone Maintenance Purchasing

#2007-812

Original Report issued April 24, 2007

Follow-up Report issued December 21, 2007

Status of the outstanding audit issues and corresponding corrective actions are detailed below.

Purchasing Approval Process: Management established and implemented an overall procurement policy throughout Plant Operations, with input from central University offices. Specifically, they created a P-Card usage policy, trained all P-Card holders, and held a separate training session for all P-Card reconcilers and approvers.

One component of the new policy requires pre-approval from a P-Card holder's supervisor for P-Card transactions above \$500. However, documentation of the pre-approval was not retained for the sample tested during follow-up review. Management should clarify pre-approval procedures with employees and supervisors to ensure consistent application across the division.

Inventory Receiving and Tracking: Plant Operations has updated the New Employee Checklist used to document information, equipment, and tools provided to employees, but the checklist has not been implemented. Procedures for usage and retention of the checklist should be reviewed with supervisors to clarify expectations.

The inventory receiving process has been largely centralized. Items are typically shipped to the central receiving dock, and then delivered to central locations for shops throughout the campus. Management is in the process of evaluating inventory tracking and equipment management programs for implementation within Plant Operations.

P-Card Administration: Management has updated the Plant Operations P-Card Policy and reduced the number of P-Cards within the division. Additionally, P-Card limits throughout Plant Operations were reviewed and adjusted based on purchasing needs. Management has also instituted a monthly random sample audit process for P-Card transactions. **This issue is closed.**

Monitoring Controls over Purchasing: Facilities Maintenance management has established monthly financial planning meetings to review purchasing concerns and other financial matters. Reports are generated monthly to analyze PO, non-PO, P-Card, and service unit billing activity. Management is also reviewing alternatives which can be used to perform additional trend analysis. **This issue is closed.**

Management has implemented corrective actions relative to P-Card administration and monitoring controls. Corrective actions related to inventory receiving and tracking, and the purchasing approval process have not been fully implemented. University Audits will continue to monitor the progress of the open issues with a second follow-up review during May 2008.

College of Engineering, Multicultural (formerly Minority) Engineering Program Office

#2006-813

Original Report issued September 29, 2006

Follow-up Report issued January 11, 2008

Management has implemented positive changes as detailed below.

- Collaboration with Resource Planning & Management (RPM):
Management has increased the collaboration and communication between Multicultural Engineering Program Office (MEPO) and RPM. A senior manager in Engineering administration worked with the MEPO Director and MEPO Staff to enhance management skills and review management practices. RPM staff worked with MEPO staff to develop financial management systems. The director of MEPO was personally involved in approximately forty training sessions and meetings (many teleconference) with the senior manager in Engineering administration and/or RPM between September 2006 and April 2007.

The new business manager role, with MEPO administrative responsibility, has joint reporting lines to the Associate Dean for Academic Affairs and to the Executive Director of Resource Planning and Management to ensure strong communication.

- Conflict of Interest (COI):
COI training was conducted for all staff when the policy was first introduced and the College of Engineering (CoE) is planning to rollout online training in the future. Employees sign COI certifications as part of their annual performance evaluation.
- Expense Reconciliation, Project Grant Management and Approval:
The Director is now approving all unit expenditures. Project grants are reconciled against source documentation. CoE management has assigned a new business manager to work with the department to strengthen controls. The new business manager has made a significant step forward in implementing new controls to ensure appropriate project grant budget management.
- Contract Management:
All partnership and affiliation agreements with external parties (including independent consultants) are reviewed by the business manager. Once the business manager has reviewed the agreements, final approval must be obtained from the Director.
- Payroll Processes:
Progress has been made in the appropriate processing of payroll documents. Temporary employees are now required to sign their own time cards and supervisors are now reviewing time reports for accuracy prior to authorization. Time reports are now reconciled to the Gross Pay Register on a regular basis.
- Employment Procedures
New employment procedures have been created and implemented by management. Management will continue to gather information on procedures used by other departments for screening applicants, conducting evaluations, setting pay rates, and verifying student enrollment status. Based on this information, they will continue to work to refine their processes.

- Equipment Inventory
Management has developed a comprehensive equipment inventory with description, location and, when available, serial numbers. Check-out and return of equipment is documented.
- Gift Processing
The Development Office agreed to provide MEPO with copies of all original gift documentation to aid MEPO in its gift reconciliation efforts. RPM also agreed to supply MEPO with a copy of the weekly gift record report received from the central Development Services Office via the CoE Development Office. The business manager of MEPO will continue to work with the CoE Development Office and RPM to streamline the reconciliation process.

MEPO has sufficiently strengthened its internal control structure to support its business operations, safeguard its assets, and promote compliance with U-M policies and procedures. MEPO management has finalized a mission statement and detailed organizational chart. Program objectives have been clarified and management has defined program metrics that will be used to evaluate the effectiveness of the program.

This audit is closed.

Procurement Services P-Card Program

Original Report issued February 5, 2007

#2007-115

Follow-up Report issued January 22, 2008

Procurement Services management responded by implementing major organizational and process changes to improve controls, achieve greater operational efficiency, and provide improved service to P-Card holders and approvers. While some of the actions undertaken are in process due to large-scale initiatives, controls are significantly improved in each of the areas addressed by the audit report. Procurement Services management has leveraged a strong partnership with Internal Controls Compliance management in the Office of the Associate Vice President for Finance (AVPF) and obtained the services of accounts payables specialists to support successful completion of in-process improvements. In consideration of these factors and actions described below, **this audit is closed.**

1. Utilization of Data Mining Resources
 - a. Procurement Services has developed an electronic exception auditing application and a supporting P-Card auditor process. Criteria for selecting potential exceptions include:
 - Transactions included in monthly P-Card statements with a balance greater than \$4,500
 - Individual transactions greater than \$700
 - Prohibited purchases identified by merchant category codes
 - Split transactions, which are single purchases charged over several days to circumvent the \$5,000 per transaction limit set by P-Card policy.

Additional exception criteria are being considered for development.

When P-Card auditors identify an exception transaction in the auditing process, an automated e-mail notification is generated and sent to cardholders and approvers. The exceptions will be tracked and trended through the application and grouped by P-Card holder, P-Card approver, and University unit. Reports of these exceptions will be available to both Procurement Services and individual unit management. P-Card exception auditing is in the pilot phase, reviewing transactions from February

through June 2007. P-Card statements from June 2007 through completion of the pilot continue to be audited manually on a current basis.

- b. The Accounts Payable office is returning all cardholder statements that are incomplete or require correction to the responsible cardholder and approver with a form explaining required corrections. Accounts Payable tracks returned statements for follow-up action.

2. Training, Support, and Accountability for P-Card Approvers

The development of P-Card approver training is progressing with a target completion timeframe of late February to early March 2008. AVPF Internal Controls Compliance and Procurement Services management are working together to ensure that training addresses all relevant internal controls. P-Card approver signatures on P-Card statements will be accompanied by a pre-printed attestation that they have taken the P-Card approver training. Training emphasizes that the approver is the "critical control" and indicates that the responsibility and accountability of the approver is equal to that of the P-Card holder for ensuring that transactions are allowable expenses and consistent with University policy. Training will also provide information for addressing issues when transactions are not allowable or consistent with policy. Additional reports are being developed to assist approvers in meeting their responsibilities for reviewing all transactions and tracking cardholder exceptions.

3. Card Issuance Criteria

Procurement Services management worked with departments to perform a review and reduce card liability as part of the migration to a new P-Card service provider in early summer of 2007. Procurement Services will perform an annual review of card usage to identify unnecessary cards or cards with excessive monthly credit limits. Procurement Services management has developed a process for approval of temporary and permanent card spending limit increases.

4. Utilization of Electronic Resources

To improve efficiency and controls through electronic resources, Procurement Services:

- a. Identified requirements and developed a model for an online application that will be used to apply for P-Cards. This new online application has the potential to interface with both M-Pathways and GE systems. This will improve process efficiency, minimize P-Card approver manual procedures, and provide the opportunity for system-embedded controls related to expenditure limits and cardholder information. Implementation of the application is scheduled for calendar year 2008.
- b. Imaged P-Card statements and supporting documentation which is now available for review on the University's WebNow site. Imaging supports faster turnaround for making central P-Card documentation available to units and electronic P-Card exception auditing.
- c. Hired a project manager and assigned resources to assist with the procurement and implementation of an automated Travel and Expense application. The application will support system-embedded controls and reduce manual, paper processing of documents. An RFP was issued, proposals have been submitted, and Procurement Services management is negotiating with vendors.

The UMHS Hospital Collection Agencies audit report was issued on October 10, 2007. University Audits completed a follow-up review to assess management's progress in addressing issues identified in the audit report. All corrective actions have been completed or are well underway. **This audit is closed.**

1. Collection Agency Fee Review

Management implemented a process of tracking patient accounts sent out to agencies for pre-collection. This process compares the accounts sent for collection to invoices to ensure that agencies are correctly billing for services rendered. Written procedures were also developed.

2. Hospital Fee Collections

Hospital Patient Accounts contacted Universal Credit Inc. advising of contract terms requiring return of all patient accounts after twelve months of inactivity. In addition, Patient Accounts is working to develop a report that will allow monitoring of the age of patient accounts held at outside agencies. This report will be put into regular production after the HealthQuest upgrade in March 2008.

3. Policies and Procedures Documentation

Management developed and implemented written policies and procedures for:

- Data transfer and balancing
- Collection agency invoice review and payment
- Account closeouts
- Account transfers from primary to secondary placement agencies

4. Account Transfer Confirmation and Reconciliation

Management developed reconciliation and confirmation processes to ensure that payments received and accounts sent out to collections are balanced with information contained in the HealthQuest patient accounting system.

Intercollegiate Athletics Sports Camps Second Follow-up

Original Report issued July 28, 2006

#2006-410
Follow-up Report issued January 28, 2008

The follow-up process was performed in two phases:

- An initial follow-up to ensure that action plans were on track to be fully implemented for the summer 2007 camp session.
- A second follow-up after the summer 2007 camp session to review support documentation for new procedures.

Results from the initial follow-up were detailed in a Memorandum issued on May 30, 2007. Results from the second follow-up are detailed below. Athletics management has adequately addressed all audit report issues. **This audit is closed.**

- Background Checks: Criminal and sex offender background checks are performed on all camp employees. Camp directors are required to submit a roster prior to the start of the camp. Athletics compares the rosters to the returned background check forms to ensure that background checks were appropriately completed for all employees.
- Contracts: A proposal to approve the summer 2007 and 2008 camp contracts was reviewed by the associate Vice President for Finance and the Office of the General Counsel, and will be submitted to the Regents for the February 2008 Board meeting. Camps and clinics conducted during the school year will now be required to sign a contract with Athletics. While the clarity of

contract documentation has improved, additional attention to camp contracts will help ensure they are all signed by the Department of Athletics.

- Reconciliation of Deposits and Payments: Athletics appropriately reconciled the deposits and staff payments to camper and staff rosters for a sample of 2006 and 2007 summer camps. However, starting with the 2008 camp season, all camps will be operating externally; therefore, this process will no longer be necessary.
- Time Away Policy: Athletics' Human Resource Officer contacted individual employees that were also employed at camps upon receiving their time sheets to verify time was reported according to the new policy. Going forward, the human resources officer will continue to review timesheets from June through August for employees working at camps. To help ensure all employees are monitored, camp directors will be required to send a list of all U-M employees working at their camps. A reminder regarding the time reporting policy will be sent prior to the start of the camp season.

University of Michigan Computing Environment Kerberos Passwords and Uniqname #2007-304
Original Report issued June 22, 2007 Follow-up Report issued January 31, 2008

Management has addressed the open issues through implementation of several positive changes as detailed below:

Kerberos Upgrades:

The Kerberos Network Authentication Protocol is currently at version 5. Although this version is in widespread use at U-M, there were still a number of processes and servers using version 4, a significantly less secure version than 5. UMCE has reduced the number of processes using version 4 from sixteen to four. The number of servers using the old version has been reduced from eight to two. These servers and processes have been isolated, and will be moved to version 5 by April of 2008. **Closed**

Pre-Authentication:

At the time of the audit, UMCE Kerberos was in the process of implementing a technology called Pre-Authentication. This technology increases the security of the Kerberos Protocol by eliminating the effectiveness of a common hacker technique. This project is nearly complete. Only 1% of usernames are left not currently employing Pre-Authentication. Efforts to complete this implementation are ongoing. **Closed**

Additional Programs on Kerberos Servers:

The servers housing Kerberos are currently also housing the Andrew File System (AFS) used across campus. Having multiple programs running on a single server creates a greater potential for security issues. While AFS is a secure application, and risk of vulnerability is low, University Audits recommended housing it separately from Kerberos. UMCE researched moving these two applications to separate servers and determined that it is not currently feasible. They are aware of the potential security risks, and are taking measures to mitigate them. University Audits agrees with their assessment. **Closed**

Patch Tracking:

Patch tracking has been done by the System Administrator Intermediate and Software Engineer Senior as an official part of their job. The process is adequate, but was undocumented. A formal methodology for tracking and applying the patches has been placed in the UMCE process collaborative website (wiki) to ensure consistency over time. **Closed**

Disaster Recovery Plan:

During the audit it was noted that no formal Disaster Recovery Plan (DRP) existed for Kerberos. UMCE noted that ITCS had been working on a DRP for pandemic flu. This was to be the base for building the Kerberos DRP. UMCE did not have a draft DRP available for the follow up. University Audits reviewed

a Business Continuity Plan (BCP) that had been prepared and a Security Plan that was developed for Information Technology Security Services. Neither document addressed the issues created by the lack of a DRP.

Program Access Control:

Kerberos security can be utilized by programs as well as users. This is done using keytabs. While keytabs themselves are not a security risk, they open a door for malicious users. A review of keytabs was performed after the completion of the audit. UMCE staff identified 8,000 keytabs that were either unused or out of date and removed them. There are currently less than 4,000 still in use and these are evaluated on an on-going basis. **Closed**

Potential Creation of Duplicate Uniqnames:

A user could create multiple identities because of the methods used to create unqnames. UMCE is addressing this issue by implementing the new M-Community module in M-Pathways. M-Community is currently in its testing phase, and will be implemented in June along with the updates of HE-Prod. The team has already completed three phases of testing and is preparing for their fourth. **Closed**

Management has taken appropriate corrective action on most of the audit recommendations. The Disaster Recovery Plan recommendation was not addressed and an additional follow-up will be performed on this issue during March 2008.

Digital Media Commons CTools

Original Report issued June 29, 2007

#2007-301

Follow-up Report issued January 31, 2008

The following are outstanding audit issues and corresponding corrective actions taken by management:

Administrator Privileges: Any CTools administrator can create or promote other accounts to administrator status. Management is advocating, in the Sakai Community, the division of administrative activities into separate privilege levels (e.g., the right to promote accounts to the administrator group). This segregation of duties feature will be prioritized as part of U-M CTools implementation activities along with other sought-after features, including some that have been specially funded by campus units. New developers are being added to the project to speed improvement.

The CTools Project Lead is using reminders on his personal Outlook calendar to prompt periodic review of CTools administrator accounts for appropriateness and other new security reviews. He will move these reminders to a shared calendar that can be monitored by other project staff to ensure the reviews are performed if he is absent or otherwise unable to perform them. He has also constructed a wiki (collaborative website) where the reviewer records any actions taken as a result of this or other security reviews.

A future release of the Sakai Project, on which CTools is based, will also be able to group sites hierarchically. With this ability, management could more easily grant CTools field-support personnel the right to administer only sites in the college or department they support. **Closed**

Persistence of Login Sessions: Users logging out of CoSign (Weblogin) are not logged out of CTools. This is contrary to other CoSign-enabled U-M services such as Wolverine Access. As an interim solution, a notice advising users of the need to quit the web browser in order to fully terminate their CTools session was posted on CTools as of January 17, 2008. This notice is visible both when arriving at the CTools site and after logging out of CTools. Users who heed the notice will be protected.

The permanent solution, reprogramming the CTools implementation of CoSign, has not been completed. Information Technology Central Services (ITCS) has allocated personnel to assist the CTools

Implementation Group with this task. This will be discussed at weekly CTools working group meetings until development has been scheduled and prioritized.

Log Review: CTools logs were not used to proactively identify unusual or abnormal activity in CTools. CTools Operations (CTOps) is profiling system usage to aid in capacity planning and increase application stability, both of which impact service availability. The CTools Implementation Group and CTOps will discuss and identify activities or measures within the CTools application that, if monitored, could improve control and oversight. Audit trails will be implemented as needed to allow specifics and/or trends in those activities to be recorded, observed, and acted upon. CTOps will initiate the analysis of monitoring needs from an application/operational perspective, and the CTools Implementation Group will contribute code to implement them.

Authorization of Outsider Access: The access privileges accorded Friend Account IDs, issued to outside collaborators, were not centrally managed or monitored for abuse. The CTools Implementation Group has begun collecting monthly CTools login statistics for Friend Accounts. Accounts that are used excessively can indicate use by more than one person or abuse. The CTools Project Lead investigates the activities of such accounts when found. Current data indicates the average Friend Account holder logs in to CTools fewer than 100 times per month, but can range as high as 200 to 300 times per month. As more data is collected and further trends are established, deviations will become easier to spot, thereby increasing the accuracy and efficiency of the review process. **Closed**

SLA between ITCS and Digital Media Commons: The service level agreement (SLA) between ITCS and Digital Media Commons (DMC) was outdated and unsigned. The SLA is unchanged. It will be revised after the new CTools governance board has been installed by the Vice Provost for Academic Information (as explained below).

Upgrade Approval Process: The process through which the CTools Advisory Committee authorizes upgrades to new releases of CTools was not consistently followed. Two organizational changes have been planned or made to enrich CTools governance.

The Digital Media Commons reorganized the CTools Development Group in November 2007 from two separately managed research labs into a single unit – the CTools Implementation Group. This group engages more frequently with the CTOps unit in ITCS, and its mission and objectives better reflect the position of CTools as a key component of U-M's academic infrastructure.

The Vice Provost for Academic Information will establish a new CTools governance board as part of a broader reimplementing of academic IT governance. The CTools Implementation Group estimates this board will be seated by Fall 2008. In anticipation of this, the CTools Implementation Group and CTOps will start developing thresholds of scope and significance at which changes will be brought before the board for approval. The final upgrade notification, review, and approval process will depend on the new board's desired level of involvement.

Integrity of Sensitive Data Exchanges: Students and instructors lacked proof of submission and proof of receipt for students submitting work through CTools. CTools now provides students with confirmation numbers and email notifications when they submit assignments to instructors. The unique identification number for the submitted assignment is shown on both the confirmation screen and the email message. Instructors can also elect to receive email notification of submitted assignments.

A planned feature automating the upload of grades from CTools Grade Book to Web Grades in M-Pathways carried the potential for unauthorized delegation of the grade input duty. Management anticipated this would require limitations on the right to perform or delegate grade uploads within CTools. The automated upload feature has not yet been finalized or approved for production by business

owners, but the CTools Implementation Group indicates that an upcoming Sakai 2.5-based CTools release will contain the programming code necessary to implement the anticipated controls. **Closed**

Size Limitations on Files and Sites: Limitations on the size of uploaded files, which can stem the illegitimate sharing of copyrighted material, was not applied consistently. Rather than standardize the file size limit, which could block educational material, management chose to pursue alternative metrics for controlling inappropriate file sharing. The CTools Implementation Group has developed a query for reporting the number of times each CTools resource – such as an uploaded file – is read during a given period. CTools Implementation Group is profiling this statistic so they can recognize and investigate extremely popular resources. Popularity can indicate that a resource may be inappropriate. To date, the resources flagged for inspection have been index files and other minor objects – not inappropriate content. The CTools Implementation Group will be upgrading the system to allow the query to report on resource size, as well as, to eliminate innocuous files and increase the value of query results. **Closed**

Management has taken appropriate corrective action on most audit recommendations. University Audits will review progress toward resolving the remaining open issues in April 2008.

College of Literature, Science, and the Arts Biological Station

#2007-205

Original Report issued August 6, 2007

Follow-up Report issued January 31, 2008

Management has implemented positive changes as detailed below:

Software License Information:

The University of Michigan Biological Station (UMBS) has a standard set of applications that are installed on all of its computers. The licenses for these applications are held and maintained by LSA Information Technology (LSAIT). UMBS also employs some specialized software that is licensed to the Station. During the audit it was noted that a comprehensive list of UMBS owned software and its installation points was not maintained. Subsequently, IT staff at UMBS have performed a software audit and created the necessary list. No license violations were found.

Data Transmission:

UMBS has staff in both Pellston and Ann Arbor. Because of this, they need the ability to send data between the two locations. Staff members were utilizing e-mail to accomplish this. University Audits recommended a change to this procedure because of the unsecure nature of e-mail. UMBS staff is now utilizing the shared network spaces provided by LSAIT as a means of transferring data between the two locations. All staff members at both locations have been trained on the new procedure.

Backups:

Backups at the Station in Pellston were the responsibility of individual users. Staff members have now been trained to use their shared drives, which are maintained and backed-up by LSAIT. A backup process has also been put in place for items stored on servers at the Station. While the local backup option is still available, users are now instructed to use the LSAIT servers to ensure that their backups are performed frequently and systematically.

Static IP Addresses:

The IP addressing scheme used for providing computers at the Station access to the network is maintained by the Resident Biologist. Static addresses were distributed at the beginning of the season for all students and faculty. A visitor wishing to use the internet had to be issued an IP address. Dynamic Host Configuration Protocol (DHCP) is now employed to automatically issue addresses to users. Students and faculty members are required to register their computer's hardware (MAC) address when they sign the acceptable use agreement. This provides the Resident Biologist the ability to track any inappropriate traffic on the network.

User Access:

UMBS does not currently employ a user authentication system. Staff machines have local accounts that users log into to keep unauthorized people from gaining access. Public use machines have generic logins for user access. It was recommended that UMBS employ a solution such as Microsoft Active Directory and use its user management capabilities. UMBS has decided that this is not currently a viable option as they are without a full time System Administrator. Potential risks have been explained to management, along with a less complicated way to minimize those risks. This alternative solution involves configuring the network so the public use machines could only access the internet, and not the Station network. This will address the concern of unauthorized access to network resources.

Atmospheric Tower Safety Forms:

There are three atmospheric towers used for research at UMBS. The Facet tower had excellent documentation and written procedures prior to the audit. This material has been modified for use on the AmeriFLUX and Prophet towers as well.

Handling of Building Keys:

Prior to the audit, Station keys were kept on a pegboard in the Facilities Manager's office. This office was generally kept unlocked during the day. Once the issue was pointed out, the door was kept locked at all times. UMBS management has subsequently installed a lockable key box for the storage of the Station keys. Additionally, a detailed key log has been created for both the Station, and the Ann Arbor office.

Deposit Transport:

UMBS office staff had been transporting deposits to the bank in standard envelopes. They are now using special deposit envelopes supplied by the U-M Treasurer's Office for their deposits.

Segregation of Duties:

Duties relating to tracking and ordering inventory in the UMBS Store were previously performed by the Office Manager. This created a segregation of duties problem. Dividing the process among multiple staff members protects the integrity of the process and the employees in case of an inaccuracy. The Office Manager and the Office Clerk now share these duties and the Assistant Director performs a review.

Inventory Held for Resale:

Because all items are not sold during the summer, the UMBS Store maintains some inventory over the winter. Inventory is taken at the end of the season, and compared to inventory sheets from the beginning of the season to determine what was sold. Items are listed by description, but some descriptions are not specific enough. UMBS management is consulting with the Associate Director Financial Operations to explore alternatives that will improve the system.

P-Card Reconciliation:

Some P-Card reconciliations were done using credit card slips instead of detailed receipts. Management has informed all staff members with P-Cards that detailed receipts are required for reimbursement. Approvers have been instructed to not approve statements without the appropriate detailed receipts.

Property Signage:

University Audits suggested that the location, frequency, and information on signs posted around the Station should be reviewed for compliance with state regulations and UMBS policy. UMBS is in the process of installing new signage around sensitive research areas. All vehicle entrances to UMBS property are under review to ensure that ownership and appropriate use are clearly noted. Signage on the rest of the property will be reviewed prior to the start of the summer season.

Cash Handling:

Segregation of duties issues were found in the payment processing functions. Payments are generally received by mail in the form of a check. One office staff member was opening the mail, endorsing the checks, and posting the payments. These duties have been split between two office staff members. An additional reconciliation step has been put in place and the UMBS Assistant Director is performing managerial oversight as well.

Manual Financial Processes:

UMBS employs a number of cumbersome manual financial processes. While effective, they are not always efficient. UMBS management is consulting with the Associate Director Financial Operations to implement a more efficient system.

Capital Equipment List:

University Audits found a small number of items on the Capital Equipment List that could not be physically verified. To reconcile this, UMBS is reviewing the list to address any old or questionable items. Those items not at the Station or the Ann Arbor offices will be removed using the appropriate procedures. A complete review will be performed as scheduled in February 2009.

LSA Conflict of Interest Policy:

A number of conflict of interest situations were noted at UMBS. Management instructed staff on LSA's policies and procedures for reporting and documenting conflicts of interest. Those situations noted have now been properly reported, and are managed in accordance with LSA policy.

Chemical Hygiene Plan:

The UMBS Chemical Hygiene Plan (CHP) was incomplete. U-M department of Occupational Safety and Environmental Health (OSEH) was consulted and advised UMBS on procedures for handling the items missing from the plan. UMBS has created all documentation requested by OSEH to complete the CHP.

Management has taken appropriate corrective action on all audit recommendations. **This audit is now closed.**

Adult NeuroRehabilitation Business Processes

Original Report issued August 24, 2007

#2007-820

Follow-up Report issued January 31, 2008

University Audits completed a follow-up review to assess management's progress in addressing these issues. All corrective action is complete. **This audit is closed.**

Patient Arrival

The Adult NeuroRehabilitation Day Treatment Program (Day Program) has fully incorporated the University of Michigan Hospitals and Health Centers (UMHHC) Ambulatory Care Services Clinic Business procedures by scheduling all patients in the Enterprise Wide Scheduling System (EWS). All Day Program patients are greeted and checked-in by patient services staff upon arrival. An additional patient services assistant was hired to help in staffing the clinic's redesigned processes.

Patient Checkout

The clinical care provider is completing a patient encounter form and submitting it to patient services staff for check-out and charge posting upon completion of each patient session. Daily census reports are run to follow-up on any incomplete encounters.

Charge Capture

Management redesigned the patient encounter forms to facilitate complete charge capture. Consultants were brought in to train staff on redesigned processes and to ensure appropriate coding of encounter forms. Open encounter form reports are monitored to ensure complete charge capture.

Medical Record Documentation

Additional laptops were acquired for direct provider input into the electronic medical record, CareWeb. Shadow medical records were scanned into CareWeb and the Day Program no longer maintains shadow files. Provider medical record documentation is scanned into CareWeb on a frequent basis. At discharge, all provider working files are shredded after being verified for completeness in CareWeb.

University Audits – University of Michigan
Open Audits Follow-up Table
January 31, 2008

Audit Title	Report Date	Issues	Expected Completion
U-M Computing Environment Kerberos Passwords 2007-304	6/22/07	Disaster recovery plan	First follow-up was completed <u>January 2008</u> Second follow-up March 2008
UM-Dearborn College of Engineering and Computer Science Departmental System Administration 2007-308	6/29/07	Vulnerabilities based on the periodic scanning of CECS servers	First follow-up was completed <u>November 2007</u> Second follow-up February 2008
Digital Media Commons CTools 2007-301	6/29/07	Persistence of login sessions; log review; SLA between ITCS and Digital Media Commons; upgrade approval process	First follow-up was completed <u>January 2008</u> Second follow-up April 2008
Michigan Administrative Information Services – eResearch	11/26/07	Network placement of production server; required application items	March 2008
Medical Center Information Technology Arbor Lakes Computing Facility 2008-307	12/20/07	Generator Plaza Security; Machine Room Security; Safety	June 2008
Department of Neurology Sleep Disorders Center 2007-206	6/22/07	Security issues; financial controls; charge capture timeliness; and data maintenance and backup procedures	February 2008
UMH Operating Rooms – University Hospitals Supply Chain Management 2007-108	8/17/07	Product recall follow-up; consistent and documented inventory practices; and conflict of interest communications	May 2008
U-M Physical Medicine and Rehabilitation Othotics and Prosthetics Center 2007-107	9/24/07	Charge capture and cash handling controls; quality assurance processes	March 2008
Hospitals and Health Centers Permanent Art 2007-827	9/26/07	Coordination of roles and responsibilities; inventory maintenance and security follow-up	March 2008
Medical School Biomedical Research Core Facilities Financial Internal Controls 2007-826	10/23/07	Recharge rates; capital equipment; separation of duties; procurement; payroll; DNA sequencing services and billing services; policies and procedures	June 2008
University of Michigan Health System Human Resources Fiscal Responsibilities	1/21/08	Payroll management; documentation of processes	July 2008
Michigan Public Media Phase II 2006-806	4/24/06	Documentation and implementation of internal control policies and procedures	First follow-up was completed <u>May 2007</u> Second follow-up February 2008

Audit Title	Report Date	Issues	Expected Completion
Plant Operations Zone Maintenance Purchasing Controls 2007-812	4/24/07	Purchasing. New methods for handling inventory receiving and tracking	First follow-up was completed December 2007 Second follow-up May 2008
Institute for Social Research, Cash Receipts Process 2007-815	5/25/07	Improved cash, check, and credit card receiving procedures; documentation of business office accounting procedures.	February 2008
Matthaei Botanical Gardens & Nichols Arboretum, Business Office Internal Control Review 2007-817	6/19/07	Phase I – cash handling, instructor payment, and credit card refund controls. Phase II - unnecessary sensitive data in files.	March 2008
Intercollegiate Athletics Academic Support Services 2007-408	7/18/07	Student counseling practices; employment and payroll controls; staff training and development	March 2008
Ross School of Business Dean's Office Fiscal Responsibility 2007-821	7/20/07	Purchasing; financial monitoring of their merchandise store; formalizing authority delegation; Statement of Account and Gross Pay Register reconciliations; employee overtime	February 2008
Intercollegiate Athletics NCAA Compliance – Student-Athlete Equipment and Apparel 2007-409	8/24/07	Record retention	June 2008
Army ROTC Business Office Internal Controls 2007-818	9/11/07	Orientation training for new Army Executive Officers to include: University purchasing, hosting, traveling, and reconciliation processes	February 2008
Intercollegiate Athletics NCAA Team Travel 2007-412	10/10/07	Cash and Travel Expense Vouchers Controls	March 2008
University Human Resources Family and Medical Leave Act 2007-403	12/17/07	Training; update relevant SPG sections; written notifications	June 2008
Ross School of Business Multidisciplinary Action Projects	1/10/08	Travel registration; procurement; expendable restricted funds; documented procedures	September 2008
Transportation Services 2007-101	1/28/08	Controls over physical access; system user access levels; commercial driver's license testing; vehicle inventory monitoring; fuel inspection upon delivery; gross pay register review; imprest cash fund; formal policies and procedures	September 2008
I-9 Employment Verification Process 2007-823	1/29/08	Filing timeliness; automation; training	September 2008