THE UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Item for Information

Received by the Regents
September 20, 2007

Subject: Report of University Internal Audits
May 11, 2007 – June 30, 2007

Background:

This is the report of the Office of University Audits activities for the period **May 11, 2007 through June 30, 2007**. 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 **June 30, 2007**.

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

Respectively submitted,

Carol F. Senneff, Executive Director
University Audits

September 2007

ORIGINAL REPORTS

Campus

Institute for Social Research Cash Receipts Process #2007-815

Issued May 25, 2007

The Institute for Social Research (ISR) plans, conducts and disseminates the finding of social science research. Survey results are disseminated a variety of ways. ISR has more than 1,000 employees and has been entrusted with many service level agreements that assist in its ability to provide services for the research enterprise to conduct its business with expediency and with a certain degree of autonomy.

ISR processes receipt transactions involving cash, checks and credit cards. The primary objective of this audit was to determine whether internal controls over cash handling were adequate to safeguard assets and promote adherence to University policies and procedures.

Control issues:

- Cash and Check Processing – To strengthen controls over cash and check processing:
  - Prepare a listing of checks received in the mail. This listing should be prepared by the individual that opens the mail (someone other than the preparer of the cash receipt ticket) and include the check number, payor, date, and amount.
  - Restrictively endorse all checks immediately.
  - Make deposits daily in accordance with Standard Practice Guide section 502.1.
  - Restrict access to checks at all times, as they contain sensitive information, such as bank routing information and home addresses.
  - Issue a numbered receipt for all payments received in person.
  - Reconcile the daily cash receipt ticket to the listing of checks received via mail and the total of the day's numbered receipts to endure that all funds received were deposited.
  - Establish single accountability of the cash drawer by:
    - Locking the drawer at all times.
    - Having a drawer for the main cashier and an additional drawer for back-up cashiers.
  - Inform customers and ISR departments that checks are to made payable to the University of Michigan, rather than ISR.

Management Plan – ISR has updated the cash and check receiving process to incorporate the controls listed above. Specifically, a log of all checks received in the mail is prepared and all checks are endorsed immediately. This log is an excel file. Once an item is input into the worksheet, the items are saved to a second "supervisors only" file. The original file and the supervisors file are reconciled monthly. Numbered receipts are provided for all cash and check payments received in person. Checks and cash are kept secure until they are transferred to the staff person responsible for preparing the cash receipt tickets. Three cash drawers are used to establish single accountability of the cash receipts.

A supervisor reviews and signs off on the cash receipt ticket. Daily receipts greater than $500 are deposited each day. Daily receipts less than $500 are made within one business day. Checks that are received for a project without a signed contract are not deposited, as they may contractually obligate the University. Instead, they will be held in the vault until the unit informs the Business Office that the contract has been signed.

The supervisor checks the deposit for accuracy and seals the deposit in a tamper proof bank bag. The bank bags are deposited every morning at the deposit station in the Michigan Union. The receipt for the deposit is returned to the supervisor as verification the deposit was made. The supervisor spot checks certain days' receipts by verifying that the receipt log and the receipt book agrees to the cash receipt tickets. The supervisor ties out cash receipts on a monthly basis. All check and credit card information (copies, numbers, expiration dates) is placed in a locked file cabinet each day.

ISR Duplication asks for checks to be made payable to "University of Michigan" not "ISR". ISR has changed their invoices and sent a general communication to the units to indicate that all checks should be made payable to the University of Michigan.

- Credit Card Processing – The following improvements would strengthen controls over credit card processing and help assure that ISR maintains compliance with the Service Level Agreement between the Treasurer's Office and ISR:
  - Reconcile refund activity to the bank reports on a regular basis.
  - Secure all hard-copy documentation that includes complete credit card numbers and do not retain credit card information for longer than 18 months.
  - Document credit card refund and sensitive information storage procedures.
  - Consider assigning separate individuals to process credit card sales and refunds.

Management Plan – ISR has updated their credit card processes. A supervisor reviews all credit card transactions on a monthly basis. A report is used to compare the current and previous month's debit activity by customer name. Supporting documentation will be compared when items do not reconcile within the two months and on a spot check basis.

All supporting documentation is kept in a locked filing cabinet and only the last four digits of the credit card are entered into the credit card database.

ISR will develop a system to begin monitoring and then shredding documents that are greater than 18 months old.

- Monitoring – To strengthen monitoring of financial activity:
  - Provide education and training to all individuals within ISR that have responsibility for reconciliation process or all that it entails. This training should include sharing of best practices, as well as defining what is expected of the reviewer, including timing of review, guidance on resolving discrepancies and documentation requirements.
  - Each month, select a sample of Statement of Activities to determine that a complete reconciliation is being performed on a timely basis.
  - Track accounts receivable at a central location. If the department chooses to perform the collection follow-up, they should email the senior account clerk with a summarization of their efforts and progress in collecting the funds. The Business Office should continue to follow-up each month, as necessary.
  - Document the guidelines for escalating communications relating to a past due receivable to a department's supervisor.

Management Plan – ISR has a very decentralized structure with the following five different centers:

- Center for Political Studies
- Inter-university Consortium for Political and Social Research
- Population Studies Center
- Research Center for Group Dynamics
- Survey Research Center

The central Business Office is referred to as the sixth center, Center for Institute Services. Each of these center's needs are very different and they look at Statements of Activity for different items and reconcile them in their own unique and distinct way. The process of making sure the statements are reconciled will be coordinated with the five different center administrators. The Business Office will review different groupings of Statement of Activities each month to make sure the department has reconciled them. The Business Office will review enough Statement of Activities to make sure all projects and grants will be reviewed at least once a year. The Business Office will fully document this procedure.

Accounts receivable items are tracked by the Business Office. We have developed a standard form that all the centers agreed to use (including the Business Office). All follow-up will be done on one consistent form. Items that are followed-up at the center level will be required to turn over their form.

A past due listing of accounts receivable items will be sent to each center administrator for their center on a quarterly basis.

- Documentation of Procedures – The most critical areas to document:
  - Cash, check and credit card receipts
  - Imprest cash handling (survey respondent check and cash payments)
  - Statement of Activity reconciliation
  - Payroll
  - Purchasing

Management Plan – Annually, the Director of ISR has agreed to review all financial statements, security protocols, and new Standard Practice Guide internal controls procedures and assure ISR's compliance in these areas. As such, this document will be reviewed annually by the Director of Business Operations and the Assistant Director of the ISR to assure timely corrections, additions, changes, etc. to ISR's internal control processes.

A follow-up review will be conducted during the first quarter of fiscal year 2008 to confirm that controls have been implemented and are working as intended.

Matthaei Botanical Gardens & Nichols Arboretum Business Office Internal Control Review #2007-817
Issued June 19, 2007

The Matthaei Botanical Gardens is a 300-acre site that includes a variety of outdoor display gardens, a 10,000+ square-foot conservatory, and miles of nature trails. Nichols Arboretum is a 123-acre living museum adjacent to Central Campus, which showcases a collection of Michigan native plants and plants from around the world.

Several months ago, the Matthaei Botanical Gardens & Nichols Arboretum (MBGNA) management performed an informal self assessment of their business office internal controls and noted several opportunities for improvement. Management contacted University Audits and requested assistance in recommending internal control enhancements specific to cash receipts. The review was expanded to look at several other areas of internal controls within the business office. A full scope audit was not performed. Review procedures consisted of interviews with MBGNA personnel to understand processes and a review of documentation used to support those processes. As management was aware, the internal controls over cash receipts did not provide an adequate level of assurance that assets are protected. Opportunities for improvement for cash handling and several other important control points are detailed below.

Cash Handling Controls - MBGNA has various procedures for receipting cash, depending on the nature of the receipt. The implementation of the following recommendations would strengthen controls over all cash receipts:

Gift Shop Receipts:

- An Excel spreadsheet, summarizing the daily deposits is prepared and reviewed weekly. The review process does not include agreeing the spreadsheet information to the Z-tape generated by the cash register. We recommend the review include agreeing deposits to the source documentation (Z-tape).

Contribution Receipts:

- When checks are received in the mail, up to three employees can handle them, prior to recording them in the University's Development Alumni Constituency System. We recommend documenting the relevant information (amount, date, payor, etc.) in a cash receipts log, as soon as the cash is received.

General Cash Receipts:

- When cash or checks are received in person at the MBGNA office, a receipt is not provided to the contributor, unless specifically requested. We recommend processing these contributions through the cash register or providing a pre-numbered receipt to all contributors.
- Cash payments that are not processed via the cash register are photo-copied and the copy is maintained in the files. Taking a photocopy of cash does not support a cash receipt as there is no means to identify that cash was from a specific individual. We recommend that MBGNA not copy cash.
- Checks received by MBGNA are not restrictively endorsed "For Deposit Only – University of Michigan" immediately upon receipt. We recommend that MBGNA restrictively endorse all checks immediately.
- Total cash receipts deposits made for the month should be reconciled to the Statement of Activity (SOA) on a monthly basis to ensure all receipts are deposited and credited to the correct account. This review should be performed and documented by someone who is not involved in the receipting process.
- MBGNA should make deposits daily in accordance with Standard Practice Guide (SPG) section 502.1.

Management Plan - We have already begun reconciling to the Z-tape daily and performing monthly reconciliations. We are also reconciling cash receipts to the SOAs monthly.

Prior to the end of the fiscal year, we will:

- Log all cash and checks received by mail
- Run all cash or checks received in person through the cash register (we rarely receive cash or checks that are not run through the cash register as part of our normal operation)
- Restrictively endorse checks upon receipt (we need to order a stamp)
- Work with the Office of the Treasurer to determine appropriate deposit scheduling.

Secure Sensitive Data - MBGNA obtains sensitive data, such as credit card numbers, checking account numbers, home addresses, and other information printed on personal checks as a result of sales and contribution transactions. Copies of checks are made when received for gifts, membership, or educational courses. Credit card numbers are documented on the registration confirmation receipt for educational courses. The check copies and registration confirmation receipt are filed in the MBGNA Business Office.

We recommend reducing the amount of sensitive data maintained by MBGNA. Checks that are imaged by the Development Office should not be retained by MBGNA. Only the last four digits of the credit card number should be documented on the registration confirmation receipt. If certain sensitive data is deemed necessary to maintain, procedures should be developed to secure and limit access to the data. These procedures should comply with the Office of the Treasurer's policy requiring secure disposal of documentation containing credit card numbers within 18 months.

Management Plan - We have stopped copying cash and the account numbers on checks. We print and copy only the last four digits of credit card account numbers.

Credit Card Refunds - Procedures to issue credit card refunds are not compliant with the Service Level Agreement (SLA) between the Treasurer's Office/Card Services and MBGNA. Refunds are processed by the same individual responsible for sales, without review or approval. MBGNA has several hourly employees that perform cashiering duties. The credit card terminal is easily accessible and procedures currently do not address who can issue refunds. Additionally, there is no reconciliation of credit card refunds per the statement of activity to the monthly reports from Fifth Third Bank.

The following improvements would decrease the risk of fraudulent credit card refunds and support compliance with the SLA:

- Verify that a previous purchase transaction existed with the same cardholder and the same card, prior to issuing a refund.
- Assign separate individuals to process credit card sales and refunds. Supervisory approval of all credit refunds is required (section 3.4 of the Office of the Treasurer's Merchant Card Credit/Debit Policy).
- Compare refunds on the bank statement to source documentation to ensure refunds are appropriate.

Management Plan - All cashiers have been instructed to verify that a previous transaction existed with the same cardholder and card, prior to issuing a refund. We are not able to assign a separate individual to process credit card sales and refunds, because we typically have only one cashier. However, we have implemented a requirement that all refunds be approved by a supervisor when one is in the building, or a person from a different area in the organization when a supervisor is not present (which can happen on weekends).

Credit card returns are rare in our organization, typically zero to five per month. Since we are not able to implement perfect separation of duties, we are more actively monitoring returns as they appear on the monthly credit card bank statements.

Instructor Payments - MBGNA pays various instructors for teaching educational courses. In the past, the education department of MBGNA was not approving the payment of instructors. Therefore, the correct amount of payment and the payee were not being verified by someone with direct knowledge of the service performed.

Standard Practice Guide section 500.01 Fiscal Responsibilities requires that individuals designated with approval responsibility should be in a position to determine that the financial activity is appropriate. We support management's plan to implement the following controls over the payment of instructors via Form G's:

- Instructors initiate payment request in writing, thereby certifying that the services were performed.
- The invoice/written request be approved by an employee in the education department.
- The education database includes the instructor name and salary (in a password protected cell) as documented in the instructors' contract.
- Accounting department agrees the approved invoice to the education database and processes the Form G payment.

Management Plan - Instructors are now giving us invoices, which are initialed by our education coordinator.

Over the last year, management of MBGNA has made great strides in implementing internal controls over cash receipts. A formal follow-up will be conducted during the first quarter of 2008 to ensure internal controls have been strengthened and are working appropriately.

Intercollegiate Athletics Ticket Counts FY2007 Men's Basketball, Ice Hockey and Other Sports Events #2007-413
Issued June 29, 2007

The Big Ten Conference requires its member institutions to prepare a "Basketball Ticket Sales and Financial Settlement Report" (Settlement Report) for each 2006/2007 home Big Ten men's basketball game. The Settlement Report shows:

- The Conference share for visiting Big Ten Teams
- How the amount was calculated

The objective of this audit was to verify the accuracy of 2006/2007 Settlement Reports for home Big Ten men's basketball games, and 2006/2007 ticket sales reports for other Intercollegiate Athletics (ICA) sporting events for which admission is charged, not including football. Verification that the amount of ticket revenue was actually received and deposited into ICA accounts is beyond the scope of this audit. External auditors include revenue in their annual certified audit of ICA.

The audit for football ticket sales was previously issued on February 26, 2007.

Procedures used to verify the accuracy of Settlement Reports included reviewing certified ticket stock manifests received from the printer, counting unsold tickets and verifying all computations. University Audits signed each Settlement Report attesting to its accuracy.

The amount of ticket revenue due the Big Ten Conference was accurately reported on all 2006/2007 Settlement Reports for home Big Ten men's basketball games. Also, the number of tickets for other ICA sporting events for which admission is charged, not including football, is accurately reported on 2006/2007 ticket sales reports. **This audit is closed.**

Healthcare

University of Michigan-Dearborn Institutional Review Board #2007-502
Issued May 31, 2007

The primary mission of the University of Michigan-Dearborn Institutional Review Board (IRB) is to protect the rights and welfare of human research subjects participating in Dearborn faculty, staff and student research projects. Board members evaluate physical, psychological, social, economic or legal risks against University policy. University policy is based on the Ethical Principles first articulated in 1979 in the Belmont Report (National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research). It incorporates the Federal Common Rule (codified for Heath and Human Services (HHS) supported work at 45 CFR 46) and takes into account additional guidance provided by the HHS Office for Human Research Protections and by other federal agencies. UM-Dearborn does not conduct clinical research subject to FDA regulations. The board also provides continuing review of approved research and serves as an information resource to the Dearborn research community on ethical and procedural issues.

IRB membership includes faculty from Natural Sciences, Behavioral Sciences, Education, and Engineering disciplines to ensure a broad knowledge base. A required non-scientist and non-University Community member contributes to a broad perspective. The IRB budget for FY 2006 was approximately $35,000 to compensate for a .6 FTE support staff and for co-chair efforts. Between March 2006 and February 2007, the board considered 42 protocols: 2 full-board, 26 minimal risk expedited reviews (performed by co-chairs), 12 exempt determinations, and two non-regulated.

During the last eighteen months, the Dearborn IRB, as one of nine University IRBs, has been participating in preparation for accreditation through the Association for the Accreditation of Human Research Protection Programs, Inc. (AAHRPP). IRB standard operating procedures (SOPs) were reviewed and updated as of January 2007 and the eResearch electronic research protocol tracking system and information repository has been implemented.

The objective of this audit was to evaluate the design and operational effectiveness of Dearborn IRB internal controls to protect the rights and welfare of human subjects who participate in research conducted by UM-Dearborn faculty, staff and students.

To meet this objective, we interviewed the IRB administrative manager and staff and one of the board co-chairs. We also reviewed the following documentation and processes using criteria established in HHS 45 CFR 46 and the Office of Human Research Protection (OHRP) quality self-assessment tool:

- Standard operating procedures for ensuring the scientific validity of proposed research studies in coordination with an ethics review process.
- Board meeting minutes and agendas for the last three years to determine if the IRB maintains adequate documentation of its activities.
- A judgmentally selected sample of eResearch protocol review records to verify that the IRB systematically evaluates studies to ensure the protection of participants.
- Dearborn Campus faculty training documentation and announcements to promote the monitoring and determination of the need for IRB review for all relevant class room research.
- IRB Board curricula vitas, training, workload, and resources documentation to determine if resources and work load is reasonable.

CONCLUSION

Based on audit scope and testing, we found that Dearborn IRB internal controls were sufficient to meet their objective of protecting the rights and welfare of human subjects involved in research under their purview. Standard operating procedures are current and thorough and protocols processed through eResearch are systematically evaluated. Board meeting minutes and agendas provide adequate documentation of IRB activity and outreach to faculty and students supports the awareness and determination of the need for IRB human research review. Board members represent the spectrum of Dearborn Campus disciplines and workload is commensurate with resources. **This audit is closed.**

Department of Neurology Sleep Disorders Center #2007-206

Issued June 22, 2007

University Audits conducted an audit of the internal control environment within the Sleep Disorders Center. The University of Michigan Sleep Disorders Center diagnoses and treats patients who have problems with their sleep or level of alertness.

PURPOSE AND SCOPE

University Audits examined the following processes to evaluate the adequacy and effectiveness of financial and operational controls governing the Sleep Disorders Center:

- Patient access and discharge
- Charge capture
- Billing
- Cash handling
- Timekeeping

University Audits interviewed personnel within the Sleep Disorders Center and the Department of Neurology to obtain information about the internal control environment. We also performed testing and analysis of charging, billing, payroll and purchasing.

In general, the business processes at the Sleep Disorder Centers and related clinics are efficient and well-managed. Some opportunities for improvement were identified. Recommendations and management action plans are detailed below.

Control Issues:

1. **Security Planning** - Several security concerns regarding access to patient care space via stairwells, elevators and other areas of the hospital were not resolved prior to the move of the Michael S. Aldrich Sleep Disorders Laboratory to Med Inn.

Management Plan - UMHS Facilities Planning & Development has completed its investigation of relevant codes and has proceeded to obtain relevant pricing information. They have begun securing the Michael S. Aldrich Sleep Disorders Laboratory at Med Inn. The following steps have been completed:

- A camera has been mounted in the vestibule of the lab check-in area to monitor the main public/staff elevator from the control room after 9:00 PM.
- Card readers, access control and accompanying hardware have been installed for the connection doors from Mott into Med Inn for floors six and seven.

Management will work with Facilities Planning and Development and Security Services to develop and implement additional measures appropriate for the security and safety of patients and staff at the Sleep Disorders Laboratories.

2. **Fire and Emergency Safety** - During an audit meeting at the Sleep Disorders Laboratory - South State Street (KMS building), an officer entered the facility and indicated that a fire drill was in progress and everyone should be outside. The fire alarm was not heard in that part of the building. At the time, no patients were undergoing studies, and only one or two staff people were onsite at the lab.

The KMS building is not equipped with fire sirens or alarms. Alarms for fires, drills and emergencies are broadcast to the control room in the lab. The notification procedures and lack of audible alarms are not sufficient to notify patients and staff of emergencies when the control room is unmanned.

Management Plan - The University of Michigan Sleep Disorders Laboratory – South State Street facility was evaluated by UMHS Facilities Services and representatives from the Department of Public Safety and the Bureau of Fire Safety for compliance with facility and business code regulations immediately following discovery. Although the facility is equipped with sprinklers and its current business operations are within the code, a decision was made to augment the existing fire safety system with enunciators to provide clear auditory warning of a fire safety incident. This equipment has been purchased by UMHS, installed and tested by the landlord, and is in place at this time.

Sleep Lab Program staff participate in periodic building-wide fire and safety drills, evacuation planning meetings and Yellow Card drills. Existing fire notification, patient/staff safety and facility evacuation plans have been modified to adapt to the laboratory sound alarm system.

3. **Fiscal Responsibilities** - Timesheets are reviewed and approved by each technician's assigned supervisor. Supervisors are responsible for performance evaluations, disciplinary actions and approval of vacation requests and timesheets. However, as technicians work a rotating schedule, a technician may not work with his/her assigned supervisor on a daily basis. Thus, the supervisor approving timesheets may not be the supervisor that was on duty during the technician's shifts. In addition, time recording and approval procedures are not formally documented within the Sleep Disorders Center.

The departmental timekeeper reviews the bi-weekly Gross Pay Register to ensure payroll was processed according to time entered. No further review by management is performed. Regular payroll monitoring by employees independent of the timekeeping function could alert management to payroll issues, irregularities and possible fraud.

Several purchasing card (P-Card) issues were noted:

- Multiple people use the same P-Card for lab purchases.
- P-Card administration procedures within the Department of Neurology appear incomplete.
- Approved statements are available to P-Card holders, which increases the opportunity for alterations to the statement after approval.
- Although monthly P-Card reconciliations are approved by the Chief Department Administrator, P-Card activity is not monitored on a regular basis.

Multiple-person use of P-Cards and cardholder access to approved P-Card statements allow opportunities for unauthorized purchases or inaccurate information to be processed without detection. Lack of appropriate segregation of duties and monitoring of P-Card usage also increases the risk of inappropriate or fraudulent activity.

Management Plan - Payroll verification and monitoring present challenges due to supervisory and staff rotations, shifts and variability associated with the termination of sleep studies. The department's payroll administrator is presently working with Sleep Lab management and supervisors to ensure more effective compliance controls with SPG 518.01, including:

- The frequency of payroll policy and procedure continuing education for supervisors and staff will increase. Written policies and procedures will be posted and provided to staff. Policies and procedures will also be emphasized at new staff orientation, staff meetings and through the Sleep Lab's newsletter.
- A payroll coordinator has been designated within the Sleep Disorders Lab to manage payroll issues as they arise and to audit the gross payroll register at the program level. Periodic audits will be performed and documented.
- Check-in and check-out procedures will be revised for shift start and end.
- Efforts to investigate mechanical timekeeping options and initiatives available through MAIS or UMHS departments will be continued.
- P-Card policies and procedures will be revised to ensure appropriate dissemination and security of cards and to ensure that the reconciliation process is secure. Routine audits will be instituted.

4. **Charge Posting Timeliness** - Analysis of facility and professional billing data for three months ending December 31, 2006 revealed that 55% of facility charges and 37% of professional charges were posted later than the institutional goal of seven days from the service date.

In addition, review of data from the software used to record and analyze sleep studies indicated that physician reports were often completed beyond the internal standard of two days. The data was not adjusted to exclude weekend days. The majority of tests were scored by the technician within two days of the service date however; the majority of physician reports were completed beyond two days of the scoring date.

Management Action Plan - These deficits have been observed, tracked and subject to improvement initiatives prior to this audit. The Sleep Lab has had a chronic faculty time deficit due to faculty transitions and vacancy. The Program Director has recently instituted aggressive measures to reduce and eliminate the backlog currently influencing the less than optimal processing of lab charges. Consequently, current performance is much improved and satisfactory. Replacement faculty and fellow appointments are anticipated soon.

Professional and technical charge mappings and ownership reviews will continue to be conducted by the department's billing office in collaboration with the Sleep Lab to help facilitate additional process improvements.

5. **Maintenance and Backup of Critical Data Stored on Workstations** - The software used to record sleep study data is housed on workstations within the Sleep Disorders Laboratories. These

computers are not supported by Medical Center Information Technology (MCIT) or Medical School Information Systems (MSIS). As a result there is a lack of back-up procedures and other support functions to ensure sufficient protection of medical procedure data. It should be noted that only the detailed graphic outpatient sleep study data resides solely on the stand-alone computers. Inpatient sleep studies (which comprise a small subset of sleep studies) and all summary physician reports are housed on servers that are supported by MCIT.

Management Action Plan - Comprehensive MCIT support of the Sleep Lab's data acquisition system and assets is not feasible, due to functional incompatibilities between the MCIT image and the lab software which serially disrupt the continuity of the data acquisition. Modifications that can be accomplished to reduce risk include:

- A tape backup system to archive and secure data on the local acquisition PCs will be implemented in each lab (South State and Med Inn). A system to backup 600GB of data at the Med Inn lab and 800 GB of data at the South State lab will be needed to do this function. A full backup will be performed weekly and a differential backup performed daily.
- A generic login ID and password is used for the acquisition system because multiple people work on each acquisition system and users do not feel comfortable leaving while they are logged in on a PC with their personal ID. MCIT has permitted a single user ID and password in another lab, provided that the password is changed once a year. The Sleep Lab's engineer will emulate the MCIT model, i.e. have a generic user ID and password, with an annual password.

Information Technology

University of Michigan-Flint Voice-over Internet Protocol (VoIP) #2007-307
Issued June 8, 2007

An audit was conducted of the server configuration and server administration of the University of Michigan-Flint campus Voice-over Internet Protocol (VoIP) implementation. VoIP is the technology used to route voice conversations over the Internet or through any other IP-based network. VoIP uses much of the same infrastructure as a data network. It does this by converting sound into small packets of data and transporting them via the regular Internet protocol (TCP/IP) between telephone sets. VoIP systems can be expected to be more vulnerable than conventional telephone systems, in part because they are tied into the data network, resulting in additional security weaknesses and avenues of attack. Confidentiality and privacy may be at greater risk in VoIP systems unless strong controls are implemented and maintained. Relevant risks include:

- The system is unavailable when needed
- The VoIP system is accessed by unauthorized individuals

A team of Information Technology Services (ITS) staff began working with VoIP technology at UM-Flint during winter 2005. The main purpose of this initiative was to provide campus telephone access in the classrooms, offices, libraries, security, and other inter-campus locations to each other at no cost to the University. VoIP phones are especially useful in buildings (like French Hall) which do not have land lines. These lines are registered by room/location number; however, there is no means to dial outside of the University campus. Since fall 2005, VoIP phones have been installed in general classrooms in the William S. White (WSW) building and the Murchie Science Building (MSB). These phones are located on the wall in the front of the room and are wired into the campus network.

The VoIP application at UM-Flint was originally designed as a pilot application for a much wider implementation of Voice-over IP to be administered by Flint ITS. Because of cost savings and other business reasons, UM-Flint has decided to take advantage of VoIP services offered by the ITCom unit of Information Technology Central Services (ITCS) in Ann Arbor, rather than extend the ITS-administered VoIP infrastructure.

ITCom is offering a VoIP service that replaces the telephone sets, dedicated telephone lines, and smaller telephone switches with VoIP equipment. The telephone handset plugs into the data network "jack" rather than a telephone "jack." ITCom's VoIP infrastructure is propriety technology offering Cisco VoIP phone sets and software.

Because UM-Flint is taking advantage of ITCom's VoIP offering, the VoIP infrastructure administered by ITS will remain a low risk implementation. This is true because the classroom-based service does not allow calls to be made off-campus. Calls can only be made to the safety department, the main office of the University and ITS tech support. This limits the risk of unauthorized use. Additionally, ITS has performed sufficient contingency planning to ensure that the VoIP application can be run on backup hardware and be available with minimal downtime. This addresses the risk of not having the system available when needed.

Based on the audit work conducted in this review, the U-M Flint VoIP implementation is securely configured and properly maintained. The controls provide a high level of assurance that management's goals and objectives are fulfilled. **This audit is closed.**

University of Michigan Computing Environment – Kerberos Passwords and Uniqnames #2007-304
Issued June 22, 2007

Kerberos is a network authentication system designed to enable two parties to exchange private information across an otherwise open network. It is a secure way for users to prove their identity to servers in order to access online resources. It works by assigning a unique key, called a ticket, to each user that logs on to the network. Once a user's identity is verified, Kerberos creates a secure session using encrypted keys. Kerberos is a product of the Massachusetts Institute of Technology, and has been in use at the University of Michigan since approximately 1990.

A *uniqname* is equivalent to a user name. It is the user's identifier to the network. Passwords and access are tied to the uniqname. The uniqname (user name) and Kerberos password combination is used for authentication to many computing services including Wolverine Access, Mail, Directory, Mfile, CTools, UM.SiteMaker, and MAIS LINC. Kerberos is the basis for CoSign web-based authentication used by approximately 200 services.

The purpose of this audit was to determine if the security and controls over Kerberos are thorough enough to ensure the system is protected, operating to its potential, and the users and their data are being properly secured. The controls on this system were evaluated against ITCS policy, University policy, and industry best practices. To do this we needed to look at not only Kerberos, but the systems directly affecting it.

This audit reviewed and tested:

- The processes used to create, remove, and maintain uniqnames
- The processes used to create, remove, maintain, and protect Kerberos passwords
- The processes used to administer servers and networks containing the Kerberos authentication system
- The IT infrastructure processes used to administer Kerberos including backup and retention, password management, upgrades, system access, and documentation

Uniqnames
The processes related to uniqnames can have a direct effect on the overall security of the Kerberos system. A duplicate or improperly assigned uniqname can create problems within the system and user community.

Servers
ITCS uses a homegrown version of Linux, called UMCE Linux, to run Kerberos. It is a stripped down version geared toward security and performance. Only the necessary components of the operating system are left in the kernel (the foundation of the operating system). This removes much potential vulnerability and creates what is called a "hardened kernel". This makes UMCE Linux a good operating system to run Kerberos.

The Kerberos environment is made up of four servers. Three of these are located at the Arbor Lakes facility, and one is housed in the MAIS Machine Room.

In order to make management of the system more efficient, a remote access system has been put in place. ITCS uses Secure SHell (SSH) to access the systems via a gateway server. SSH is a well known and well respected method used for secure remote access. The addition of the gateway server adds another layer of protection increasing the security of these machines.

The servers at Arbor Lakes are networked together using a Virtual Local Area Network (VLAN) which helps isolate them from the rest of the network. While they connect to each other using the same physical network as other machines, the VLAN makes it as if they were on their own network hardware. This adds to the security of the Kerberos Servers.

While the systems are well secured, there are some recommendations to increase internal controls for both the servers and the networks that are detailed below.

Other Areas
Data backup and continuity are always concerns in computing environments. The Kerberos servers are set up so that in the event of a server being lost, the system will use the remaining three and continue to function. If the Key Distribution Center (KDC) server was to go down, creation of new keys would cease, but the remaining systems could continue authentication. The servers are backed-up to both on and off site locations.

System access is limited to those on the Kerberos team. Physical access is dependant upon the location, but limited to those with access to the respective data centers.

Documentation is a critical part of applications such as Kerberos due to the sensitive nature of the Kerberos system. We found the documentation relating to processes for creation and distribution of Uniqnames and passwords to be thorough and complete. ITCS has also put a good deal of effort into creating effective *wikis* (living online data stores) for documenting their projects.

Control Issues:

1. **Kerberos Upgrade Issue** - Until recently, U-M has been using version 4 of Kerberos developed by MIT (K4). UMCE has been in the process of upgrading all of our Kerberos systems to version 5 (K5).

The move from K4 to K5 is significant for a number of reasons. Chief among those is the significant upgrade in security gained by removing the old technology from the campus-wide computing environment. While there will be a small number of systems still running K4, they will be isolated to the Arbor Lakes facility. The Operating System Programming Manager has assured us that applications using K4 are "internal only".

Management Plan - ITCS is currently working on this. We are approximately 98% of the way to complying with the recommendation. K4 is blocked everywhere except for 5 machines at the Arbor Lakes facility. K4 is further restricted to these five machines by the use of client firewalls, and user access is limited to ITCS personnel and computers.

2. **Pre-Authentication Issue** - Even secure systems have vulnerabilities. Kerberos, by itself, is vulnerable to off site dictionary attacks, where a hacker obtains a network packet containing Kerberos authentication information and uses a program to crack the password contained within. The program uses a brute force dictionary technique, repeatedly trying different combinations of words found in a list (i.e. the dictionary) provided by the hacker. It records successes and failures until it unlocks the Kerberos key.

Pre-Authentication is a method used to nullify such attacks. It requires identifying information from a user requesting a Kerberos key before it starts the process of authenticating the user.

Management Plan - ITCS is in the process of implementing Pre-Authentication University wide. At the time of this report, ITCS is in the testing phase of the Pre-Authentication implementation.

3. **Additional Programs on Kerberos Servers** - Along with Kerberos, the Kerberos servers are the central directory for the Andrew File System (AFS). AFS is used across campus for the purpose of file storage and access. The extra traffic through the Kerberos servers caused by AFS poses a potential security risk. If AFS was compromised, the Kerberos system would be vulnerable.

As the central directory for AFS, all traffic for AFS runs through these servers. Whenever a system tries to talk to an AFS resource, it accesses the Kerberos servers first. The Kerberos server analyzes the request, and redirects it to the appropriate end point AFS server, where their data is located. Separating AFS would require a configuration change on all systems running AFS within the UMCE. While AFS integrates well with Kerberos, and is considered quite secure, there are some known vulnerabilities that could compromise the system.

Management Plan - ITCS has agreed to research separating AFS and Kerberos with future system upgrades.

4. **Inadequate Patch Tracking** - Keeping systems patched is a vital part of keeping them secure. To help deal with patches and updates, a tracking system needs to be in place. This normally involves checking for new patches, researching them, applying them to a test server, and implementing them in the live environment.

While it is understood that not all patches should be applied to every system, a procedure needs to be in place to ensure that all patches are reviewed and the appropriate ones are applied. Currently no such procedure is in place.

Management Plan - ITCS is in the process of consolidating many of its operations. This will allow for greater ease of oversight on the people responsible for system patches. ITCS agrees to create a high-level document outlining patch management procedures, and those responsible for them.

5. **Lack of a Comprehensive Recovery Plan** - A Disaster Recovery Plan (DRP) is important in every environment. It is a vital tool for bringing operations back to normal after an unforeseen event. The lack of a DRP can cause confusion and long delays in recovering critical systems, like Kerberos.

Management Plan - The associate vice president for ITCS has been working on their DRP for pandemic flu. It has been submitted and is being reviewed by the MAIS Disaster Recovery / Business Continuity Officer. This completed document will be used as a base for a comprehensive DRP plan. All items necessary for our DRP currently exist across a number of wikis supported by ITCS. The comprehensive DRP will pull all of this information into one place. In addition, system redundancy will be achieved once we have moved into the MACC facility.

6. **Lack of Control Over Program Access to Kerberos** - Keytabs are used by Kerberos to allow programs to communicate across the network using Kerberos authentication. A keytab can be obtained for a program by sending an e-mail to keytabs@umich.edu. The Operating Systems Programming Manager reviews the e-mails, checks to make sure the sender is authorized to request such access, collects the computer name and the program that the keytab is to be assigned to, and creates it.

There is currently no procedure in place to review the activity of the program using the keytab. There is also no system in place to keep track of specific keytabs that have been issued, and whether or not they are still in use.

The purpose for an activity review is two fold. First, a review of active keytabs and their activity could identify any inappropriate use. Second, identifying and removing inactive keytabs reduces the risk of an attacker using the keytab for unauthorized system access.

Management Plan - ITCS is in the process of cleaning up the existing keytabs. Use of the keytabs can be tracked via the DNS servers, and user IP address.

7. **Potential Creation of Duplicate Identities** - The current uniqname system inadvertently gives users the ability to create multiple uniqnames for a single user. This defeats the purpose of having one unique username for each unique user. Identification of unique users is an important control consideration. Multiple uniqnames can also create problems for the user in regard to access and permissions. If a user attempts to log into a system with the wrong uniqname, they will not be able to access the system, even though they (as a person) have permission to do so.

Management Plan - UMCE is addressing this and will be implementing M-Community to take over the management of uniqnames.

OTHER ITEMS OF NOTE

Some potential issues in the areas of passwords and session token lifetimes were resolved through discussions with management. ITCS is constantly working with ITSS to ensure that they are following recommended guidelines. Below are some items that we have discussed with ITCS. They will be reviewing these with ITSS and investigating future changes to enhance security.

Account Lockouts

It is considered an IT best practice to lock accounts after a certain number (usually 3-5) of incorrect password entries. This prevents attackers from using password guessing attempts on accounts. ITSS has stated a concern for people arbitrarily locking accounts to create problems for others.

Password Requirements

Tests on the Kerberos password system indicated the following potential security risks:

- Users can reset their passwords to their current password, thus negating the change
- A password can be changed and then immediately changed back
- Slight changes to dictionary words such as changing the letter O to a zero are allowed
- A number of very weak passwords are allowed

ITCS agreed that these did not conform to typical industry best practices, but that they fell within ITSS recommendations. Given the computing environment at U-M, we can understand the reason for these risks to be in place. However, we think that serious consideration by both ITSS and ITCS should be given to strengthening the password requirements.

Session Token Lifetimes

A session is opened when a user logs into a system. It allows for information to be exchanged between a user and a server. A session token keeps a user logged into a system for a set amount of time. Session tokens for Kerberos currently last for 24 hours, and requests can be made to lengthen that to

four days. An inactive session that has been left open can be subject to an attack called session hijacking. This is where an attacker uses a legitimate user's credentials to access a system. We have suggested that ITCS consider shortening the default token lifetimes to eight hours.

Again, ITCS is in conformity with ITSS recommendations. ITCS has stated that they frequently get requests from users to lengthen the default token lifetime. While they agree that a shorter token lifetime is more secure (as it leads to fewer inactive open sessions), they have stated that user complaints would be great and time lost due to handling complaints would make the change difficult to justify.

UM – Dearborn College of Engineering and Computer Science Departmental System Administration
Issued June 28, 2007 #2007-308

An audit of Information Technology (IT) controls was conducted on the servers at the College of Engineering and Computer Science (CECS) at the University of Michigan-Dearborn (UM-Dearborn) campus. These servers are attached to the UM-Dearborn network but not administered by Information Technology Service (ITS) technicians. ITS is the main provider of IT services to the UM-Dearborn campus. ITS manages the campus network, including:

- High-speed access to the Internet
- IT infrastructure
- Building wiring
- Fiber runs between buildings
- Active electronics located in each building on campus

They support campus routers, work with other departments in Ann Arbor to integrate the University network, and monitor the network to help identify and resolve problems. The College of Engineering and Computer Science (CECS) has the largest number of servers on the UM-Dearborn network that are not administered by ITS. At least 95% of the Engineering students use their UM-provided unique name to obtain an Engineering login. CECS also has its own Domain Name Service (DNS) and can provide uniqnames and create accounts. This is done for the other 5% of the students under special circumstances. CECS maintains Sun, Linux, and Windows servers. Research data is housed on many of these servers. Within CECS, one Linux server is used mainly for content management. Windows servers are used as file systems, license servers, and used to push updates to Windows desktop machines. There are multiple desktop images used at CECS. These are all maintained by CECS IT staff consisting of one manager, four full-time staff, and two part-time staff. Some CECS researchers run servers that are administered by students on a part-time basis. These remain the responsibility of the CECS administrators.

Computer and Information Science (CIS), within CECS, maintains a few of their own servers. Electrical and Computer Engineering (ECE), also within CECS, maintains a proxy server and file sharing server. The servers at CIS and ECE are administered by students on a part-time basis. CECS administrators have oversight responsibility for these servers.

ITS has created and published network and security standards that are consistent with University of Michigan (Ann Arbor) standards and industry-recommended policies, to help ensure the security and integrity of all systems on the Dearborn campus. These minimum IT security standards are to be applied to servers attached to the UM-Dearborn network, including those housed and administered by CECS. All servers should be located in a physically secure environment with controlled area. Associated processes should:

- Clearly define functions and run the minimum number of services required to complete that function
- Apply and maintain security fixes
- Log unauthorized access to server resources and take appropriate action

Backup standards have also been defined for servers at UM-Dearborn. These include:

- Daily backup of critical data
- Backups run off-hours to minimize the impact to users and systems
- One full backup located off-site, in case on-site backup becomes unavailable for any reason
- Test backups for reliability and data integrity
- Log items critical for monitoring security and access
- Log data used for planning upgrades and resolving security and performance issues

An Information Security Incident Response Procedure has also been developed for the Dearborn Campus, consistent with UM-Ann Arbor's IS Incident Management Guideline and Standard Practice Guide section 601.25, Information Security Incident Reporting Policy.

- The designated UM-Dearborn information security coordinator is the manager or senior member of the ITS security team who ensures that the campus is following established information security policies and procedures.
- The coordinator ensures that incidents are promptly reported to the appropriate department or office, and collaborates with Information Technology Security Services (ITSS) on the response and mitigation of serious incidents.

Purpose and Scope:

The purpose of this audit was to ensure the servers at the CECS are administered in a manner that securely maintains data, applications, and the servers themselves. The audit assessed the adequacy of CECS servers security against UM-Dearborn's policy, procedures, and best practices.

The detailed objectives of this audit were to:

- Determine if CECS servers conform to the published Network Standards for the Dearborn Campus
- Determine if the servers are being administered in accordance with system administration "best practices" related to:
  - Data classification
  - Incident response and reporting serious IT security incidents to ITSS per the Incident Reporting Standard Practice Guide section 601.25
  - Training of system administrators
  - Remote access to servers for administration
  - Logical security to servers, applications, and data files
  - Deploying patches

As part of this audit, ITS conducted a current scan of the CECS servers using eEye's Retina product to help identify server vulnerabilities.

Physical security of the CECS computer facilities and its business contingency planning were not included in the scope of this audit.

Summary - As a result of the findings noted in the scans, IT management at CECS has agreed to research all the vulnerabilities and take corrective actions. Another scan of the CECS servers should be run in a month to determine that the existing high risk vulnerabilities have been addressed. Subsequently, scans should be performed periodically and new significant vulnerabilities should be addressed on a timely basis. During the closing meeting, CECS IT management noted that many of the scan vulnerabilities had been addressed.

Digital Media Common – CTools #2007-301

Issued June 29, 2007

CTools is the University's web-based system for coursework and collaboration. It allows students, faculty, and staff to access and share course and project materials. It facilitates interaction between

group members by serving as a conduit for chat, email, and discussion. CTools even allows online testing, homework submission, and grading.

Control Issues:

1. **Administrator privileges** - Management authorizes Administrator accounts, but any Administrator can create or promote other accounts to Administrator status. Under these circumstances, Administrator privileges could be granted without management authorization, leading to unapproved or unsupervised system changes. Extra Administrator accounts could also be used to obscure inappropriate privileged activity.

Risk is mitigated by the small, trusted nature of the CTools Administrators group. Compensating control is provided by management's periodic review of accounts with Administrator privilege.

CTools Support noted that the underlying Sakai product would need to offer more granular Administrator privileges to allow the provisioning of new Administrator accounts to be restricted to management.

Management Plan - The nature of Administrator accounts is one of unlimited privilege, which support personnel, some of whom may be temporary, need in order to do their jobs. Members of all three CTools teams currently require Administrator accounts: CTools Development, CTools Support, and ITCS CTools Operations. The risks noted in the finding are real but necessary in the course of CTools administration. As noted in the finding, the list of Administrator accounts is reviewed periodically (approximately every 4-6 weeks), and those that shouldn't be there are removed.

CTools Support will develop more specific procedures and guidelines for conducting this review of Administrator accounts. Options for automating parts of the review process and improving documentation of the results are also being considered.

CTools Development will also make changes to CTools addressing these risks. Several alternatives are being considered that will increase managerial oversight of the creation of Administrator accounts. The boundaries of Administrator privileges between CTools instances (Test, Pilot, Production, etc.) are also being reviewed.

2. **Persistence of login sessions** - Statements by CTools developers and auditor testing confirmed that logging out of CoSign authentication ("Weblogin") does not log the user out of CTools, as it does for many other CoSign-enabled services. Users who do not explicitly log out of CTools may be putting their data at risk. Individuals subsequently using the same computer could impersonate the user and access the user's private CTools data.

A safe logout procedure allowing users to mitigate this risk is described in the "Known Issues" section of CTools Help. These instructions are not prominently displayed, which may limit their value.

Management Plan - Notifications will be added or emphasized informing users, especially those at public site workstations, that they remain logged in to CTools until they restart the browser. CTools Development will create a specification and reprogram the CoSign implementation for CTools to end the session and fully log the user out.

3. **Log review** - CTools maintains extensive logs of user and system activity, including security events. However, these logs are not used to proactively identify unusual or abnormal activity in CTools. CTools Support only uses event logs and web logs to investigate and diagnose specific reported issues e.g., when a student's submission is not received by the instructor.

The most effective approach to security is to identify signs of security violations as early as possible. One means of accomplishing this is to analyze logs for unusual, abnormal, or suspicious patterns of activity.

The types of activity sought could include:

- Trading inappropriate content (file transfer activity, especially via WebDAV; suspicious file types; disk space usage)
- Attempts to compromise passwords (failed logins)*
- Attempts to compromise via URL manipulation – manual or automated fuzzing, or SQL injection*

Analysis of CTools event logs and web logs may be valuable to the extent they provide evidence of such activities.

*Analysis of these activities may require correlation with logs from other sources, such as CoSign or load balancers.

Management Plan - Some monitoring and review of CTools activity is provided by other units: the ITCom Network Operations Center (NOC) and the ITCS IT User Advocate. The NOC currently serves as the first-level alert agency for detecting suspicious activity across all campus networks, and has the capability to isolate the source(s) within the campus network, including CTools applications and course/project sites. Management is reviewing the NOC alert thresholds and will develop specifications and policy if more CTools-specific alert thresholds would be beneficial.

The User Advocate also serves to identify security, network, and IT resources abuse. Network logs, including CTools logs, are retained and reviewed to aid the User Advocate's investigations. Management is also reviewing the ability of its web log analysis tool to parse the substantial data retained in CTools log files in a way that identifies standard and exceptional CTools usage.

4. **Authorization of outsider access** - CTools, possibly more than any other IT service at the University, delegates significant authorization powers to end users. Site owners/organizers can share their content publicly, or share it privately with selected individuals both inside and outside U-M. This empowerment encourages adoption of CTools and collaboration with other institutions and the community, but raises potential control issues.

CTools' ability to reach beyond the confines of U-M is based largely on a system of self-serve guest IDs known as Friend Accounts. Friend Accounts can be used with a number of U-M IT services, but in CTools their potential is fully realized.

Guests can register their e-mail address and choose a password to set up their Friend Account in less than a minute. Once established, Friend Accounts are immediately available for CTools site owners to include in their sites. Friend Accounts acquire CTools access only by being added to a site.

In contrast, some Friend-enabled services require the service owner (typically an IT department) to grant Friend Accounts access to the service before making them available to users. For example, in IFS Online File Storage, directory owners cannot grant a Friend Account access to their material until an ITCS administrator authorizes the Friend Account for basic IFS access.

CTools' implementation of Friend Accounts erases this boundary. By delegating access decisions fully to content owners, management has abdicated any centralized control over external access to CTools resources, relying instead on end users' judgment of their invited guests.

It is important to note that when granted access to a CTools site by the site owner, Friend Account guests can only utilize the resources of the permitted site. Furthermore, Friend Account guests do not

acquire the ability to create sites of their own. All owners of CTools sites are therefore U-M students, faculty, or staff.

These site owners, not CTools administrators, control access to private, confidential, or sensitive data stored within sites. They are primarily responsible for its care under Standard Practice Guide (SPG) section 601.12 *Institutional Data Resource Management Policy*. Owners of CTools sites have a responsibility to oversee the activities of all site participants, not just guests, ensuring they abide by SPG section 601.7-0 and other policies on the proper use of information technology.

The risk is that users who choose to violate policy, perhaps trafficking in inappropriate content, face fewer measures preventing them from doing so. File-trading rings can be established with ease, increasing dependence on traffic and log analysis, including content monitoring, to detect such activities.

Management Plan - The U-M Friend Account was created specifically to enable useful inter-institutional collaboration by providing guest access to resources stored on campus network resources, including CTools among many others. The granting of privileges to these guests has intentionally been widely distributed and unmonitored. Any CTools policy limiting the creation and use of Friend Accounts should be developed with these broader benefits in mind, particularly in research collaboration beyond U-M participants.

The CTools team is considering several alternatives for managing risk in this area. Initial ideas include:

- Tools to help site owners monitor their sites for indications of abuse
- Automated reports showing abnormal Friend Account behavior based on a number of factors

These and other ideas will be studied further to arrive at a feasible solution.

5. **SLA between ITCS and Digital Media Commons** - Management indicated the service level agreement (SLA) between ITCS and Digital Media Commons (DMC) is outdated and was never actually signed.

ITCS hosts and administers the CTools servers, tests performance, and facilitates change management, while the DMC supports users and develops the CTools software and middleware. These groups demonstrate a clear understanding of their relationship, and communicate well. The SLA is crucial in documenting this relationship, and forming a basis for internal controls.

The SLA on file was not reviewed for content. SLAs typically document management's expectations of services to be delivered, performance tracking and reporting measures, problem management and dispute resolution procedures, customer (here, DMC) duties and responsibilities, and security arrangements. The risk of inadequate controls in each of these areas is increased without sufficient documentation such as an approved, current SLA.

Management Plan - ITCS will review and update the current SLA to reflect the experience gained in the past twelve months of operating the CTools production infrastructure and collaborating with the CTools Implementation Team (DMC). A new agreement will be drawn up, and a timetable and conditions for regular review established.

6. **Upgrade approval process** - An approval process is in place for authorizing upgrades to new releases of CTools, but it is not consistently followed.

The CTools Advisory Committee (CTAC) meets periodically as needed. One of its duties is to discuss and approve major new releases of CTools for deployment. "Major" releases are defined as a .1 or greater change in version number, e.g., 2.1 to 2.2. Major releases include new or revised features and functionality, which requires more testing and communication to users than mere bug fixes.

Management noted that since CTools has stabilized, these approvals are not always obtained. Thus, a fair proportion of changes takes place without formal approval, unless the development team encounters an issue they feel must be elevated to CTAC.

CTAC approval is an important step in ensuring that stakeholders in CTools have an opportunity to review and comment on significant system changes. Approval by the committee also ensures shared accountability for any adverse effects arising from changes.

Management Plan - Standard practices are being developed for:

- Scheduling, conducting, and documenting CTAC action/authorization
- Communicating (to CTAC) and documenting upgrade status, design issues, and production readiness

A higher level governance function, which may continue to employ CTAC- and CFAC-like functions, is necessary to translate the priorities of U-M academic leadership, and to gate the resources and campus appetite for current and future CTools services. To date, CTAC has served in a technical advisory role only, e.g., confirming that performance testing has revealed adequately robust behavior to include a specific tool in the next production release. The CTools Faculty Advisory Committee (CFAC) has filled a similar advisory/focus group role in assessing faculty interest in new tools to be implemented within the CTools framework. Implementation goals also derive from U-M executive officer priorities, e.g., the desire to conduct course evaluations or pre-order textbooks through CTools.

The Digital Media Commons and the Provost's Office have begun discussing the need for a more comprehensive governance model for the CTools infrastructure from both the implementation and production services perspectives. Once a new governance model is developed, the roles of other advisory functions, including CTAC, CFAC, IT Security Services, and the User Advocate, shall be redefined and include appropriate decision-making and documentation procedures.

7. **Integrity of sensitive data exchanges** - CTools provides an optional Grade Book tool allowing instructors to:

- Record assignment and test scores
- Calculate course grades
- Adjust, scale, and share grades with students

Grade Book grades can be exported and uploaded to the University's official Web Grades system through a manual process.

Based on interviews, observation, and testing, the transfer of Grade Book data and student submissions to and from CTools is adequately protected from disclosure and tampering. Strong encryption is used to effectively provide a trusted path. As the number of assignments processed through CTools continues to grow, management may wish to consider additional controls supporting proof of submission, proof of receipt, and the authenticity of submissions and grades. Controls offering proof of submission and proof of receipt could be helpful for students submitting work in CTools. Scenarios were noted several times in which students claimed to have submitted work that the instructor claimed never to have received. Providing more tangible evidence of submissions could more clearly differentiate user errors from system errors. For example, students could be sent confirmation e-mails for work submitted, or tracking numbers could be issued to uniquely identify each submission upon receipt. Notifying students of successfully submitted assignments was one of the top requests from faculty and students surveyed on their use of CTools by the Digital Media Commons Usability, Support, and Evaluation Lab in 2006.

Controls proving the authenticity of student submissions and grades could also be a worthwhile addition to CTools. Authenticity and non-repudiation are often provided by a Public Key Infrastructure (PKI), a substantial investment that is best addressed at an institutional level. The ability

to sign documents would enhance the value and integrity of CTools, and provide the institution another reason to invest in PKI.

Management Plan - CTools version 2.4, being released to production this summer, implements the main control recommendation; automatic confirmation emails to students providing more tangible evidence of submissions. Instructors can optionally receive notification whenever a submission is made to an assignment.

Automation of grade uploads from the Gradebook tool to M-Pathways is slated for a future CTools release based on Sakai 2.5. The planned mechanism will reflect the controls over roles and privilege delegation enforced in M-Pathways, and will reduce the need for authenticity checks of the type envisioned in the above finding. Additional options for increasing control over submissions and grades are also being considered.

8. **Size limitations on files and sites** - CTools imposes limits on the size of sites and of files uploaded to the "Resources" tool: Sites are limited to 1 GB (increasable upon request), and uploads cannot exceed 20 MB. These limitations were tested and are functioning as designed.

Although the intent behind it was to preserve system performance, limiting file and site sizes curbs sharing of movies, music collections, and other undesirable material. The 20 MB file size limit, however, can be bypassed by uploading via WebDAV, significantly weakening its control value.

Teaching and research increasingly require the use of large file formats such as image-rich PDF documents, audio/video content, and massive data sets. Users need access to upload and retrieve such large files. These legitimate uses require a fresh examination of control policies designed to prevent abuse of intellectual property primarily by screening for excessive file size of shared material.

Management Plan - The CTools team will examine existing tools, such as security scans and log analysis, to devise other ways of identifying potential file sharing abuse. Published policy on file size/upload limits or requests for file size limit changes will be reviewed to address the disparity between CTools Resource Upload limits and WebDAV capability. Moreover, the Implementation and Production teams will consider ways to streamline and standardize the transfer and management of files of all sizes.

New governance agents being sought for the CTools infrastructure will be asked to evaluate policy options that support realistic file sizes while aligning with responsible institutional monitoring for content abuse.

Summary:

Based on the audit work conducted, controls in and around CTools provide reasonable assurance of its security, its availability and its ability to maintain the confidentiality and integrity of data. All significant issues identified during the audit have been presented here along with recommendations for correcting them.

A number of important controls and management initiatives affecting CTools' treatment of sensitive or critical data were noted during the audit. Most of these are works-in-progress and were not reviewed. In our opinion, however, they are valuable measures that will either directly improve security or inform future security decision-making.

- To ensure continuity of service, redundant CTools servers are being deployed between the Arbor Lakes Data Center (ALDC) and the Michigan Academic Computing Center (MACC)
- Sensitive projects' resources reside on a separate storage server with separate backups for increased security

- Contingency planning has been undertaken to ensure that CTools, as a critical piece of communication infrastructure, remains available during emergency campus closures to support remote work and interaction
- A U-M Privacy Committee is examining and classifying the data stored in CTools and other institutional systems; CTools management will enact appropriate controls to protect any private, sensitive, or confidential data identified

Germane examples of sensitive data, such as personal health information protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), should be considered as these initiatives proceed.

The CTools Advisory Committee and U-M Privacy Committee are weighing other CTools privacy matters as well:

- The scope of access granted to guests (non-students) whom instructors invite to their course sites
- Whether to allow instructors to monitor their students' activity (or absence of activity) on the instructor's course site(s)

Privacy and security should continue to be given due consideration, to both protect the community and further its trust in CTools, encouraging further integration and success of CTools.

FOLLOW-UP REPORTS

Veterans Administration Billing #2006-128

Original Report issued November 30, 2006 Follow-up Report issued May 17, 2007

1. Inefficient Billing Processes - The Graduate Medical Education (GME) Administrator, the Veterans Administration (VA) Director of Education, and the VA Billing Coordinator have met several times to discuss improvement to billing procedures. Draft procedures for a revised process and a procedures flow chart have been developed and reviewed at the last meeting on March 20, 2007. Final sign-off by the VA Director of Education and the GME Administrator is expected at their next quarterly meeting in July 2007.

2. Use of Social Security Numbers - Social Security numbers are manually removed from electronically generated billing reports of resident services to the Veterans Administration Medical Center (VAMC). A request has been submitted to the software vendor to systematically omit them from the report.

3. Defined Roles and Responsibilities for VAMC Billing - Draft procedures referenced in #1 above include assignment and definition of roles and responsibilities for VAMC billing. Training is being provided to program coordinators; and the procedures will be posted on the GME web site when completed.

4. VAMC Billing, Monitoring and Tracking - GME has resumed advance billing for resident hours provided to the VAMC on a quarterly, estimated basis. Adjustments to actual hours are made in subsequent billings. Accounts receivable records are being used to monitor and track billing and payments.

All open items have been addressed appropriately. **This audit is closed.**

Intercollegiate Athletics – Sports Camps #2006-410
Original Report issued July 28, 2006 Follow-up Report issued May 30, 2007

The follow-up process will be performed in two phases:

- An initial follow-up to ensure that action plans are 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 are included in the following summaries:

1. Background Checks: Athletics management has documented a formal background check policy, which includes a procedure to reconcile background checks submitted to camp staff rosters. Additionally, an Athletics Department intern will perform all of the background checks for the summer camp employees. Management is working with the Department of Public Safety and Office of Risk Management to determine the extent of background checks that will be conducted outside of the State of Michigan. In September 2007, University Audits (UA) will review documentation which supports that background checks and reconciliations are being completed in accordance with policy.

2. Contracts: Athletics management created a camps and clinics policy which states that all camps must be supported by written agreements between the Department of Athletics and the camp director. The policy also requires that all concession sales during camp sessions be processed in the same manner as the campers' fees. External camp contracts for the summer 2007 session will be approved by the Regents. Management is in the process of determining whether an agreement is necessary for smaller camp sessions held during the school year. In September, UA will review the summer 2007 contracts for clear documentation and Regent approval, as well as the agreement process for the camp sessions held during the school year.

3. Financial Records: The external camp financial disclosure form was expanded to include more meaningful and complete financial data and comprehensive instructions for completing the form are now included. The 2006 external camps were required to complete the updated form. These forms were reviewed for reasonableness by Athletics; Athletics will continue to review the external camp financial disclosure forms and perform follow-up as necessary. **This issue is closed.**

4. Reconciliation of Deposits and Payments: Athletics management reconciled the deposits and staff payments to camper and staff rosters for three of the 2006 summer camps. Reconciliations will be performed for a sample of camps each year on a rotating basis. Management is in the process of documenting the procedures to complete reconciliations, including guidance on variance resolution. In September 2007, UA will verify that the reconciliation procedures have been clearly documented with all variances explained.

5. Time Away Policy: Athletics' timekeeping policy was updated to provide specific guidance for recording exception time while working at camps. The policy was reviewed by Human Resources. In September 2007, UA will review time reports for a sample of camp employees to verify compliance with the updated policy.

6. Cash Management: Athletics' cash receipts policy was updated to include that cash and equivalents must be deposited daily and adequately secured. The new camps and clinics policy also states the daily deposit requirement. Athletics Business Office completed the conversion to the new depository procedures with LaSalle Bank and has a courier service pick up deposits daily. **This issue is closed.**

University Audits will look at these same processes after the summer camp season.

U-M Autism & Communication Disorders Center #2006-814
Original Report issued November 21, 2006 Follow-up Report issued June 19, 2007

1. Segregation of Duties
   - Management implemented new procedures for processing payroll and reconciling the Gross Pay Register. The new procedures appear to establish an adequate segregation of duties over the payroll function.
   - Management also established new charge capture procedures. U-M Autism & Communication Disorders Center (UMACC) now uses encounter forms to track patient visits. Encounter forms are printed for all billable visits, including series visits.
   - Management is currently considering the cost and benefits of implementing more robust security controls in Lytec (UMACC's patient billing system). They expect to reach a decision by Fall 2007.
   - Management revised UMACC procedures for reconciling the daily cash receipts log to deposit slips and the statement of activity. Under the current procedures, the individual responsible for making deposits is performing the daily deposit reconciliation. Ideally, this function should be performed by an individual independent of cash handling responsibilities. We recommend that UMACC management either segregate these functions or periodically review the reconciliations to ensure appropriate oversight.

2. Cost Transfer Documentation
   UMACC is now providing detailed explanations for cost transfers initiated on non-federal and federal-sponsored accounts. UMACC provides these explanations on the journal entry documentation.

3. Authorized Refunds and Write-offs
   Management revised and documented procedures for authorizing and issuing refunds and approving and writing off bad debt. The revised process establishes an adequate segregation of duties for approving and monitoring refund and write-off activity.

4. Accounting Errors
   Management established new procedures for performing Statement of Activity (SOA) and P-Card reconciliations. The new SOA reconciliation procedures should assist in identifying charges that may be applied to the wrong account. New P-Card reconciliation procedures will assist in identifying inappropriate charges, including items that should be re-billed to third-party sponsors.

5. Documented Processes
   Management revised and documented many of its internal procedures and communicated those procedures to the appropriate staff members. Management will continue to document other procedures as needed and have ongoing reviews of procedures during regularly scheduled staff meetings.

   All open items have been appropriately addressed. **This audit is closed.**

UMHHC Vendor Discounts, Allowances, and Rebates #2006-119
Original Report issued July 2006 Follow-up Report issued June 28, 2007

An initial follow-up was performed in February 2007.

A second follow-up review has been completed to determine whether vendor rebate checks are deposited daily. The UMHHC Contracts and Procurement Office is now promptly depositing checks on the day of receipt. Appropriate corrective action has been taken. **This audit is closed.**

Intercollegiate Athletics NCAA Compliance – Recruiting #2007-405

Original Report issued November 16, 2006 Follow-up Report issued June 28, 2007

Recruiting guidelines and documentation requirements were discussed at the October and November 2006 coaches' rules education meetings. All coaches are now required to submit rosters for tournaments they attend for contact/evaluation purposes. The Athletics Compliance Services Office (CSO) performed their first annual review of telephone bills and contacts and evaluations for a sample of prospective student-athletes during May/June 2007 and no areas of non-compliance were noted. The following sports were included in the review: football, men's basketball, women's basketball, men's soccer, men's tennis, women's crew and women's volleyball. The CSO is adequately monitoring recruiting telephone calls and contacts and evaluations. **This audit is closed.**

University Audits – University of Michigan
***Open Audits* Follow-up Table**
June 30, 2007

Audit Title	Report Date	Status	Expected Completion
University of Michigan Computing Environment CoSign Web Authentication 2006-303	11/28/06	Issues being addressed include relocation of a server and formalization of departmental procedures.	September 2007
MCIT Taubman Machine Room 2007-306	2/28/07	MCIT is addressing environmental problems in the Taubman machine room; also moving 40% of servers to new Arbor Lakes computer room.	September 2007
UMMS Surgery Research Labs IT Security 2006-403	2/28/07	Department of Surgery is addressing issues related to IT administration and security.	July 2007
U-M Computing Environment Kerberos Passwords 2007-304	6/22/07	Issues being addressed include completion of the upgrade of Kerberos, implementation of pre-authentication, patch tracking, controlling Keytabs, and addressing the potential for duplicate identities.	December 2007
UM-Dearborn College of Engineering and Computer Science Departmental System Administration 2007-308	6/28/07	Vulnerabilities based on the periodic scanning of CECS servers need to be addressed.	September 2007
Digital Media Commons CTools 2007-301	6/29/07	Issues included controlling Administrator privileges, restricting persistence of login sessions, log review, controlling 'friend' accounts, updating and signing the C-Tools SLA, and formalizing the upgrade process.	December 2007
Urban Health and Wellness Center – Flint 2007-207	3/8/07	MOU with UMHS was renewed. Improvements in clinic operations are underway.	August 2007
UMH Quality Improvement - Office of Patient Relations 2007-816	3/14/07	Management is addressing controls over financial activity, access to database and use of SSN's.	September 2007
Department of Neurology Sleep Disorders Center 2007-206	6/22/07	Management is addressing security issues, financial controls, charge capture timeliness and data maintenance and backup procedures.	December 2007
Michigan Public Media Phase II 2006-806	4/24/06	Documentation and implementation of internal control policies and procedures are in progress.	First follow-up completed May 2007 Second follow-up November 2007

Library Special Collections 2006-205	6/16/06	Library administration is still addressing space needs for unprocessed materials.	First follow-up completed April 2007 Second follow-up August 2007
Intercollegiate Athletics Sports Camps 2006-410	7/28/06	Second follow-up scheduled to ensure operational improvements were successful for the summer camp season.	First follow-up completed May 2007 Second follow-up October 2007
College of Engineering – Minority Engineering Program Office 2006-813	9/29/06	CoE and MEPO created a thorough management plan to address the audit issues; the follow-up review is currently being conducted.	July 2007
Procurement Services Procurement Card Program 2007-115	2/5/07	Phase I - Procurement Services will utilize data mining tools and reduce transaction based monitoring; additional focus on training and accountability of P-Card approvers, provide guidelines for card issuance, and utilize electronic resources. Phase II – annual monitoring of card activity by dept.	Phase I – July 2007 Phase II – March 2008
Recreational Sports Business Office Internal Controls Review 2007-813	2/20/07	IM Building procedures were reviewed but action plans will be implemented in all Recreation Services locations.	August 2007
Plant Operations Zone Maintenance Purchasing Controls 2007-812	4/24/07	Management is in the process of strengthening internal controls over purchasing. New methods for handling inventory receiving and tracking are being studied.	September 2007
Office of Technology Transfer Key Processes 2007-105	4/30/07	Accounts receivable best practices will be addressed; the royalty report review process will be formalized.	September 2007
Institute for Social Research, Cash Receipts Process 2007-815	5/25/07	ISR is implementing improved cash, check and credit card receiving procedures; documenting the business office accounting procedures.	September 2007
Matthaei Botanical Gardens & Nichols Arboretum, Business Office Internal Control Review 2007-817	6/19/07	Phase I – Management is implementing additional cash handling, instructor payment, and credit card refund controls. Phase II – Management will eliminate unnecessary sensitive data from all files.	Phase I September 2007 Phase II January 2008