UNIVERSITY OF MICHIGAN

REGENTS COMMUNICATION

Received by the Regents
March 15, 2012

Item for Information

Subject: Report of University Internal Audits
December 2011- January 2012

Background:

This is the report of the Office of University Audits activities for the period **December 2011-January 2012**. 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, 2012**.

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

University Audits
December 2011- January 2012
Summary of Reports Issued

ORIGINAL REPORTS

Campus

Plant Operations Information Management and Reporting #2011-102
Report issued December 22, 2011

Plant Operations (Plant), a division of Facilities and Operations, is responsible for maintaining all aspects of the University's facilities along with any related services such as grounds keeping, cleaning, and recycling. Plant employs over 1,300 full-time employees to manage operations, which vary significantly by department:

- **Construction Services** – Renovation, painting, signs and graphics, upholstery, cabinetry, spray and finishing
- **Facilities Maintenance** – Building maintenance, building automation, electrical repair, specialized hospital maintenance, mechanical systems, roof repair, metal shop, elevator repair
- **Plant Building and Grounds Services** – Building services (custodial), grounds keeping, heavy equipment garage, recycling, landscape architecture, pest and waste management
- **Plant Material and Moving Services** – Plant receiving, moving and trucking, and distribution of maintenance, repair, and operations materials to maintenance, construction, and utilities work groups
- **Utilities and Plant Engineering** – Business services (billing), central power plant, electrical operations and engineering, energy management, and mechanical engineering
- **Work Management** – Call center, preventative maintenance planning, and coordination of project related estimates, utility and service shutdowns, and quality assurance
- **Plant Academy** – Numerous courses in supervision/leadership, facilities work, ethics, effectiveness, and empowerment
- **Plant Administration** – Finance, Information Technology (IT), Payroll, and Accounts Payable

The objective of the audit was to assess the effectiveness of Plant's oversight and management of division-wide and department-specific information management. Reporting was included in the audit to support Plant management's planned review of reports within the division for effectiveness and efficiency of use.

The review primarily focused on:

- Formal policy and procedure around management reporting and analysis
- Monitoring and oversight of data and reporting at both the divisional and departmental level
- Effective information sharing and access to data throughout the division and University
- Sufficient data-related communication and education across the division to promote solid business practices

For a broader view of reporting and information management practices across the division, an online survey was developed to collect information on department procedures, systems, and report use. The survey was distributed in collaboration with Plant and Facilities and Operations management to 165 Plant employees.

University Audits selected a sample of management reports and databases for testing from two Plant departments - Utilities and Plant Engineering (UPE) and Building and Grounds Services (BGS) to better understand existing controls around the development and maintenance of data and reporting throughout Plant. A sample of reports from divisionally supported systems was also reviewed.

Plant's information and management reporting environment is complex and decentralized. Approximately 80 data management tools and systems are currently used within Plant. Many of Plant's systems were purchased or developed to accommodate operational reporting and information management needs not initially met by PeopleSoft, the University's enterprise reporting system. Plant IT supports the sixteen core systems including the Facilities Management System (FMS) is the division's primary information management system and supports many facets of Plant's daily operations, maintenance, and workflow. The remaining systems, consisting primarily of Excel spreadsheets and simple relational databases, reside in the departments where they are maintained by department staff.

Over 300 management reports are available through FMS and Plant's other centrally managed systems. Not included in this count are reports generated by local systems maintained within Plant's departments. Some of these local systems house data not currently available through PeopleSoft or any of Plant's divisionally supported systems. The number of reports generated from this locally stored data is unknown.

Observations and recommendations specific to information management and reporting processes are primarily based on our assessment of the sampled reports and information systems and analysis of survey results. Additional efficiencies could be achieved by applying these recommendations to reports and data repositories throughout the division.

Risk and Control Discussion

- Data Management – Management is currently compiling a comprehensive inventory of available management reports and information systems within Plant. Based on audit interviews and testing, some of the reporting and analysis produced within departments is derived from locally maintained data. Survey results produced some information on departmental data reporting but did not provide a comprehensive list of all available reports and systems.

  Plant is planning to migrate relevant locally held data into the FMS system. Understanding what data resides within the departments and how it supports departmental operations is critical to effective management and oversight of operations. Once a comprehensive inventory of Plant's information resources is developed, management can use this information to identify, evaluate, and prioritize data for centralization.

  The unique nature of some reports and data may necessitate the supplemental systems housed within Plant departments. Oversight and monitoring are essential for data and reports that cannot be integrated into centrally supported systems. Policies and procedures around data management and reporting should be formally documented. Some departments have formalized policies and procedures governing the maintenance of their data systems, and regularly provide reports to Plant and University leadership. UPE is an example of a department with well-defined procedures. The department regularly provides consumption information to Plant management and the Provost's Office of Budget and Planning for analysis. Utilities-related work requests and energy consumption data is automatically uploaded into PeopleSoft to facilitate service unit billing and support business reporting across the University.

  Based on observations of the reviewed sample systems at BGS, some other departments may not have robust controls. While the systems reviewed in GBS housed data that did not directly

impact central Plant operations, department level controls could be improved. In some cases, output from local systems is not validated against Plant IT's reporting standards and data is not shared widely. However, the department is working with Plant IT to incorporate priority data into FMS to improve controls and information sharing.

Management is in the process of centralizing locally maintained data in the following departments:

- Building and Grounds Services
- Construction Services
- Facilities Maintenance

Plant is encouraged to maintain momentum in this effort. Consider:

- Incorporating departmentally maintained data and systems in a division-wide inventory
- Evaluating and identifying data for integration into FMS and PeopleSoft

Management Plan – Plant IT has made significant improvements within the past year, not only in the realm of data and information management but also within its core operations. There has been a considerable effort to restructure the IT department to maximize value, while enhancing services and support for the customer and user base. In addition, Plant IT has become a better business partner, leveraging information technology opportunities, suggesting tools and methodologies to help support Plant's changing business environment.

Plant IT will continue to work with local departments to identify information systems (essentially Excel spreadsheets and Access databases) that have the potential to be housed in centrally maintained systems. For those systems identified, a gap analysis will be conducted along with the needed planning to aid in data consolidation. For those systems where it is not operationally feasible or efficient to centrally maintain, an information systems inventory will be created along with policies and procedures to help support local development and ensure data integrity.

- Reporting and Analysis – Statistics indicate approximately one-third of Plant's known management reports have been accessed less than ten times over the last two years. The reports may provide different data views that are not available within PeopleSoft. Many reports listed have a very specific focus (e.g., biweekly time reporting) and are at least partially redundant to reporting available through PeopleSoft.

  Similar to Utilities consumption data, Plant's work request data is uploaded to PeopleSoft to provide reports accessible to the rest of the University. High-level oversight reports comparing Plant operational and General Ledger financial data are located within Plant's unit-maintained folder in Business Objects. Access to this information helps inform business decision makers across campus. The process to validate data and accuracy of the reports is unclear.

  Management is encouraged to evaluate and document both its financial and operational information and reporting needs, particularly as it relates to oversight reporting. As part of that effort:

  - Incorporate departmental reports and analysis into the division-wide report listing. Make sure this inventory is accessible to staff throughout the division to guard against redundant reporting and duplication of effort.
  - Identify any access barriers for locally maintained data. Division-level oversight and monitoring of reporting and data across the division, regardless of source and location, is a critical control.

- Assess the accuracy and usefulness of reports and purge those no longer considered relevant. Retain documentation of eliminated reports in case a need to reproduce the report or track down the origin of historical data should ever arise.
- Evaluate training and Plant Academy's current course offerings based on the revised reporting inventory.
- Formalize a process for regular review and clean-up of the division report inventory.
- Identify unmet reporting needs and when feasible, allocate resources to address these needs on a continuous basis.
- Develop and provide guidance to aid departments in implementing appropriate controls over department maintained systems. Include guidelines on:
  - Data validation
  - Security
  - Access Controls
  - Backup and Recovery
  - Maintenance
  - Monitoring
- Consider transitioning unit PeopleSoft reports to the UM Maintained repository to improve awareness and accessibility.

Management Plan – Finalize the annual policy to review and evaluate reports that are centrally maintained and/or housed in Plant Operations' systems, including the portal. An additional effort will be made to transfer knowledge to the user population, to provide education regarding reporting and data content.

Additionally, for those systems that cannot be incorporated centrally, guidelines, policies, and procedures will be drafted to aid in data validation, accuracy, integrity, controls, and data recovery. These guidelines, policies, and procedures will be distributed to support local information system development. Plant IT will also provide help desk related support for locally developed and maintained reports.

Plant's information needs are as diverse as the many services it offers and buildings it maintains. Creating a reporting environment dynamic enough to meet such complex information needs is a challenge. University Audits will review progress of action plans during the fourth quarter of fiscal year 2012. A formal follow-up review will be conducted in the second quarter of fiscal year 2013 to evaluate implementation of planned process improvements.

Office of the Provost #2012-203
Report issued December 22, 2011

The Ann Arbor Provost's Office is the top academic unit on campus. The deans of each of the nineteen schools and colleges report directly to the Provost, as do some central administration offices, such as the Office of Budget and Planning, along with academic support units such as Financial Aid and the Registrar's Office. The Provost's Office is also the administrative home of a wide variety of institutes and centers across campus. In addition, University units that serve the overall community, such as the University Library or the University Botanical Gardens, report to the Provost. This wide span of oversight makes the Provost's Office a key unit on campus to establish a strong "tone at the top" for internal controls and fiscal responsibility.

The Provost's Office provides not only strategic support for each unit under its authority, but also significant financial support to programs across the University. Disbursements from the various Provost Office discretionary funds provide substantial funding to numerous programs across campus.

In the past twenty years there have been ten different individuals in the top academic position, and each transition has brought with it different variations on goals, objectives, and priorities.

The primary objectives of this review included:

- *Purchasing* – Evaluated controls over expenses, including P-Cards, travel and business hosting, POs, and non-POs, for appropriateness and adequacy
- *Discretionary Funds* – Assessed oversight of funds managed by the Provost's Office to ensure appropriate use and fiscal responsibility
- *Financial Oversight* – Evaluated financial oversight of Provost Office sub-units
- *Payroll* – Determined if adequate controls exist over payroll functions
- *Office Management* – Determined adequateness and completeness of office policies to ensure consistency of operations
- *Grants and Effort Reporting* – Evaluated policies designed to monitor compliance with grant and effort reporting requirements
- *Asset Management* –Appraised controls over physical assets to ensure appropriate use of University resources
- *Delegated Authority* – Reviewed controls regarding delegation of authority and electronic signatures

Our review identified sound internal controls and a prudent view of fiscal responsibilities from employees within the Provost's Office. Opportunities to strengthen internal controls further are noted below.

Risk and Control Discussion

- Information Systems Shared Services - Recharge Activity – Information Systems Shared Services (ISSS) reports to the Vice Provost for Academic and Budgetary Affairs and supports many offices within the Fleming Building. These include the President's Office, the Provost's Office, and the Office of the General Counsel. ISSS has established an annual fee that is billed to each supported unit to cover the cost associated with services. This qualifies as recharge activity, where one unit charges another for providing goods or services. The Office of Financial Analysis (OFA) must review and approve the cost structure for all recharge activity to ensure the billed rate is appropriate. ISSS recharge activity was not reported to OFA, so no review or approval has taken place.

  Management Plan - We will ask the Office of Financial Analysis to review the current rate structure for the ISSS support fee.

- Concur Approvals – Deans of eighteen schools and colleges are required to submit their expense reports to the Office of Budget and Planning (OBP) for final approval. (Reports for the Dean of the Medical School are approved by the Executive Vice President for Medical Affairs.) However, audit review of approved expense reports of deans showed a significant number that were not approved by OBP, but rather by employees within their own school or college.

  Management Plan - The Office of Budget and Planning will review on a periodic basis the "Travel and Expense Workflow Audit" report to ensure dean expense reports comply with the approval procedures.

A follow-up will be conducted during the third quarter of fiscal year 2012.

Information Technology

Institute for Social Research Data Security #2011-308
Report issued December 7, 2011

University Audits completed an examination of computer and data security controls at the Institute for Social Research (ISR). For over 60 years, ISR has performed interdisciplinary research into the attitudes and behavior of society. Much of this work involves the collection or analysis of sensitive, personal information. Some of this work is also highly publicized, such as the University of Michigan Consumer Sentiment Index[1] and the Monitoring the Future Study[2]. This sensitive data and the discoveries it contains are valuable assets to the University, making information security a high priority for ISR.

Administrative Service Sharing and Collaboration
ISR has five research 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 research centers are all relatively autonomous with regard to staff and faculty hiring, sponsored research activities, budgets, and operations. They are supported by the Center for Institute Services (CIS), which handles functions such as payroll, accounting, timekeeping, facilities maintenance, human resources, event planning, and mailroom services that are shared by all the research centers. This enables coordination and consistent performance of these activities and makes staffing and budgeting more efficient.

Three of the research centers (Population Studies Center, Survey Research Center, and Inter-university Consortium for Political and Social Research) have their own IT units. The Research Center for Group Dynamics has one staff member who provides IT support for the people in that center. Survey Research Center IT provides support for their own center employees as well as for the Center for Political Studies, Research Center for Group Dynamics more broadly, and CIS. Survey Research Center IT also maintains email, network, and Windows infrastructure shared by all of ISR[3]. The leaders of these center IT units, and a few administrative personnel, comprise the ISR Administrative Computing Group.

The ISR Administrative Computing Group meets monthly to promote transparency, facilitate troubleshooting of the varied computing platforms used by each center, and to create any ISR budgets for shared infrastructure costs such as servers, electrical upgrades, and firewalls. These ISR-level budgets, which are distinct from research center-specific IT budget components, are brought forth as part of an annual ISR review process for consideration and approval. The handling of project-specific IT security needs, such as with current sponsored projects from the Department of Defense or data from the

[1] The Index of Consumer Expectations (a sub-index) is included in the Leading Indicator Composite Index published by the U.S. Department of Commerce, Bureau of Economic Analysis.
http://en.wikipedia.org/wiki/University_of_Michigan_Consumer_Sentiment_Index
[2] Monitoring the Future is an ongoing study of the behaviors, attitudes, and values of American secondary school students, college students, and young adults funded by grants from the National Institute on Drug Abuse, a part of the National Institutes of Health. http://monitoringthefuture.org/
[3] Windows infrastructure is shared by all centers except Inter-university Consortium for Political and Social Research, which maintains its own separate infrastructure.

U.S. Census Bureau, are managed by the IT unit of the applicable research center conducting the research. The dominant recipient of these projects to date has been the Survey Research Center.

Escalating Research Partner Expectations
The agencies sponsoring or contracting with ISR have begun promoting information security by imposing increasingly significant security obligations through grant or contractual terms. These terms can be limited and straightforward, or they can be extraordinarily complex. For example, Survey Research Center IT worked diligently with the Department of Defense to assess and improve a plethora of security controls to achieve certification and accreditation of the ISR systems housing Army STARRS project data. This process, known as DIACAP[4], represents a significant accomplishment for the Survey Research Center and ISR. ISR similarly worked with the U.S. Department of Health and Human Services (HHS) to achieve security accreditation under FISMA[5] for ISR systems supporting the National Children's Study and the National Center for Health Studies (NCHS); and the U.S. Center for Disease Control (CDC) to achieve FISMA certification for the National Study of Family Growth.

A proposed regulatory change may further increase ISR's security and compliance burden. HHS published an advanced notice of proposed rulemaking[6] on July 26, 2011, containing Common Rule[7] revisions. The changes include "mandatory standards for data security and information protection whenever data are collected, generated, stored, or used." While other revisions are likely to reduce the regulatory burden on ISR investigators, these mandatory standards will require additional work by ISR IT units.

ISR has risen to meet these expectations in a number of ways. High Security data enclaves were developed to meet FISMA requirements. Two-factor authentication is now required to obtain access to the secure enclaves where highly sensitive research data is stored. Laptops used in the field are fully encrypted. The Survey Research Center also added two full time members to their IT security team and allotted time to two other staff members; growing the team by more than three hundred percent.

Physical security improvements have been made to help protect data within the Survey Research Center managed data centers as well. These data centers house the bulk of the sensitive data in use within ISR. Motion sensitive cameras are in place in the data centers and at access points to the IT offices. Entrance to data centers is protected by two factor access requirements (swipe card and a PIN). Fire suppression systems are being upgraded to inert gas suppression, protecting hardware from damage in the event of a fire. All of these changes have created a safer and more secure environment for sensitive data at ISR.

The purpose of this audit was to validate the design and effectiveness of internal controls supporting data security and management at ISR. University Audits evaluated the policies, procedures, and practices of ISR and its component centers against University policies and research partner obligations, and tested controls when necessary to confirm their proper functioning. Specific audit objectives included:

- Evaluating the ISR IT security program against Standard Practice Guide (SPG) Section 601.27 *Information Security Policy*
- Confirming that IT security initiatives address the risks identified by ISR through assessment processes
- Reviewing ISR centers' compliance with research partner-imposed security requirements

[4] Department of Defense Information Assurance Certification and Accreditation Process
[5] Federal Information Security Management Act of 2002
[6] http://www.hhs.gov/ohrp/humansubjects/anprm2011page.html
[7] The Common Rule is a federal policy regarding Human Subjects Protection that serves as the baseline standard of ethics by which any government-funded research in the U.S. is held.

- Evaluating the incident response process against SPG Section 601.25 *University Information Security Incident Response Policy*
- Confirming the reporting and escalation of serious IT security incidents

Risk and Control Discussion

- Identification and Assessment of Sensitive and Critical Systems – IT inventory systems at ISR are fragmented, and do not uniformly classify IT assets by their confidentiality, integrity, and availability requirements. Without a clear picture of which systems need to be assessed and how to prioritize them, ISR will find it more difficult to ensure that its risk assessments encompass all significant systems.

  The complexity of ISR's IT environment is very high and increasing. The risk assessments completed by the ISR centers represent a point in time. Newer systems must be assessed either individually as they are brought online, or the original assessment re-performed in the new environment. Based on documentation provided, it is not evident that every sensitive or critical ISR system is covered by an existing or planned RECON assessment[8].

  Management Plan – The general type of information recommended lives within each research center and is under that center's governance. Given the acknowledged need for uniformity and to ensure comprehensive assessment across all centers, ISR will develop a plan to identify and track sensitive and critical systems in a formalized, consistent manner. From this plan, an inventory system and assessment schedule will be developed. This will enable a more timely transfer of knowledge and assist with IT work plans for future assessments.

- Risk Mitigation Activities – University Audits obtained and reviewed the RECON assessments completed by the Survey Research Center, the Survey Research Center's Survey Support Lab, and the Population Studies Center. Based on review of the reports and discussion of status, some corrective actions have been significantly delayed because they are contingent on improvements to ISR shared infrastructure.

  The Survey Research Center RECON also identified a number of risks that ISR management should consider mitigating. One of these risks is an overabundance of users with administrative privileges on their workstations. Control of administrator privileges is one of the top twenty security controls recommended for all organizations by The SANS Institute[9]. Malicious websites and email attachments encountered by users with administrative privileges can penetrate a workstation more deeply and pose a greater threat to other systems on the ISR network. The RECON stated these privileges would be reviewed after transitioning from Novell to Windows file servers. That transition occurred four years ago, and administrative privileges remain relatively common among ISR employees using laptops. Survey Research Center IT is gradually reducing privileges as they upgrade workstations to Windows 7.

  Management Plan – Work is ongoing to implement software and hardware upgrades that will allow the security team to improve ISR's security posture.

  The Inter-university Consortium for Political and Social Research and the Population Studies Center are already limiting their user's access to administrative accounts. User accounts are limited to non-administrative access. Selected users are given a secondary, local only,

[8] Risk Evaluation of Computers on Open Networks (RECON) is the standard U-M tool for assessing risks to electronic information.

[9] http://www.sans.org/critical-security-controls/control.php?id=8

administrator account. The other centers within ISR are beginning this transition with the rollout of Windows 7. The Inter-university Consortium for Political and Social Research and the Population Studies Center will be used as models as the other centers make this transition.

The most recent RECON assessment will be reviewed and suggested changes considered.

- IT Security Incident Management – ISR has developed a unit-level incident management procedure, and is following it. Based on review of this procedure and a judgmental sample of recorded IT security incidents, ISR's process could be improved.

  Relevant incident details, such as the name of the affected computer and the date when the incident was first reported, were frequently absent from the reviewed sample of incident reports. ISR's procedure does not specify the information to record when employees report security incidents.

  In documenting incidents, ISR does not consistently address the four questions suggested by Information and Infrastructure Assurance (IIA) to determine whether an incident is serious, and to whom it should be escalated. The four questions are:
  - Is sensitive, confidential, or privileged data at risk?
  - Is business continuity at risk?
  - Does the incident involve Protected Health Information (PHI)?
  - Does the incident involve personal information about a human subject?

  ISR considers all of these factors when handling incidents, but only systematically tracks the involvement of personally identifiable information (PII).

  More explicit documentation would provide better support and evidence of the decision-making process, and would facilitate accurate reporting of the number and nature of serious incidents.

  Management Plan – Survey Research Center-CMT has updated the form in use for reporting potential security incidents. This updated form is now embedded in the FootPrints helpdesk software and incidents are being tracked in the FootPrints database. Information collected in the form is concurrent with the information required by OVPR and IIA in the event of an incident. Survey Research Center-CMT will make this form available to the other ISR IT providers so it can be adopted Institute wide.

- Security Plan – The ISR Information Security Plan reviewed in the audit was written in 2006, and no more recently updated copy was provided. ISR furnished a more frequently updated document on security policy and practices, but it does not contain the same information as the University-required Information Security Plan. SPG Section 601.27 requires that units maintain the information security plans they develop.

  Management Plan – While the ISR Information Security Plan has not been fully updated since 2006, ongoing feedback from IIA Security Progress Reports indicates ISR has met expectations. In any case where ISR was found noncompliant in these Progress Reports, policies and practices were reviewed and updated by ISR as requested. Additionally, ISR has regularly updated the Information Security Concerns and Risks table incorporated in the Security Plan. Understanding the need to formalize the maintenance of the entire Security Plan and its components, the ISR Administrative Computing Group will review, discuss, and update the document as needed with a regular review performed annually. Review dates will be recorded on the front page of the Security Plan. Any relevant changes and updates will be communicated to IIA.

ISR and its component centers are fulfilling their information security responsibilities to the University and their research partners in a responsible and organized manner. The University and partner requirements are very explicit, and ISR is looking for ways to fulfill each of them in a productive and efficient manner. Their IT environment is growing more complex and requires increasing effort to manage and monitor to the degree that partners such as the U.S. Government require. Despite these challenges, ISR has successfully implemented control improvements such as secure computing enclaves, two-factor authentication, encrypted laptops, increased security staffing, and advanced firewalls and intrusion detection systems. Through these improvements, they have achieved the government certifications necessary for ISR to move forward with sensitive research.

University Audits will return to follow-up on outstanding issues in the fourth quarter of fiscal year 2012.

UMHS Lost Laptop Exercise #2011-809
Report issued December 16, 2011

This audit evaluated the effectiveness of the University of Michigan Health System's (UMHS) response to a theoretical exposure of confidential patient data against the privacy and security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. The U.S. Department of Health and Human Services Office for Civil Rights (OCR) enforces the HIPAA Privacy Rule, the HIPAA Security Rule, and the confidentiality provisions of the Patient Safety Rule. Enforcement is handled through investigation of complaints, compliance reviews, and training and outreach programs provided by OCR. OCR has received over 64,000 HIPAA Privacy complaints since April 2003, most frequently alleging impermissible use and disclosure of protected health information (PHI) or lack of safeguards for PHI. Findings of non-compliance can result in significant civil and monetary penalties.

The UMHS Compliance (Compliance Office) was a key participant in this audit. The Compliance Office oversees compliance with all laws and regulations governing UMHS missions in education, research and health care including billing, coding, Medicare and Medicaid, patient privacy, security, relationships and conflict of interest, and governmental investigations. The program's purpose is to maximize compliance with laws and regulations in order to minimize risk of violations and penalties.

The Compliance Office asked University Audits to assist with a mock incident exercise involving an inquiry from Office of Civil Rights ("OCR"), the agency that is responsible for the enforcement of the privacy and security rules. University Audits simulated the theft of a laptop within UMHS and proceeded to identify the presence of sensitive information contained on the laptop. The thief had no previous knowledge of passwords used to secure the computer or the types of data contained on it. To gain access to the computer, the thief used typical "hacking" tools and techniques. A desktop drill was conducted with University Audits, the Compliance Office, Information and Technology Services Information and Infrastructure Assurance, the Health System Legal Office, and the Institutional Review Boards of the Medical School (IRBMED) under the premise that a researcher's laptop containing PHI had been either lost or stolen. The Compliance Office conducted a mock interview with the researcher to determine if the incident was a reportable incident, and if OCR notification was necessary. The interview identified the presence of unencrypted PHI on the laptop, which would trigger Compliance Office notification of OCR. Based on an actual request letter from OCR, University Audits requested the following information from UMHS:

- Documentation of an internal investigation conducted by the covered entity in response to the allegations including a copy of the incident report prepared as a result of the lost laptop.

- Documentation of the covered entity's corrective action taken or plan for actions the covered entity will take to prevent this type of incident from happening in the future, including documentation specifically addressing, if applicable:
    - Sanctioning of the workforce member(s) who violated the Privacy and Security Rules, in accordance with the covered entity's current policies and procedures, and as required by the Privacy Rule.
    - Re-training of appropriate workforce members.
    - Mitigation of the harm alleged, as required by the Privacy Rule.
- A copy of the HIPAA policies and procedures related to the disclosure of and safeguarding of PHI.
- A copy of the policies and procedures implemented to safeguard the covered entity's facility and equipment.
- Evidence of physical safeguards implemented for computing devices to restrict access to PHI.
- A copy of the most recent risk assessment performed by or for the covered entity, per Security Rule requirements.
- Evidence of security awareness training for involved workforce members including training on workstation security.
- Evidence of the implementation of a mechanism to encrypt PHI stored on the workstations.
- A copy of the written notification of the breach provided to the affected individuals.

The scope of this audit was to identify any weaknesses in the process for responding to an OCR investigation.

Risk and Control Discussion

- Risk Assessment – UMHS was unable to provide a risk assessment covering the information stored on the lost laptop. The HIPAA Security Rule requires that organizations conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information. "All e-PHI created, received, maintained, or transmitted by an organization is subject to the Security Rule. The Security Rule requires entities to evaluate risks and vulnerabilities in their environments and to implement reasonable and appropriate security measures to protect against reasonably anticipated threats or hazards to the security or integrity of e-PHI. Risk analysis is the first step in that process."

  The Compliance Office should ensure adequate resources are available for conducting Risk Assessments on systems containing sensitive information on an on-going basis according to UMHS Policy. UMHS should mandate and ensure all University of Michigan Health System units that create, receive, maintain, or transmit PHI have an accurate and thorough assessment of potential risks and vulnerabilities to the confidentiality, integrity, and availability of that PHI. Unit-developed risk management tools should be reviewed by the Compliance Office to ensure they are adequate and meet the requirements of the HIPAA Security Rule.

- Encryption – The subject laptop contained PHI that was not encrypted. UMHS Policy 01-04-502 states: "Sensitive information stored on portable electronic devices or removable media shall be encrypted with the strongest encryption method practicable." Encryption protects data from unauthorized access and provides covered entities a safe harbor if the device is lost or stolen. Therefore, UMHS would not have been required to report the loss of the subject laptop to OCR if encryption was implemented under UMHS Policy 01-04-502.

The Compliance Office should enforce policy that directs personnel to encrypt sensitive data. Units that handle sensitive information (e.g... ePHI) on mobile devices need to work with the Compliance Office to ensure that current methods used to protect their sensitive data are available, adequate, properly used, and in line with HIPAA standards. Possible expansion of encryption software licenses to include all units that deal with PHI would help ensure all units have access to an acceptable method for encryption.

- Compliance and Security Awareness Training – The Compliance Office is unable to show 100% completion rate of mandatory training for UMHS personnel. Workforce members are required to attend training programs designed to explain UMHS compliance plans, but not everyone participates. The Corporate Compliance Program Policy indicates that: "Attendance at a minimum of one annual training program shall be mandatory for employees. The training programs will be designed to review the compliance plan and to delineate with specific employees any changes in current policies that effect their specific position." Units are responsible for ensuring appropriate training is assigned to their personnel, and acting on centrally provided notification of missing or expired training.

  Management Plan – The Compliance Office acknowledges the risk and control discussions initiated by this exercise and is prepared to facilitate remediation efforts in collaboration with other key stakeholders in UMHS that will manage this risk and mitigate the likelihood of a breach.

  The Compliance Office will take the following actions: (1) submit a request for two additional FTEs; (2) verbal support has been given to ITS/IIA to purchase risk assessment services from IIA should this service be reconstituted; (3) pending outcome of #1, the Compliance Office will seek an increase in operating dollars to acquire contract services; (4) conduct benchmarking to determine adequate IT auditor staffing for Compliance Office.

  The Compliance Office will take steps to increase enforcement of encryption requirements and mandatory training requirements for all staff and faculty within UMHS who access, store or transmit ePHI.

Based on the results of this exercise, UMHS is well prepared to respond to and remediate an exposure of PHI, but controls for preventing the exposure could be improved. The internal investigation process was thorough, gathering all of the appropriate information. Corrective action plans resulting from the exercise suitably addressed the areas of concern. The group discussed creating a formal process for following up on corrective action plans with the units involved. Policies were complete and up to date. A suitable notification letter was prepared, and would have been sent to affected individuals in a timely manner if this were an actual breach. Follow-up on management responses to identified issues will take place during the second quarter of fiscal year 2013.

Healthcare

University of Michigan Medical School Department of Emergency Medicine #2011-204
Report issued December 5, 2011

The Department of Emergency Medicine has nationally recognized clinical expertise in trauma, chest pain, toxicology, brain injuries, and pediatric emergency medicine. The Department is part of the Medical School and is an integral part of Emergency Services at the University of Michigan Hospitals and Health Centers (UMHHC). UMHHC provides a full service Level 1 adult and pediatric trauma center staffed and equipped to deal with all urgent and emergency problems. Emergency Services is a

major access point to the services and facilities of the University of Michigan Health System and it provides emergency care to approximately 60,000 adults and 20,000 children annually, operating 24-hours a day, 7-days a week.

Emergency Medicine was originally part of the Surgery Department; it was recognized as its own department in 1999. Since then, clinical activity and research funding have continued to increase and the Department has seen an expansion of its education and clinical programs.

The Department of Emergency Medicine offers a four-year residency training program and a Pediatric Emergency Medicine Fellowship program. The Department receives over $9 million annually in research funding from the Departments of Health and Human Services, Defense, and Transportation and nationally ranks first in extramural research funding among Departments of Emergency Medicine. The Department is currently conducting a nation-wide search for a new chair. The current chair has led the department since it was founded in 1999 and is stepping down to devote more time to patient care and research.

The primary objective of the audit was to review key operational processes within the Department of Emergency Medicine to determine if policies, procedures, and the internal control structure adequately protect University assets and comply with U-M and UMHS policies and procedures. The scope of the audit was departmental activity directly under the financial and operational management of the Medical School, and did not include the Emergency Department patient care operations, which are jointly managed by U-M Hospital and the Medical School Faculty Group Practice.

University Audits evaluated the adequacy and effectiveness of controls governing the following processes within the Department of Emergency Medicine:

- Financial and operational controls and accountability
- Timekeeping and payroll
- Purchasing, P-Card, and travel expenditures
- Financial reporting and budgetary functions
- Grant management and compliance with effort reporting requirements

Risk and Control Discussion

The Department of Emergency Medicine has a robust process for reviewing financial statements and performance metrics. The Chair, the Finance Department Administrator, the Finance Department Manager, and faculty meet monthly to review a detailed financial package and analyze variances between projected and actual financial performance. Grant activity and effort allocations are monitored closely to ensure expenses charged are appropriate and allowable. The administrative staff is relatively small in number, given the size and complexity of the Department. The Department has a dedicated and hardworking staff that performs many functions. Because of limited staffing resources, there is a lack of segregated roles and internal controls. Opportunities to strengthen the overall control environment are discussed below.

- Internal Control Assessment Certification – Each year, University management is required to assess and certify departmental compliance with University stewardship and fiscal responsibilities as part of an ongoing University initiative to establish and maintain strong internal controls. The annual certification process helps the University fulfill financial management responsibilities towards organizational governance and accountability. An important and required part of the certification process is the completion of internal controls gap assessments. The gap assessments are completed between January and September of each year.

Based on the assessments within their units, the Dean or other official certifies on an annual basis that the assessment is complete.

The Medical School requires certification at the departmental level to ensure appropriate internal controls are at the unit level. Over the past few years, UMHS Financial Services took the leadership role in educating UMHS unit management of their responsibilities as part of the certification process. At the time of the audit, the Department of Emergency Medicine was not fully aware or engaged in the process. In prior years, annual certifications were signed as fully compliant without performing the underlying assessment and detecting existing internal control gaps that are highlighted as part of this report. In September 2011, the Department certified their internal control assessment for fiscal year 2011 as partially compliant and is in the process of remediating gaps.

The Emergency Department management and staff are actively working with the Office of Internal Controls and UMHS Financial Services to improve their internal control environment.

Management Plan – Department Administrator, Department Finance Manager, and Department Human Resources Manager met with the Office of Internal Controls and UMHS Financial Services to review the internal control process and begin assessing internal control gaps. The Department Administrator will collaborate with department managers in maintaining and updating controls education and completing the annual gap assessment.

- Non-Certified Effort Reporting – The federal government (Office of Management and Budget Circular A-21, *Cost Principles for Educational Institutions*) requires annual effort certification for all employees working on federally sponsored research or who allocate effort between functional activities such as instruction and administration or patient care and instruction. A review of effort certification for fiscal year 2010 and 2011 identified several employees who had not certified their effort.

  To improve effort certification in the Department:
  - Discuss roles and responsibilities with project administrators and individuals responsible for monitoring effort reporting, ensuring they have resources and knowledge necessary to monitor processes.
  - Develop an effort reporting compliance monitoring process to identify employees not complying with certification deadlines. The process should be formally documented and include an escalation process for employees who do not certify after repeated reminders and procedures for certifying for staff who terminated during the year or are on a temporary leave of absence.
  - Complete past due certifications as soon as possible.

  Management Plan – The Human Resources Manager circulates effort reports on a quarterly basis to faculty and staff to review accuracy. Management revised the department's effort certification process to include the recommendations above. At the end of the fiscal year, the Human Resources Manager will monitor the effort reports until all applicable employees have certified. The Human Resources Associate will continue to monitor the reports monthly to identify new effort certification issues.

- Purchasing – Purchasing procedures are outdated. System reports should be reviewed to ensure P-Card limits and cash withdrawal privileges are appropriate, Concur expense approvers receive annual training, and Concur expenses are processed timely. Purchasing approval limits for approving non-POs are not documented.

Management Plan – Purchasing policies are in the process of being revised by the Human Resources Manager and Finance Manager. Policy will be updated and staff informed of changes by February 2012. Every June, the Human Resources Manager will review P-Card limits and usage with Managers and make adjustments as deemed necessary. In the future, the Human Resources Manager will review Concur reports and work with department management to ensure approvers have completed their annual training. The Human Resources Manager will follow-up with the appropriate manager and the Department Administrator for non-compliant staff. The Finance Manager revised procedures for processing non-PO vouchers.

- P-Card Transactions – The department has many opportunities to improve preparation and approval of Concur expense reports including:
    - Using report names that include a keyword or description that identifies the primary reason for the expense
    - Documenting a clear business purpose that explains why the specific expense is necessary
    - Attaching receipts containing appropriate detail, including detailed item charges
    - Analyzing P-Card expenses for items and purchases to identify expenses that may be more appropriately purchased through an internal service unit or University preferred vendors
    - Selecting accounts for expenses that best matches purchase category
    - Reviewing receipts to ensure supporting documentation is included and accurately reflects the purchase made
    - Utilizing the Department Reference field to tie related expenses from multiple expense reports together
    - Ensuring all approvers complete annual Concur training

The Standard Practice Guide recommends that approvers have the responsibility for approving expenses for no more than 25 expense submitters. More than 115 employees submit expense reports. The Human Resources Manager and the Chief Department Administrator approve all expense reports.

Management Plan – Department Administrator will review the University policy at the November Emergency Medicine Managers Meeting and will request that managers review policies with their staff by December 15, 2011. Concur users and delegates will go thru Concur Refresher Training as required. The Department Administrator and Human Resources Manager will revise department P-Card procedures to outline the recommendations noted above. This will be accomplished by February 2012. The Department Administrator will begin the process of reducing the number of Concur reports approved by the Human Resources Manager and Department Administrator by engaging shared responsibility with other department managers by January 2012.

- Gross Pay Register Reconciliation – The reconciler of the Gross Pay Registers also initiates payroll transactions. These roles should be segregated. In addition, management does not regularly review pay registers or the completed reconciliations.

Management Plan – The Human Resources Manager will review and approve timesheets with overtime compensation and verify Gross Pay Registers for accuracy. The Human Resources Manager will review Gross Pay Registers to ensure accurate reconciliation and will ensure unusual transactions are followed-up. This will be implemented January 2012. The Department

will seek guidance from UMHS Financial Services on utilization of eReconcilation verses current reconciliation process.

- Statement of Activity Reconciliation – The department utilizes various mechanisms for Statement of Activity (SOA) reconciliation and financial oversight. Not all transactions are reconciled to source documentation on a monthly basis. Reconcilers also perform purchasing functions and create and enter journal entries; roles are not always segregated. Management does not review the monthly reconciliation.

  Management Plan – The Financial Manager has updated the reconciliation procedure and will work with managers/grant administrators in confirming/designating account reconcilers and reviewers by December 31, 2011.

- Delegation of Authority – University Audits identified several situations where individuals were approving expenditures that require the approval of the department chair or grant principal investigator.

  Management should identify all existing delegation of authority permissions. The delegator should evaluate if the assignee has the knowledge needed to assess the appropriateness and reasonableness of the expense. The delegator is still accountable for transactions the assignee performs on their behalf. All delegation of authority permissions should be documented according to University guidelines and renewed annually; see *Employee Travel and Expense Internal Control Matrix* at http://www.finance.umich.edu/controls/tools.

  Management Plan – The Human Resources Manager is currently in the process of obtaining delegation of authority documents and will maintain copies in our files and ensure that the delegators understand they are still accountable. The Human Resources Manager will monitor and renew delegation of authority forms annually.

University Audits will conduct a follow-up review in the first quarter of fiscal year 2013 to assess progress on management action plans.

Follow-up Reviews

Information and Technology Services Shared Desktop #2010-315
Original report issued February 28, 2011 Follow-up report issued December 20, 2011

Changes to requirements and timing for deploying new services within Information and Technology Services (ITS), and resource reallocation to NextGen Michigan initiatives have impacted the Shared Desktop program and the management action items identified below. In light of these changes and action taken by management, **this audit is closed.**

- Included Software – University Audits recommended that ITS ensure applications that are preinstalled on the shared desktop image are licensed correctly and copies of the licenses are available. In response, ITS has obtained the appropriate distribution license for Adobe Reader and RunTime software. The Citrix ICA Client is being removed from the Shared Desktop image.

- Shared Desktop Program – At the time of the audit, the Shared Desktop program was still considered a pilot program by ITS. It was recommended that ITS determine if the program

should go to production or be removed. At this time, current procedures to provide a shared desktop service within ITS are being modified. The Shared Desktop Image is being evaluated for inclusion into the NextGen End User Computing project. Management has made a commitment to providing the Shared Desktop Image on an ongoing basis and continues to work towards implementing the End User Computer service as a fully supported ITS service.

- Disaster Recovery Plan (DRP) – University Audits recommended that the ITS Infrastructure Services Desktop Infrastructure group and other units responsible for distributing the Shared Desktop image should develop Disaster Recovery Plans. Since the original audit, circumstances surrounding the Shared Desktop have changed significantly. Due to the NextGen End User Computing project, Disaster Recovery Plans will not be developed specifically for the Shared Desktop image. Disaster Recovery Plans will be developed for the End User Computing service. Based upon these circumstances there will be no need for a specific Shared Desktop Disaster Recovery Plan.

- Windows 7 Security/Configuration Design – The Windows 7 Shared Desktop image lacked security and configuration design documentation. Presently, Group Policy is being utilized to configure the Shared Desktop image. A draft document identifying the configurations has been developed and is awaiting review and approval.

- Updates (Patch Level) – At the time of University Audits review, vulnerability scans identified missing security patches for Adobe and Java (JRE/JDK) products. Currently, ITS is providing two versions of the Shared Desktop image, the current version and one previous version. The Shared Desktop image is updated three times a year. In addition, ITS will also be providing an image that is continually updated with minimal hardware testing for those users requiring the latest updates. Work is also being done to update the Service Level Agreement with the administrators to convey the importance and responsibilities for updating computers prior to deployment.

Portable Electronic Devices UMHS — #2009-305
Original report issued August 26, 2010
First follow-up report issued September 8, 2011
Second follow-up report issued January 3, 2011

University of Michigan Health System (UMHS) Medical Center Information Technology (MCIT) is in the process of addressing all action items and is working with UMHS Compliance and Medical School to proceed with implementing the changes. **This audit is closed.**

- Proper Use Standards – UMHS agreed to implement a User Agreement specific to the Portable Electronic Devices and a training process. MCIT has developed a course for MLearning that will present all of the necessary Portable Electronic Device compliance and security information. At the end of the course, staff will be required to confirm that they have read, understand, and agree to follow the information contained in the course.

- Exposure Based on Standard Configuration – At the time of the Audit, University Audits recommended that password complexity be increased. MCIT is deploying a policy for BlackBerry devices that utilize the BlackBerry Enterprise Server that is similar to Exchange ActiveSync policies.

- Mobile Devices Policy – University Audits asked UMHS to ensure that UMHS and MCIT policy governing portable electronic devices are not changed in such a way that they contradict each other. Verbiage found on the MCIT policy was clarified so that UMHS and MCIT policies complement each other. This policy is still in draft form and awaiting review.

- Access Control – It was noted during the audit that MCIT should document the procedures that are taken to identify users who are no longer authorized on UMHS networks and the steps taken to remove a user and the Portable Electronic Device from the BlackBerry Enterprise Server ensuring that the Portable Electronic Device can no longer access UMHS networks or systems. MCIT is in the process of fully documenting the complete process from initial activation to final deactivation of all BlackBerry devices that exist on the BlackBerry Enterprise Server. MCIT has conducted and now completed documented interviews capturing the lifecycle of a blackberry device on the BlackBerry Enterprise Server. A detailed analysis report was completed.

LSA Research Computing #2010-809
Original report issued July 27, 2010 Follow-up report issued January 4, 2012

LSA is the largest college at the University of Michigan, and is home to a large research community. LSA Information Technology (LSA IT) provides support for the entire college. The Research Systems Group (RSG) and IT Security and Asset Management (LSA-Sec-ITAM) teams provide many services, depending on the requirements of the researchers.

Despite the support offered by LSA IT, many researchers chose to manage their own systems. The audit focused on the systems managed by researchers or their designees, not IT professionals. These systems are referred to as "unmanaged" machines. University Audits reviewed some of these systems and the policies and guidance provided by LSA IT for these systems.

- Security Policy – Departmental policies reviewed during the original audit were of varying quality. Many departments within LSA had no security policy and relied solely on LSA IT's security policy for defining acceptable behavior. While LSA IT's policy was well written, it did not address many concerns in regard to unmanaged research systems. University Audits recommended LSA IT revise their policy and provide assistance to departments in creating their own policies where appropriate.

  LSA IT's new security policy is a significant upgrade to its predecessor. Requirements for all networked systems are clearly stated. Consequences for violation of policy are clear and sensible. The procedure for obtaining an exemption to specific requirements is clearly laid out and very practical. Templates of policy documents have also been created for departmental use. These documents contain suggestions for formatting and content of department-level policy.

- Data Classification – The departments within LSA represent a great variety of academic disciplines. Therefore, there is a wide variety of research data to be managed. Different types of data require different levels of management, security, and control. Data that is sensitive requires more security protection than data that is not as sensitive. University Audits noted at the time of the original audit that no guidance was available to researchers to help them determine what data was sensitive. University Audits recommended LSA management work with LSA IT, departmental system administrators, and researchers to create a document defining sensitive data and correlating levels of sensitivity to the way the data should be managed. It was also recommended that a process be put in place for assessing data that did not fit neatly into an existing classification.

LSA IT has created a document with questions to help researchers determine the level of sensitivity of their data. These questions are followed by a chart detailing what measures must be taken to secure data depending on its classification. These charts are complete and will assist researchers in properly classifying and securing their data.

- Data Storage and Backups – Many of the researchers within LSA work with very large data sets. These large repositories of data create unique storage problems. To solve these problems, researchers often purchase their own additional storage (usually in the form of external hard drives) instead of utilizing solutions provided by the department, college, or University. University Audits recommended LSA IT, department level IT staff within the college, and Information and Technology Services (ITS) work together to develop an affordable, easy to use storage and backup solution for the research community within LSA.

  LSA IT has assembled a packet of information for researchers detailing the various backup solutions available to them and the strengths and weaknesses of each solution. LSA IT has also created a proposal for a new, researcher focused, backup and data storage system. They are working with ITS on the possible implementation of this system. The proposed system is robust and would meet the needs of LSA's research community. It would also serve as an excellent test environment for a University wide system. LSA IT has provided researchers with the information they need to make informed decisions about the storage and backup of their data using current options.

- Training and Guidance – Researchers' areas of expertise lie within their particular disciplines. They are not, and should not be expected to be, IT professionals. They are often unaware of IT best practices, security concerns, and the solutions to their computing needs and problems. University Audits found that many researchers were unaware of current services provided by LSA IT and ITS that would address their research computing needs. University Audits recommended that LSA IT develop training materials for their research community to help raise awareness of available solutions.

  LSA IT developed a website with information on the various services they provide as well as those from ITS. This site contains best practice information on items such as data storage, backup, and computer security. Plans are in place to ensure the site is regularly updated to stay current with new technologies. This guidance provides researchers with the necessary tools to better manage their data and computers.

- Antivirus Software – University Audits found that some researchers were not using antivirus software on the systems they use to perform research and store research data. Mandatory use of antivirus software was recommended for all machines on the LSA network.

  LSA IT has created a new policy requiring antivirus software on all network connected machines. In anticipation of potential problems for older systems running custom software and hardware, an exception process is described within the policy. Systems that are exempted from the antivirus policy must have a compensating control to protect them, and the rest of the network. This policy is clear, thorough, and sensible for the environment.

- Disaster Recovery Plan (DRP) – Some of the units reviewed during the audit had no disaster recovery plans. University Audits recommended departmental IT staff work with their researchers to develop plans as appropriate.

The National Science Foundation (NSF) began requiring data management plans (DMP), which are similar to DRPs, for grants issued after January 18, 2011. This is forcing many researchers who did not previously have DRP-like documents to develop them. To help, LSA IT has put together an instructional website with links to multiple documents that will help researchers prepare their DMPs. This site also provides the researcher with guidance on preparing a formal DRP, as much of the information is similar. The guidance provided by LSA IT is detailed, easy to follow, and addresses the need for unit DRPs.

- Physical Security – The level of physical security for research systems reviewed during the audit varied widely. University Audits recommended that each department review their physical security practices.

  LSA IT developed college-wide requirements for physical security of computers and data as part of its overall security plan. The document includes a chart prescribing security requirements for systems based on the level of sensitivity of the data they contain. This document provides clear guidance on physical security for researchers and department IT staff.

LSA has made significant progress in improving the security of unmanaged systems used within their research community and their network as a whole. Researchers now have the information and tools they need to ensure their systems and data are properly protected. **This audit is now closed.**

Building Automation Systems #2010-809
Original report issued April 19, 2011 Follow-up report issued January 20, 2012

The Building Automation System (BAS) is part of the University of Michigan's Facilities Maintenance department within Plant Operations. It facilitates the monitoring of critical functions in buildings across campus, in real time, from a central location. BAS monitors conditions such as temperature, air flow, and humidity at 146 different facilities with 199,681 data collection points.

Information is gathered by data collection points (sensors) located throughout buildings. These data sensors relay information to panels, monitoring computers, and servers that are connected through a diverse and complex network. All of this information is collected on a central server that tracks building status and alerts BAS technicians of inappropriate changes and building system problems.

An initial follow-up review was issued on April 19, 2011. This follow-up review examined the remaining open audit issues and the corrective actions taken by BAS management.

- Open Ports on Monitoring Devices – Data collection points throughout buildings connect to panels that, in turn, connect to the BAS central server. There are two types of panels that have the ability to connect directly to the University network to deliver data. Other types of panels connect through intermediate devices; one of which connects to the University network. University Audits performed vulnerability assessments on these network-connected devices and found multiple open ports that did not need to be open. An unused open port provides an unnecessary point of access to the device and could provide an avenue for inappropriate or malicious access. University Audits recommended BAS management contact the suppliers of the network connected devices to investigate the possibility of disabling unnecessary ports.

  In lieu of working with the vendor to make fundamental changes the devices, BAS management has elected to move the devices to a private, secure network. This change will also require moving most of the BAS infrastructure to a private, secure network, but is a superior solution as

it offers greater protection from malicious activity. Management has made significant progress in moving monitoring devices from open networks to BAS dedicated networks. The remaining devices are planned to be isolated and management has committed to applying resources to complete this effort in the next six months.

- Network Security – BAS's central server is critical to building monitoring. It functions as the clearinghouse for all monitor and alarm information coming in from all of the data points across campus. University Audits recommended that BAS management work with Plant IT to ensure that appropriate network security practices are being employed to secure the central server. BAS and Plant IT have implemented a redundant two server cluster for the database and user restricted access to the monitoring application interface to a single terminal server machine. This terminal server enables a secure managed environment for interacting with BAS monitoring devices.

- Network Isolation – BAS building panels and monitoring systems are connected using dedicated lines, the University's data network, or a combination of the two. Newer panels and devices are designed to work over a data network. As BAS has grown and upgraded equipment, more of their devices are connected using the University's data network. As this transition has taken place, BAS has utilized existing network hardware and connections resulting in devices using multiple networks across campus. Some of these networks are unsecured and are not controlled by BAS or Plant IT. BAS and Plant IT are working with ITSComm to move BAS devices to a private, secure network. One set of data points and the monitoring PC they communicate with have been successfully moved. Work on this item is ongoing.

- BAS management and Plant IT have collaborated with ITSComm to make private Virtual Local Area Networks (VLANs) available to BAS devices. A significant majority of devices have already been moved onto these VLANs and a plan is in place to move the remaining devices.

Management has made significant progress in resolving the issues identified in the audit. Challenges facing management require cross-functional collaboration with other units due to their complex nature and the multiple parties involved. The issues reviewed in this follow-up have either been completed or are in the end stages of issue mitigation. **This audit is closed.**

Financial Analysis Management of Asset Data, Space Data, and University Surplus #2010-111
Original report issued May 10, 2011 Follow-up report issued January 24, 2012

Financial Analysis' Property Control Office, Office of Property Disposition, and Office of Space Analysis are responsible for managing University of Michigan property, including the tagging and tracking of capital and government-titled assets, asset disposal, and tracking space and location data of University owned and occupied spaces.

University Audits recently performed a follow-up review to assess the status of management's action plans. Management has significantly implemented all but three of the control recommendations identified during the audit. University Audits will conduct a second follow-up review in the fourth quarter of fiscal year 2012 to follow-up on open items. A summary of management's actions is noted below.

- Staff Oversight – University Audits recommended that management revise Property Control business practices to ensure management has an effective system of oversight for inventory coordinators. In response, management is revising procedures, reassigning responsibilities, and retraining Property Control staff. This effort has been precipitated by the need to prepare for the

departure of an inventory coordinator, who will be taking a military leave of absence beginning February 2012. As part of this response, the inventory coordinator function will be reexamined. The Business Operations Manager will work with the Inventory Control Manager to ensure inventory coordinators update their calendars and input data entries on a timely basis. **University Audits will continue to follow-up on this item.**

- Capital Asset Inventory Management – Property Control Office management revised practices for following up on missing assets and reporting inventory discrepancies to department administrators. The new process includes more efficient communication with departmental staff regarding missing items and escalated communication to higher administrative authorities if assets continue to be missing. **This item is closed.**

- Government-Titled Assets – Office of Management and Budget (OMB) Circular A-110, *Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations*, requires an annual inventory of government-titled assets. Management reduced the number of physical inventories of these assets to one per year in compliance with this regulation. Previously, two inventories were done per year. Management also updated the Property Control Office procedures manual to ensure robustness and efficiency. Inventory coordinators continue to perform periodic random site visits to verify high-dollar value equipment and equipment susceptible to theft are maintained in designated locations. **This item is closed.**

- Asset Tagging – During the original audit, inventory coordinators began logging untagged equipment that was noted during fieldwork. Coordinators now follow-up on equipment that remains untagged for more than 30 days. The template for logging untagged equipment examined during the audit did not contain space for the inventory coordinator to designate when the equipment was eventually tagged. Management modified the template to include columns for indicating the tag number and tag date. **This item is closed.**

- Data Security – Computers and other electronic devices are included in the surplus property processed by Property Disposition. Departments that send surplus electronic equipment to Property Disposition for sale are required to ensure all software and data are removed from the equipment (cleansed/wiped) and sign an affidavit attesting that the equipment has been cleansed. During the audit, certain machines received from other departments were found to contain either data or software. In response, Property Disposition:
    - Revised processes for handling surplus electronic equipment. When departments send computers and electronic storage media to Property Disposition, Property Disposition requires them to include the Declaration of Surplus (DOS) form with the signature of the individual who cleansed the data from the equipment.

    - By agreement with Property Disposition, University Libraries and Business and Finance cleanse the data from their own machines before sending them to Property Disposition. Two signatures, the person who cleansed the machine and that person's supervisor, are required for Property Disposition to accept the machine for disposition. Property Disposition's experience indicates that the Library and Business and Finance are effectively cleansing their machines, so they place those machines directly onto the sales floor upon receipt.

    - Property Disposition staff continues to test and cleanse surplus equipment as necessary. Testing has become more systematic and focused on the types of machines that have

historically not been cleansed properly resulting in a larger percentage of machines tested. Staff currently:

- Cleanse all electronic equipment received from departments with missing or incomplete DOS forms (i.e., missing certification that equipment was cleansed)
- Test ten to twelve computers from each shipment from departments that send a properly completed DOS form
- Test and cleanse all single machine deliveries
- Track offenders. Property Disposition is considering imposing a cleansing fee for departments that repeatedly fail to fully cleanse machines

Audit testing indicated that the machines offered for sale are being effectively cleansed of proprietary software and data. **This item is closed.**

- Outside Trucking – Management is in the initial stage of developing practices that will ensure proper controls over deliveries of surplus to Property Disposition. Management plans to work with UMH Interior Designs and Procurement Services to strengthen delivery protocols. **University Audits will continue to follow-up on management's progress.**

- Sale of Goods – Management enhanced processes to identify surplus and ensure departments receive credit for sales. Management also documented its markdown and discount policy. Property Disposition recently purchased a new point-of-sale system and expects it to be installed in January. Management will document all processes after the new system has been tested and the old system has been converted. **University Audits will continue to follow-up on management's progress.**

- Physical Security of Assets – University Audits recommended that management institute procedures to verify that customers are leaving the facility with only legitimately purchased items. Management has implemented several practices to strengthen sales floor controls that appropriately address this item:
  - Property Disposition staff randomly questions customers to verify customers have receipts for items they are removing from the warehouse.
  - Warehouse staff closes delivery doors during non-public shopping hours. University employees shopping during this time must enter the warehouse through the main entrance near the central office. Effective December 2011, University employees will need to show ID if Property Disposition staff does not recognize them.
  - During non-public hours, Property Disposition office staff makes public announcements to let floor staff know when customers are in the warehouse.
  - Management is reviewing the usage of all signage throughout the warehouse. They are also discussing the feasibility of hanging signs to discourage loitering as an added security measure.

  This item is closed.

- System Access/Data Integrity – Review of the PeopleSoft Space Management System (the authoritative source for all University space data), the PeopleSoft Asset Management System (the authoritative source for capital asset information), and a stand-alone database system used by Property Control to track government-titled assets revealed potential risks to data integrity due to improper access by individuals who have left the University or the department.

- Management developed a termination checklist to assist in performing the necessary tasks to successfully exit employees. The department's Human Resources (HR) Unit Liaison is responsible for completing this checklist. Effective December 2011, managers also began using the checklist. This is appropriate because management, as opposed to HR, is generally responsible for collecting keys, University identification, and other items from departing employees and terminating system access.

- Management terminated improper system access rights for several individuals. Although it remains HR's responsibility to monitor system access, in the future, management will periodically review access reports to ensure system access roles are assigned appropriately.

- Management worked with Information Technology Services (ITS) to develop a process to ensure Property Control Office staff monitors department-modified serial/model numbers in the Asset Management System. The new process is in test phase.

This item is closed.

- Space Survey Submissions – Space Analysis staff revised the department's practice for follow-up on late surveys. During the last survey, the new process resulted in a faster response time. **This item is closed.**

- Building Phase Definitions – Management has defined building phases and consistently applied new definitions to existing buildings, structures, and spaces. **This item is closed.**

Open Audits Follow–up Table
January 31, 2012

Audit Title	Report Date	Issues	Expected Completion
CAC and ITS Use of Federal Hardware in the Flux HPC Cluster 2011–810	4/12/11	Transitory oversubscription of federal hardware	First Follow–up June 2011 June 2012
UM–Flint Business Continuity 2011–303	8/12/11	University impact analysis; BCP standards template; business continuity testing; disaster recovery plan	March 2012
UMHS Level 2 Identity Management 2011–306	8/26/11	Password distribution	March 2012
ITS CTools Software Development Processes 2011–808	8/29/11	Documentation; back–ups; Use of wush.net	March 2012
College of Literature, Science, and Arts Information Technology Asset Management 2011–311	7/22/11	Use of the K2 client; firewalling license servers; changing and deleting users; key process areas; project management; disaster recovery and business continuity plans testing; management of copyrighted software; licensing processes; maintenance of access control lists	March 2012
Information and Technology Services eResearch Proposal Management 2010–304	6/27/11	Contractual restrictions on vendor access; "Site Manager" access	February 2012
Information and Technology Services MCommunity Sponsored Accounts 2011–304	11/22/11	Sponsorship administrator roles; improper permissions; monitoring of sponsored accounts; data verification policy; recurring training; policy enforcement	May 2012
Institute of Social Research Data Security 2011-308	12/7/11	Identification and assessment of sensitive and critical systems; risk mitigation activities; ITsecurity incident management; security plan	August 2012
UMHS Lost Laptop Exercise 2011-809	12/16/11	Risk assessment; encryption; compliance and security awareness training	December 2012
Center for Human Growth and Development 2009–206	11/17/09	Security/maintenance of sensitive data; monitoring grant budgets; imprest cash fund management/subject fee payments; disaster recovery/business continuity planning; statement of activity reconciliation/segregation of duties	First Follow–up August 2010 March 2012

Division of Research Development and Administration Export Controls Compliance 2010–402	10/21/10	Training and education; export control identification; technology control plans; information technology controls; technology disposition	First Follow–up June 2011 March 2012
UM–Flint School of Health Professions and Studies 2010–209	1/25/11	Segregation of duties; faculty and staff certifications; privacy and data security; policies and procedures; P–Card controls; conflict of interest and conflict of commitment management; affiliate payment processing	March 2012
University of Michigan–Flint Educational Opportunity Initiatives 2010–201	2/18/11	Strategic oversight and guidance; campus support and collaboration; budget and financial management; staff management; time reporting and payroll; event management; cash handling; business continuity; documentation of policy and procedure	March 2012
Conference Services 2010–102	2/25/11	Contract compliance; department accounting and reporting; billing and payment accuracy; payroll and time reporting; statement of activity reconciliation; background check verification; client management	February 2012
Division of Student Affairs Recreational Sports – Club Sports 2010–816	3/2/11	Sponsored student organizations; guidance; financial management; practice, game, and fitness space; medical support; property	February 2012
University of Michigan Flint Cashier's Office 2011–804	3/22/11	Vault balance; accuracy of cash; petty cash reimbursement; deposit delays; segregation of duties; collection process efficiency; security and access; policies, procedures, and training	First Follow-up January 12 April 2012
Office of the Vice President and General Counsel 2010–207	4/22/11	Physical and electronic document security; conflict of interest/conflict of commitment; monitoring matters requiring retention of outside counsel; document management; expense reimbursements; OGC procedures; annual certification and controls assessment	March 2012

Financial Analysis – Management of Asset Data, Space Data, and University Surplus 2010–111	5/10/11	Staff oversight; capital asset inventory management; government–titled assets; asset tagging; data security; outside trucking; sale of goods; physical security of assets; system access/data integrity; space survey submissions; building phase definitions	First Follow-up January 2012 May 2012
College of Literature, Science, and the Arts Center for Afroamerican and African Studies 2010–820	6/1/11	Cash handling; travel advance procedures; purchasing review; P–Card/Concur process; conflicts of interest; payroll records; CAAS equipment; study abroad program administration; storage of business critical data	December 2011
Emergency Loans in Financial Aid 2010–112	6/7/11	Inconsistent processing; regulatory compliance; policies and procedures;	February 2012
Leased Employees 2011–112	6/7/11	Central process owner; identification of leased employees; U–M guidance; contracts	March 2012
University Unions 2011–814	6/15/11	General control environment; financial monitoring and oversight; purchasing management; human resource management; building renovation and maintenance	March 2012
Financial Considerations for International Activity 2011–101	6/30/11	Coordination of effort; documented policies and procedures; currency exchange; cash purchases; international bank accounts	March 2012
UM–Dearborn Office of the Provost 2011–210	6/30/11	Segregation of duties; timekeeping; policies and procedures; Fairlane Center procedures; collections and exhibitions	March 2012
Service Unit Billing 2011–104	7/26/11	Ownership of SUB process; identifying recharge activity; inactive recharge information; FTP account management; reporting options	March 2012
Department of Geological Sciences Camp Davis Rocky Mountain Field Station 2011–813	7/28/11	Fire safety and inspections; documented policies and procedures; inventory management; documented emergency plans; cash handling; external entities	May 2012

Ross School of Business 2011–202	10/19/11	Budget preparation and review; Ross art collection; institutes and centers – oversight and monitoring; loans to international students; international programs – coordination; verification of Aramark reported data; sub–certification of internal controls; credit card monitoring/guidance; continuity of operations planning; unit assessments	June 2012
School of Dentistry Admissions and Financial Aid 2011–812	10/26/11	Multiple Mini Interviews (MMI); application review; documentation; application fees; spreadsheet controls; need–based aid	June 2012
Intercollegiate Athletics Stephen M. Ross Academic Center 2011–212	11/4/11	Laptop loan programs; attendance tracking	June 2012
Intercollegiate Athletics Complimentary Tickets 2011–110	11/16/11	Documented policy and procedure; monitoring and oversight; recording of complimentary tickets; complimentary parking and access passes; system access and use; compliance monitoring	March 2012
Plant Operations Information Management and Reporting 2011-102	12/22/11	Data management; reporting and analysis	Review progress June 2012. Follow-up December 2012
Office of the Provost	12/22/11	Information Systems Shared Services - recharge activity; Concur approvals	March 2012
UMHS Professional and Hospital Customer Service Charity Care Policy 2011–107–1	6/21/11	Policy reforms needed due to the Patient Protection and Affordable Care Act (PPACA)	March 2012
University of Michigan Comprehensive Cancer Center 2011-203	6/24/11	Travel and hosting; recharge activity; financial review; donor Access database	February 2012
UMHS Staff Licensure/Certification/ Registration Policy Review 2011–107–2	6/30/11	Documentation of required certifications; handling of credentialing time extensions; annual review and updating of licensure matrix	March 2012
UMHS Michigan Health Corporation 2011–109	6/30/11	Assess effectiveness of JV compliance programs; standardized management analysis and operational reporting; streamline consolidation accounting; update COI policy; documentation of board deliberative process	June 2012

Michigan Nanotechnology Institute for Medicine and Biological Sciences Fiscal Responsibilities 2012–218	11/22/11	Subcontract payments to NanoBio; conflict of interest disclosures; financial management; safeguarding of assets	June 2012
Medical School Department of Emergency Medicine 2011-204	12/5/2011	Internal Control Assessment certification; non-certified effort reporting; purchasing; P-Card transactions; gross pay register reconciliation; statement of activity reconciliation; delegation of authority	September 2012