May 31, 2013

Dr. Kirk A. Calhoun, President
The University of Texas Health Science Center at Tyler
11937 U. S. Hwy 271
Tyler, TX 75708

Dear Dr. Calhoun:

As part of our FY 2013 Audit Plan, we completed the Laptop Encryption and IT Inventory Audit. This audit was included in our Plan at the request of the UT System Audit Office.

The objectives of the audit were to determine whether:

- Laptop inventory at UTHSCT is complete, accurate, and up-to-date,
- All institutional laptops have been properly encrypted or exempted, and
- Processes and controls are adequate to properly record and track the institution's Information Technology inventory

In our opinion, laptop inventory at UTHSCT is complete for equipment meeting capital and controlled equipment dollar thresholds. Although the institution made adequate efforts to identify laptops costing less than $500, we cannot validate the completeness of these records since there is no tracking mechanism in place for these assets. Based upon procedures performed, we believe all laptops identified have been properly encrypted. UTHSCT has exempted no laptops from encryption requirements. Overall, we believe processes and controls over IT inventory are adequate to properly record and track the institution's IT inventory, except as noted in the report.

This audit was conducted in accordance with guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. We appreciate the assistance provided by management and other personnel and hope the information presented in our report is helpful.

Sincerely,

Kris I. Kavasch
Director of Internal Audit

Enclosure

cc:  Dr. Kenneth I. Shine, UT System Executive Vice Chancellor for Health Affairs r buckingham@utsystem.edu
Mr. J. Michael Peppers, UT System Chief Audit Executive systemaudito ffice@utsystem.edu
Mr. Richard St. Onge, UT System Associate Vice Chancellor for Shared Services richardstone@utsystem.edu
Mr. Vernon Moore, Vice President, Chief Business and Financial Officer vernon.moore@uthct.edu
Mr. John Yoder, Associate Vice President, Chief Information Officer john.yoder@uthct.edu
Ms. Donna Martin, Information Security Officer donna.martin@uthct.edu
Ms. Anne Heitke, UT System Audit Manager aheitke@utsystem.edu
Legislative Budget Board - ed.osner@lbb.state.tx.us
Governor - internalaudits@governor.state.tx.us
State Auditor’s Office - iacoordinator@sao.state.tx.us
Sunset Advisory Commission - sunset@sunrise.state.tx.us
## TABLE OF CONTENTS

**Executive Summary** ................................................................. 4

**Background** ........................................................................... 4

**Audit Objectives** ..................................................................... 5

**Audit Scope and Methodology** .................................................. 5

**Audit Results** .......................................................................... 5

**Conclusion** ............................................................................... 12

**Summary of Significant Findings** ................................................ 13
Audit Report

Executive Summary

This audit was completed as part of the FY 2013 Audit Plan in the area of Information Technology Audits. The audit was included in the Plan at the request of the UT System Audit Office and the purpose was to provide assurance as to the status of the encryption of University laptop computers, and personally owned computers used for University business. In addition, Audit was asked to provide assurance on the adequacy of processes and controls over the institution’s information technology inventory. The scope of our review was laptop encryption status and information technology controls and processes in effect in FY 2013 (September 1, 2012 through April 15, 2013).

We provide reasonable assurance that laptop inventory at UTHSCT is complete, accurate and up-to-date, except for laptops costing below $500 that are currently not adequately tracked. We believe all institutional laptops identified have been properly encrypted. Information Technology management allowed no exemptions to laptop encryption requirements. We believe processes and controls are adequate to properly record and track the institution’s information technology inventory, except for certain computer acquisitions, transfers, and disposals that are detailed in the report.

Background

On June 20, 2012 the UT System Executive Vice Chancellor for Health Affairs issued a memorandum to the Presidents of the UT System Health Institutions asking all campuses to encrypt 100% of the institution’s laptop computers (including any personally owned computers used to conduct University business). All laptops were to be encrypted by August 31, 2012. The UTHSCT Information Technology Department immediately began the process of identifying and encrypting all University laptops as required. The IT Department also performed work to identify any personally owned laptops used for institutional business. UTHSCT reported to UT System that 100% of University laptops were encrypted before August 31, 2012 as required. The UT System Audit Office requested for each institution’s Audit Office to perform an audit to provide assurance as to the encryption of laptops reported and processes and controls in place for recording and tracking the IT inventory.

On May 3, 2013, after fieldwork was complete for this audit, the UT System Executive Vice Chancellor for Health Affairs issued a memorandum to the Presidents of the UT System Health Institutions. This memo informed the institutions that as a result of faculty input the requirement to encrypt all personally owned computers that contained University data was reviewed and modified to focus specifically on the types of data that pose risk to the people served by UT System and its institutions. Additional guidance was provided that indicates that a personally owned computer must be encrypted when it contains:
• Information made confidential by federal or state law, regulation, or other legal agreement.
• Federal, state, university or privately sponsored research that requires confidentiality or is deemed sensitive by the funding entity.
• Any other information which has been deemed by the UT System or a UT System institution as essential to the mission or operations of System to the extent that its integrity and security should be maintained at all times.

As a result of the release of this updated guidance, we modified the first recommendation below prior to final report issuance to promote corresponding adaptation of changes to institutional policy as soon as possible.

Audit Objectives

The objectives of the audit were to determine whether:

• Laptop inventory at UTHSCT is complete, accurate, and up-to-date; and
• All institutional laptops have been properly encrypted or exempted.
• Processes and controls are adequate to properly record and track the institution's Information Technology inventory.

Audit Scope and Methodology

The scope for determining laptop encryption was all institutional laptop computers (including personal computers that faculty or staff used to conduct any UTHSCT business) and the scope for determining the adequacy of controls over IT inventory was all computer related assets. The scope of our review was FY 2013 (September 1, 2012 through April 15, 2013).

We conducted our audit in accordance with guidelines set forth in The Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing.

Audit Results

Laptop Inventory and Encryption

We began by determining the adequacy of the process used by the IT Department during FY 2012 in identifying laptops. We found that although it was a highly manual process we believe it to be an acceptable approach to fulfill the charge since electronic configuration tools were not installed at a level to completely identify these assets. The UTHSCT Chief Information Officer asserts that the institution maintains one official record of laptop inventory which is from the PeopleSoft Asset Management system that is maintained by the Accounting Department. The institution historically has not maintained a separate inventory of laptop computers and these were not specifically categorized separately from other computer equipment in the PeopleSoft
The University of Texas Health Science Center at Tyler
Laptop Encryption and IT Inventory Audit
FY 2013

system so identifying these assets was a significant undertaking for the Information Technology Department.

Although the institution has purchased vCenter Configuration Manager (VCM - formerly Configuresoft) that has the capability of identifying laptops with batteries when they are on the network, due to technical problems experienced during installation this software has not been installed on all laptops owned by the institution. The Health Science Center has worked with the vendor as recently as December 2012 to resolve the issues and has been rolling out the tool in a controlled manner as recommended. Laptop identification for the encryption effort was a highly manual and labor intensive process where IT staff pulled data from a variety of sources including PeopleSoft Asset Management, McAfee Electronic Policy Orchestrator (EPO), System Center Configuration Manager (SCCM - formerly SMS), and the Information Technology Department’s manually maintained encryption reports. Staff assignments were made and staff members physically inspected and verified encryption software was installed and running properly on a number of laptops. The encryption project was completed by July 26, 2012 which was within the August 31, 2012 deadline prescribed by UT System. The Chief Information Officer reported at that time there were 609 University laptops and that 100% of these were encrypted. At July 26, 2012, no employees were reported to be using personally owned computers for University business.

When comparing the institution’s Information Technology encryption and security policies with the UT System mandates for encrypting University laptop computers, and personally owned computers used for University business, we found existing policies in effect do not fully encompass all details of the updated UT System encryption requirements just released on May 3, 2013. Current institutional Information Technology Security, Encryption Guidelines and Information Resources Acceptable Use policies require the encryption of all University owned laptops and personally owned laptops used for University business when they contain confidential data; however, these policies do not fully detail the recently updated mandates from UT System for encryption of personally owned laptops.

**Recommendation #1:** The Associate Vice President, Chief Information Officer and Information Security Officer should ensure the institution's Information Technology Security, Encryption Guidelines and Information Resources Acceptable Use policies are updated to incorporate the mandate from UT System to encrypt all personally owned computers if they contain any of the following types of University information:

- Information made confidential by federal or state law, regulation, or other legal agreement.
- Federal, state, university, or privately sponsored research that requires confidentiality or is deemed sensitive by the funding entity.
- Any other information which has been deemed by the UT System or a UT System Institution as essential to the mission or operations of System to the extent that its integrity and security should be maintained at all times.
The University of Texas Health Science Center at Tyler
Laptop Encryption and IT Inventory Audit
FY 2013

Management's Response: The Chief Information Officer and Information Security Officer will update IHOP Policy 2.16 Encryption Guidelines to include encryption requirements set forth in the UT System Executive Vice Chancellor for Health Affairs memorandums dated June 20, 2012 and May 3, 2013. The Information Technology Security and Information Resources Acceptable Use policies were reviewed and deemed to be consistent with the revised Encryption Guidelines requirements without revision, since these policies are designed to support the more detailed Encryption Guidelines policy where the newly issued UTS encryption provisions will be listed.


We performed procedures to independently assess the completeness of the laptop inventory records and found the official laptop inventory record provided by the Accounting Department as of February 18, 2013 was not complete. The official record noted 562 laptops but the number reported should have been 591. We compared the February 18, 2013 official laptop inventory record to the July 26, 2012 inventory record provided by the Information Technology Department to the Information Security Office to support the assertion that 100% of University laptops were encrypted by August 31, 2012. We also compared the February 2013 laptop inventory record to purchase order documents and equipment deletion records. Audit identified twenty-nine more laptops for addition to the official record provided. The most notable cause for the differences is that there is no tracking system in place for laptops and other computer equipment that cost less than $500. Currently, the only computer equipment being tracked by the institution is controlled equipment costing between $500 - $4,999.99 and capital equipment costing $5,000 and above. We believe for laptops that meet controlled and capital asset threshold the institution’s inventory is complete, accurate and up-to-date. However, the inventory records do not include computer equipment that costs less than $500. From a financial perspective the laptops costing less than $500 may not be significant but from a security standpoint they pose the same or similar risks to the institution as some higher dollar equipment. It is important to note that Audit tested a sample of these assets costing below $500 and found they were encrypted; however, they were difficult to locate and we are not certain that we identified 100% of this equipment owned by UTHSCT.

We tested a sample of 40 laptops from a cross-sectional representation of the institution and all were found to be properly encrypted. Although one laptop awaiting donation could not be located, adequate documentation existed to support that encryption software was installed. Based upon the results of procedures performed and this testing, we are reasonably assured that all institutional laptops have been properly encrypted. Due to the manual process for identifying laptops and processes in place that do not require tracking of expensed computer equipment costing less than $500 Audit is reasonably assured but not absolutely assured that 100% of University laptops were identified.

IT Inventory Processes and Controls

We reviewed processes and controls for recording and tracking the institution’s Information Technology inventory focusing on acquisitions, record maintenance and disposals and we found
processes and controls to be adequate to properly record and track this inventory, except as noted below:

**Acquisitions**

Most computer equipment purchases are centrally processed by the Senior Client Services Analyst, who functions as a satellite buyer in the Information Technology Department. The computer equipment purchase must be authorized by the department head, administrator (when applicable) and the Chief Information Officer. The Senior Client Services Analyst is responsible for ensuring that controlled and capital equipment is properly tagged and reported to Accounting for inclusion in the institution's official asset records. When configuring newly purchased computer equipment the IT staff member who sets up the computer must request a property number from Accounting because it is required data for input into the system during configuration. This is important in the process because it helps to ensure the property is tagged and added to the PeopleSoft Asset Management (PSAM) system. Although we believe controls to be in place to ensure the property is appropriately tagged and tracked for controlled and capital assets purchased within this process, we believe controls need to be improved over the following computer equipment purchases:

- In some instances, Purchasing Department buyers are ordering computer equipment when they receive departmental requisitions for the equipment. These computer equipment purchases may by-pass the review and approval of the Chief Information Officer who determines whether the equipment will function within the institution's IT environment and whether the IT Department can provide adequate support for the equipment. These purchases may also by-pass the IT Senior Client Services Analyst who has processes in place for ensuring new computer equipment purchases are properly tagged and recorded in the official inventory record. The Purchasing Department has no communication processes in place for ensuring the property is properly tagged and added to the inventory records but is relying upon departments to do so, which increases the risk that the asset will not be properly documented and tracked.

- Although not a common practice, upon occasion UTHSCT has reimbursed an employee who personally selected and purchased business computer equipment outside the normal institutional purchasing process. These employees are reimbursed within the Direct Payment Request process and currently there is no process in place to ensure this equipment meets the institution's specifications. Also, there is no process in place to ensure the equipment is properly tagged and added to asset records for tracking.

- Computer equipment that is not tracked because it costs less than the $500 controlled equipment threshold for tagging and tracking poses a risk to the institution. Most of these assets can store confidential data at some level and are at high risk for loss due to portability and lack of an adequate tracking mechanism.

- Although not common, some computer equipment has been delivered directly to the Research Enterprise, by-passing the Information Technology Department process which is designed to help assure the asset is properly tagged, recorded in the records and distributed.
Recommendation #2: The Vice President, Chief Business and Financial Officer in collaboration with the Associate Vice President, Chief Information Officer should:

- Establish policies and procedures which ensure that all computer equipment purchases must be submitted to the Information Technology Department for approval prior to order processing.
- Prescribe policies, procedures and responsibilities for ensuring computer assets are properly tagged and added to the PeopleSoft Asset Management system when computer inventory purchases are made by employees using their personal funds and they subsequently seek reimbursement from the institution for these purchases.
- Establish an inventory tracking system for computer equipment such as notebooks, tablets, removable hard drives and other portable devices that cost less than the controlled equipment threshold of $500 to ensure adequate security and control of these assets. The UTHSCT Chief Information Officer should consult with the UT System Chief Information Officer and Chief Information Security Officer for UT System's directives for this equipment.
- Establish procedures to ensure that all new computer inventory is processed through the Information Technology Department for distribution to ensure these assets are properly tagged and recorded in the official asset record or alternately develop procedures in distributed receiving areas for ensuring the assets are properly tagged and recorded.

Management’s Response: The Information Technology Department will work directly with the Purchasing Department and Accounts Payable to ensure policies and procedures are in place to require that all IT related purchases are, at a minimum, reviewed by the CIO or an IT designee for standards compliance and compatibility prior to purchase or reimbursement. The IT department will be responsible for tagging computer related equipment and making sure policies for hardening, encryption, etc… are followed. The Information Technology Department will contact UT System for guidance in best practices for tracking IT equipment costing less than $500 and will work with the Accounting Department to develop an appropriate tracking system for these assets. The IT Department will ensure processes are deployed for ensuring all computer-related equipment is ordered, received by and dispensed to departments through the IT Department to ensure proper tagging and tracking of these assets.


Tracking System for Assets Costing Less Than $500 – Identify a Solution - October 31, 2013; Implement by April 30, 2014

New Computer Equipment Purchases - September 30, 2013
Computer Inventory Records Maintenance

The institution annually requires all areas to perform a count of their controlled and capital equipment. The Accounting Department updates inventory records based upon this count. In addition, when assets transfer between departments IT staff who take care of the transfer immediately initiate an electronic transfer form that routes to departmental management for authorizations and then the form automatically routes to the Chief Information Officer for approval. The process ends with the system routing an electronic notice of the change to the Senior Accountant in the Accounting Department who manages the asset module. The asset record is updated according to the electronic form. Although we believe this process has greatly improved over time, during the course of our work we identified the following administrative issues concerning processes for maintaining and updating the official computer inventory records in the PeopleSoft Asset Management system:

- For the most part, when new computer assets are transferred from Information Technology to the departments IT Computer Transfer forms are being completed and electronically sent to the Accounting Department for update of the inventory records. However, we found one instance where the transfer form was not completed and sent to Accounting for update of the records. Currently there is no reconciliation performed between IT records of computer equipment issued and PSAM computer inventory records to ensure PSAM records are properly updated as computer equipment is issued from IT to departments.
- Departments are not consistently ensuring the institution's inventory records are updated when an employee leaves the institution and computers are reassigned within the department. This sometimes makes it difficult to identify who has custody of the asset.
- Removal of Equipment from Campus forms are not consistently completed for laptops and other computer equipment taken off-campus which also makes it difficult to locate the asset.

**Recommendation #3:** The Vice President, Chief Business and Financial Officer in collaboration with the Associate Vice President, Chief Information Officer need to consider implementing process improvements to ensure the PeopleSoft Asset Management official computer inventory records are updated timely. Internal Audit’s suggestions for improving processes are as follows:

- Since the institution’s official IT Department inventory record includes newly acquired computer equipment that transfers to other departments, surplus equipment for re-issue or disposal, and computers assigned to IT Staff it is important for the IT Department to thoroughly review the PeopleSoft Asset Management computer inventory report at least quarterly to verify that all required transfer and deletion forms were submitted to the Accounting Department for computer equipment transferred to and from the IT Department’s custody. The Chief Information Officer needs to assign responsibility for this quarterly review and records update. As part of the quarterly review process, transfer
forms should be completed and submitted to the Accounting Department for any deficiencies identified.

- Since UTHSCT considers the PSAM computer inventory record maintained by the Accounting Department to be the official institutional record and the institution needs to know where property is at all times it is important for management to implement processes for ensuring records are updated when the property transfers between employees.

- Management needs to ensure “Removal from Campus” forms are completed for any computer equipment removed from campus or alternately consider whether exceptions are appropriate for portable devices such as laptops, tablets and other portable devices. If exceptions are allowed, these need to be properly documented in policy and custodians need to be properly identified for accountability.

Management’s Response: The Chief Information Officer will assign responsibility and processes for quarterly review of the Information Technology Department’s PSAM computer equipment inventory report to verify all required computer inventory transfer forms needed as a result of computer inventory transferred to and from the IT Department were prepared and provided to the Accounting Department as required.

To help ensure that the institution’s records are kept updated so the institution can locate computer equipment at all times, during the FY 2013 annual equipment inventory count process the Property Management Accountant will provide departmental management with directives and instructions for making regular updates to the records when asset custodians are reassigned within the department.

The IT Department will work with Asset Management to discontinue requiring “Removal from Campus” forms for all portable computing devices. The Property Management Accountant will ensure that applicable policies and forms will be updated appropriately to support the requirements. The Chief Information Officer in collaboration with the Information Security Officer will update IHOP Policy 2.04 – Acceptable Use to include a statement identifying the custodian’s responsibilities for maintaining and returning portable devices.


Surplus Computer Equipment

Surplus computer inventory is reassigned, used for parts or donated. Prior to reassignment the hard drives are wiped and prior to donating computer equipment the hard drives are removed and put thorough a degausser. A degausser is a device that generates a magnetic field for degaussing magnetic storage media. For certain forms of computer data storage such as hard drives and some tape backup drives, degaussing renders the magnetic media completely unusable and damages the storage system. Although IT has implemented processes for handling surplus
equipment there are no written institution-wide procedures for guidance in surplus computer equipment security, disposal method processes and required documentation. We found processes deployed vary between the Information Technology and Research areas that handle this equipment. The Information Technology Department has a secure location for storing computer assets that are awaiting disposal while the Research area does not. Also, the IT Department has a method in place for documenting the eradication of data from the equipment in a manner where this information can be retrieved should the asset be lost or stolen, but the Research Enterprise does not. When testing, we identified one laptop that was missing which was assigned to Research and reportedly being held in Research for future donation by the IT Department. Although the responsible employee indicates the hard drive had been wiped, and we were able to prove encryption software had been installed on the laptop the asset was being held in an insecure location and documentation was inadequate for Audit to verify whether data was actually removed before the asset went missing. The missing asset was reported to the Information Security Officer, Chief Information Officer and Senior Accountant who manages the inventory records.

**Recommendation #4:** The Associate Vice President, Chief Information Officer should prescribe institution-wide policies and procedures for the security, disposal and documentation required for surplus computer equipment.

**Management’s Response:** The Chief Information Officer will prescribe institution-wide policies and procedures for surplus computer equipment security, disposal and documentation requirements by updating IHOP 2.02 Computer Inventory Management and IT Departmental Procedure “Eradication of Data Stored on Electronic Media and Disposal of PCs”.

**Implementation Date:** Draft Policies – July 31, 2013; Final Approved Policies - August 31, 2013.

**Conclusion**

In our opinion, laptop inventory at UTHSCT is complete for equipment meeting capital and controlled equipment dollar thresholds. However, for laptops costing below $500 that are not tracked by UTHSCT, we cannot be certain whether all of these laptops were identified. We found the institution has exempted no laptops from encryption requirements. Based on work performed, we believe all laptops identified have been properly encrypted. We believe processes and controls over IT inventory are adequate to properly record and track the institution’s IT inventory, except as noted above.

Kris I. Kavasch, Director of Internal Audit
Summary of Significant Findings

According to The University of Texas System, a significant finding is one that may be material to the operation, financial reporting, or legal compliance of the university if corrective action has not been fully implemented. This would include an internal control weakness that does not reduce the risk of irregularity, illegal act, error, inefficiency, waste, ineffectiveness, or conflict of interest to a reasonably low level.

In view of the above requirements, the Laptop Encryption and IT Inventory Audit for FY 2013 had no significant findings.