# RIVERSIDE: AUDIT & ADVISORY SERVICES

August 23, 2018

To: Ethics & Compliance Risk and Audit Controls (ECRAC) Committee

Subject: Financial Analytical Review – Low Value/Theft Sensitive (LV/TS) Computing Equipment

Ref: R2017-11C

We have completed our Financial Analytical Review – LV/TS Computing Equipment audit in accordance with the University of California, Riverside Internal Audit Plan. Our report is attached for your review. We will perform follow-up procedures in the future to review the status of management action. This follow-up may take the form of a discussion or perhaps a limited review. R2017-11C will remain open until we have evaluated the actions taken.

Should you have any questions concerning the report, please do not hesitate to contact us.

 Gregory Moore

 Director

UNIVERSITY OF CALIFORNIA AT RIVERSIDE

AUDIT & ADVISORY SERVICES

MEMBER OF ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

REPORT R2017-11C

FINANCIAL ANALYTICAL REVIEW – LOW VALUE/THEFT SENSITIVE COMPUTING EQUIPMENT

AUGUST 2018

Approved by:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Laura Bishin Toffee Jeturian

Principal Auditor Assistant Director

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 Gregory Moore

 Director

**UC RIVERSIDE**

**FINANCIAL ANALYTICAL REVIEW-**

**LOW VALUE/THEFT SENSITIVE COMPUTING EQUIPMENT**

**REPORT R2017-11C**

**AUGUST 2018**

**I. MANAGEMENT SUMMARY**

Based upon the results of work performed within the scope of the review, we noted that internal controls over Low Value/Theft Sensitive (LV/TS) computer equipment and its compliance with applicable University of California (UC) policies need to be strengthened to effectively manage these assets, as well as to enhance efficiency and effectiveness of operations.

See Observation III –Campus-wide internal controls and policy compliance over LV/TS Items.

Minor items not of the magnitude to warrant inclusion in this report were discussed verbally with management.

**II. INTRODUCTION**

 **A. PURPOSE**

University of California, Riverside (UCR) Audit & Advisory Services (A&AS), as part of its Audit Plan, performed analytic review procedures to evaluate the campus-wide internal controls and policy compliance over LV/TS computer equipment (i.e. laptops, etc.). We will refer to these items as ‘Non-Capitalized (Non-Cap) Computer Equipment’. The analytical review included procedures to compare and evaluate relationships among data on a campus-wide basis in order to identify unexpected fluctuations, trends, discrepancies or activities, the absence of expected fluctuations, trends or activities, and other unusual items. Additionally, we also reviewed how UCR monitors LV/TS items like laptops and other computers to determine whether there are appropriate controls and systems to effectively manage these assets.

**B. BACKGROUND**

Prior to June 2017, UCR utilized a legacy green screen end-of-life mainframe system called Equipment Management System (subledger) to track capitalized and some non-capitalized assets. One of the issues with the system was the absence of end-user reporting. Moreover, because of lack of integration with our existing PeopleSoft Financial system (UCRFS), items were recorded into this system manually. Completeness checks (to ensure all items are entered) were manual and decentralized.  We noted errors wherein items were not recorded in the subledger, which may have created opportunities to conceal misappropriation of University assets.

An in-house developed asset management replacement system was implemented in June 2017. While it does not currently offer integrated functionality with PeopleSoft, it does offer better end-user reporting.

However, in both the old and new systems, there is no ability to track nor is there a campus-wide system to track LV/TS items such as laptops, powered hand tools, theatre props, Arts Block art, vehicles, etc.

UC Policy BUS-29 Management and Control of University Equipment states that ‘University locations may establish guidelines governing the control over theft-sensitive items valued at less than $5,000.’

Historically, we have noted many departments recording LV/TS items in tools like Excel spreadsheets, while some departments do not use any monitoring tools. The accuracy and controls over such tools (i.e. Excel spreadsheets) are questionable and there is no higher level reporting capability.  For example, we would not easily be able to report all low value vehicles or computer equipment at UCR.

Some computer equipment may contain Personal Health Information (PHI) (e.g. at School of Medicine) or Personal Protected Information (PPI) and would be subject to Health Insurance Portability and Accountability Act (HIPAA) or Senate Bill 1386 (SB 1386). SANS[[1]](#footnote-2) 20 Critical Controls: Control #1 states that a company should maintain an inventory of authorized and unauthorized devices. Without such information, it is difficult to evaluate security and insurance requirements, comply with some sponsor or agency reporting requirements, or determine losses.  Business & Financial Services indicated that as the campus considers plans to upgrade the financial system, implementation of an integrated Asset Management module (which meets more than just external capital asset financial reporting requirements) should be included in the project plan.

**C. SCOPE**

This review analyzed selected data for four Fiscal Years (FY) ended 2015-2016 from the following General Ledger (GL) accounts:

* 720200 - Equip, Non-Inv/Comp $200-1499
* 720205 - Equip Non-Inv/Comp $1500-4999

These expenditures generally represent computer equipment (laptops, desktops, tablets, monitors, etc.) that individually costs less than $5,000 per item.

Test work was performed from July to September of 2016. However, more recent developments were incorporated into this report as we became aware of them.

We designed the methodology to provide sufficient, competent, and relevant evidence to achieve the objectives of the review. Due to factors beyond our control, it is possible that not all Non-Cap Computer Equipment expenditures were reviewed. Furthermore, because of the nature of this review’s global perspective and other limitations, the review procedures could not ensure that errors and irregularities were detected, especially minor or isolated incidents.

The review included, but was not limited to the following areas:

* + 1. Compliance with policies and regulations
		2. Payment/reimbursement methods for purchasing Non-Cap computer equipment
		3. Inventory management practices, systems, and controls
		4. Physical inspection of sample selection
		5. Other implications of asset management practices.

**III. OBSERVATIONS, COMMENTS AND MANAGEMENT CORRECTIVE ACTION**

**Campus-wide Internal Controls and Policy Compliance Over LV/TS Items**

Internal controls over Low Value/Theft Sensitive (LV/TS) computer equipment and its compliance with applicable University of California (UC) policies need to be strengthened to effectively manage these assets, as well as to enhance efficiency and effectiveness of operations.

While the scope of the audit was to review controls over Non-Cap computer equipment, it is deemed that inadequate internal controls apply to other LV/TS assets (cell phones, vehicles, etc.).

**COMMENTS**

Following are the Non-Cap computer equipment LV/TS expenditures by Unit for four years ended FY 2015-16:



While the increases above are not unexpected (the UCR 2020 Strategic Plan calls for increasing ladder rank faculty hires by 300, growing student population, etc.), we note a number of internal control weaknesses over these equipment items as explained below.

**Policy BUS29 -** OTHER INVENTORIAL ITEMS “Items purchased for less than $5,000 or that have an expected normal life of one year or less, which are not inventoried as equipment or Government property, but which are nevertheless subject to safeguards provided by the inventorial process. This category includes theft sensitive items and items specifically identified for inclusion as inventorial items by the sponsor of an extramural award. Such items are expensed (vs. capitalized), subject to local University location inventory control procedures, and need not be reported in the Equipment, Infrastructure and Assets (EFAX) database.”

Section III.A.1.c.iii. of the policy states: “University locations may establish guidelines governing the control of theft- sensitive items valued at less than $5,000. These items should be expensed; not capitalized. Examples of theft-sensitive items include, but are not limited to:

a) Computers and communication devices, including desktop, laptop, tablet and smart phones,

b) Cameras and projectors, stereo and video components,

c) Binoculars, telescopes, periscopes, microscopes and microscope assemblies, optical elements and assemblies,

d) Recorders and playback units, audio or video,

e) Wheeled stretchers,

f) Powered hand tools.”

**Types of Expenditures –**

**Vendors without Contracts** - We performed an analysis of Non-Cap Computer Equipment expenditures in Accounts Payable (AP) by vendor (excluding employee reimbursements) and tested some large expenditures to determine if we had a Systemwide (SW) or UCR vendor contract. Following were the expenditures with no SW or UCR contract.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| FY | 2012-13 | 2013-14 | 2014-15 | 2015-16 | Grand Total |
| Non Contract Expenditures | $260,537 | $277,054  | $705,585  | $1,061,893  |  $2,305,069  |
| % of Total AP Expenditures | 13% | 13% | 21% | 22% | 19% |

We inquired about some of the large vendor expenditures (i.e. one vendor had $534K in expenditures over 4 years). Central purchasing indicated that there were bids, multiple quotes, or some of the smallest expenditures were Low Value Purchase Authorization (LVPA) items and that the purchases were in accordance with policy.

**Vendors without Purchase Orders (PO)** – We performed an analysis of Non-Cap Computer Equipment expenditures that were made without a PO (excluding employee reimbursements). The ‘non-PO’ expenditures appear to be mostly credits (i.e. returned items) on items that were originally purchased on POs. A best practice would be to attribute credits to the corresponding PO. The non-PO expenditures, exclusive of credits, totaled $15K in four years. Some of those items also pertain to POs. One appeared to be a 40% price adjustment, and one was a chargeback on a return[[2]](#footnote-3). In those cases, it would be a best practice to reference the original PO.

**Reimbursements** – We noted $166K in reimbursements (i.e. where faculty or staff buy direct from vendors like Best Buy and get reimbursed via ePay[[3]](#footnote-4)) across four FYs ended FY16. Departments with the highest expenditures in this category (over $10K in any of the four FYs ended FY16) were:



**Purchasing Card (PCard) Purchases** – We note that the PCard purchases in Non-Cap Computer Equipment were as follows:



This is another area where purchases could be made off-contract and increase risk.

**Inventory and Inspection of Non-Cap Computer Equipment** – A&AS initially planned to select some purchased Non-Cap Computer Equipment and verify the physical existence of the items selected. We selected items on 44 Accounts Payable (AP) vouchers across 22 departments. We queried AP and eBuy[[4]](#footnote-5) systems to obtain information about the purchases (i.e. quantity, description, price, transactor, approver, and department). We noted that some purchases were charged to Federal Contract & Grant (C&G) funds.

Since there is no campus asset management system that tracks LV/TS items, A&AS contacted various departments to obtain inventory listings that would indicate the description of the equipment, serial number (SN), custodian, location, etc.

In many cases, the departments were unable to provide a listing of the LV/TS items. We noted that some departments are in units that have an IT resource and in some cases their IT personnel were able to provide computer listings from systems like Sophos, Spiceworks, Microsoft SCCM, Faronics Deep Freeze, etc. We note a number of distributed IT functions on campus using different systems to track assets, with no common system. Several departments that provided listings (not from unit IT) were maintaining listings in tools like Excel or Sharepoint. We noted difficulty in maintaining a proper segregation of duties and ensuring accuracy of items tracked in Excel and such systems. There were a couple of departments that had purchased third-party asset management solutions (like WASP or BNA), but they are not integrated with the purchasing system so they are difficult to maintain. One of these two departments reported abandoning the asset management system it purchased for that reason. In the instances where we obtained asset listings (even ones produced by IT), we could not locate some of the items because they did not have complete information (i.e. SN) or because the item was not on the listing. In those cases, we were unable to determine the location, existence, or potential disposition of the asset.

In audit R2017-05 CNAS Dean’s Office Audit, we noted one department created their computer inventory only in response to the audit. A&AS noted that the department had omitted a half dozen laptops from the listing; the department did not know about existence of these laptops, but they were found during A&AS’ physical inspection. Unrecorded assets are at greater risk of misappropriation. From a sample selection of 20 items from the GL, A&AS was unable to locate seven items (35%) initially due to poor record keeping and errors. One laptop, which was purchased with Federal C&G funds could not be located. Another half dozen laptops had been sitting for reportedly many months waiting for a non-IT employee to scrub the data so they could be sent to equipment surplus[[5]](#footnote-6). These are unreported and underutilized assets which could have been redeployed to other departments or even underserved students.

One department noted that not having an inventory makes it difficult to off-board employees. Some departments simply ask faculty and staff to self-report the computer equipment they have to turn in, but they have no effective way to verify if the equipment was returned. Some departments search through POs to try to determine what equipment might exist and the location, which is inefficient and ineffective. Inadequate inventory controls make it difficult to locate assets purchased on C&G funds.

One department reported that they do not have instructions or guidelines to track LV/TS computer items for their department. This department has 40 labs and millions of dollars invested in these items. One researcher in the department has over 20 iPads.

**Compliance –** Inadequate inventory controls also make it difficult to comply with SB-1386[[6]](#footnote-7) requirements. Some computers may contain Family and Educational Rights and Privacy Act (FERPA), PHI, PPI or sensitive data. Laptops can also be subject to export controls.

**Redeployment of Underutilized Assets** – The campus does not have a way to identify underutilized assets to redeploy them.

**Purchasing Assets that cannot Be Used (nor Returned)** - One unit reported a purchase of 40 Microsoft Surface pro tablets (approximately $2k each) without consulting IT staff. These tablets had the Windows 10 operating system (which was not supported at the time) so they were unused. We noted several other instances of this mentioned in this report.

**Purchasing without IT staff input** - Some departments do not have a unit IT function involved with IT related purchases; or if they do, consultation with the IT staff when making purchases was not always done. We noted instances when computing equipment was purchased then determined to be incompatible with our systems, but could no longer be returned. In some cases, items can no longer be returned because if they are under LVPA, the department would not necessarily involve purchasing or use contracted vendors that offer a better return policy.

**IT Risks** - Some departments leave it up to the individuals to make sure their devices meet minimum network standards for connectivity. However, distributing responsibility for keeping laptops and devices patched with proper security updates and virus/malware scanning increases risk. Verifying that assets were properly wiped and disposed of also become difficult. Other risks associated with distributed IT are discussed in Appendix A.

**Off Campus Use** – There is a form ‘Authorization to use University Property in an Off-Campus Location’ that some departments fill out for LV/TS assets for off campus use. However, many users do not use the form and some departments were unaware of such forms. Accounting Services stated that the form is required to be completed and submitted to Equipment Management only for Inventorial Equipment and Other Government Property as per UCR Policy 750-99. For non-inventorial assets, Accounting Services requests that departments complete it for their records.

**Other LV/TH Items and Implications** – Other units have to track tools, student programming items like Xbox, vehicles under $5K, etc. Tracking assets, regardless of the type of asset is generally the same process. To the extent possible, assets should be tracked in a single asset management system where they are initiated with a PO and monitored until its retirement or disposition. This improves reporting (i.e. regulatory), planning (i.e. replacements), and ability to redeploy underutilized assets. This decentralized and inconsistent approach to laptops and computers is not limited to just these assets. This is generally the way other Non-Cap assets are handled on campus (i.e. supplies inventory, tools, vehicles, phones, etc.). Instead of using an Enterprise Resource Planning (ERP) system to handle various assets, the departments determine and devise ways to track their respective assets. We have built and purchased a myriad of asset management systems for different kinds of assets, but lack a single integrated asset management system that can offer asset management solutions for many types of assets. The legacy and currently implemented in-house asset management system was devised as a specific solution to an accounting requirement to track assets over $5K. It is meant to meet financial reporting requirements and does not take into account the need to track assets less than $5K for compliance and management purposes. While this audit was focused on laptops and computers, it also applies to other assets on campus. This is an opportunity to consolidate many systems, provide integration, and reporting to properly account for assets across the campus. This will hopefully help in planning; enable the redeployment of underutilized resources; enhance accountability, efficiency, effectiveness; and reduce loss and risk.

**Recommendations**

The campus should create a sound local policy on LV/TS assets, require tracking of certain assets like computers, laptops, etc. and that IT equipment be vetted with IT staff prior to purchase (or purchases can be from a list of approved devices). The campus should also consider implementing an integrated Asset Management solution (like PeopleSoft Asset Management Module) that will work for many diverse constituents.

**Management Response/Corrective Action – Business Financial Services -** The functionality noted above will be evaluated with the implementation of a new financial system.

**Appendix A**

While administrative units have centralized and rationalized IT, the academic units provide IT resources on a decentralized basis (including staff, hardware and software). For academic units, some functions are outsourced to Information Technology Services (ITS) or third parties. However, certain functions remain at the unit including provisioning access to file, mail and other unit or department specific servers, virus scanning, etc. Purchase of hardware and software is managed by each academic unit. Each unit has a different software/systems for virus protection, patch application, incident monitoring/help desk ticketing/bug tracking, data sanitization, physical security, backup, logging and review, and to inventory hardware and software. It is not surprising in this environment that some units could not provide a listing of hardware and software. This implies that management does not have a sound understanding of IT assets under their purview. Units have varied local policies and procedures. For example, some units tightly control administrator rights preventing users from installing software, others provide administrator rights and assume the risk. The departments in some academic units are largely left to administer IT controls autonomously. Some units lack unified control of desktop and other devices. Some units have formal UCR Information Security Plans in place, others are developing a formal plan or have addressed components of the plan informally.

The 2013 annual inventory coordinated by ITS of Personal Protected Information (in response to Senate Bill 1386), but largely performed by the unit IT functions, indicated several departments with unencrypted PPI, some data custodians were not familiar with University of California Office of the President Information Security (IS)-3 escalation policy. Some end-of-life operating systems were discovered, which may introduce vulnerabilities. While these are not policy violations, it increases risk which could be mitigated via a unified PPI risk management strategy. While ITS responded in part with automating the self-reporting of PPI, we note that without a comprehensive inventory of devices, we cannot begin to determine the completeness or accuracy of reporting.

1. SANS is the most trusted and by far the largest source for information security training and security certification in the world. It also develops, maintains, and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet's early warning system - the Internet Storm Center. [↑](#footnote-ref-2)
2. The note on the return was that the item was not compatible with our equipment. [↑](#footnote-ref-3)
3. UCR’s in-house developed online payment request application. [↑](#footnote-ref-4)
4. UCR’s in-house developed front end PO system, which interfaces to PeopleSoft’s PO module. [↑](#footnote-ref-5)
5. This is an inefficient process because in some cases we are relying on non-IT employees to wipe computers, when ideally they could all be wiped centrally (i.e. Equipment Surplus, central IT, certified vendor). [↑](#footnote-ref-6)
6. A bill passed by the California legislature regulating the privacy of personal information. [↑](#footnote-ref-7)