INTERNAL AUDIT
IAS
ADVISORY SERVICES

Internal Audit Report

WORKSTATION SECURITY

Report No. SC-10-07

August 2010

UC SANTA CRUZ

August 18, 2010

MARY DOYLE
Vice Chancellor

Re: Internal Audit Report No. SC-10-07 – Workstation Security

Dear Mary:

UCSC Internal Audit and Advisory Services (IAS) has completed an internal audit of Workstation Security. A copy of the report is attached. The audit was conducted to determine if processes are adequate and result in properly configured and secure computer workstations.

In general, the adequacy of existing campus processes for ensuring that workstations are properly configured and secured varied. Some campus units provided support for their own workstations and other units were administered by Information Technology Services (ITS). In either case, our testing confirmed that a relatively large percentage of campus computer workstations contained one or more security vulnerabilities. In addition, the campus did not maintain an inventory of campus computer workstations.

ITS has identified a remote solution for addressing existing vulnerabilities and for building an inventory of campus computer workstations through the acquisition and rollout of the BigFix Enterprise Suite (BigFix) and Sophos Enterprise Console project.

Campus management has been responsive in addressing report observations and management corrective actions. Agreements were reached on all of the report's recommendations. Normal follow-up will be performed to verify completion of agreements during the next quarter.

We would like to express our appreciation to ITS, ITS Support Center Services, Student Health Center, Ticket Office, University Police, Transportation and Parking Services, Educational Partnership Center, and the School of Engineering for their cooperation and assistance throughout this engagement.

Sincerely,

Barry Long, Director
Internal Audit & Advisory Services

Attachment

Distribution:

Principal Auditor Lane
Vice Chancellor McGinty
Divisional Liaison McMillian
Manager Melgares
Director Roeth
Associate Vice Chancellor Whittingham

UCSC Audit Committee:

Executive Director Beaston
Vice Chancellor Delaney
Vice Chancellor Doyle
Assistant Vice Chancellor Lew
Vice Chancellor Margon
Assistant Vice Chancellor Moreno
Vice Chancellor Murphy
Assistant Chancellor Sahni
UCOP SVP Vacca
Vice Chancellor Vani

INTERNAL AUDIT
IAS
ADVISORY SERVICES

WORKSTATION SECURITY

Report No. SC-10-07

August 2010

David Lane
Principal Auditor,
Assistant Director

Approved:

Barry Long, Director
Internal Audit & Advisory Services

UC SANTA CRUZ

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Internal Audit and Advisory Services (IAS) has reviewed campus administration over workstation security to determine if processes are adequate and result in properly configured and secure computer workstations.

In general, the adequacy of existing campus processes in ensuring that workstations are properly configured and secured varied as some campus units provided support for their own workstations and other units were administered by Information Technology Services (ITS). In either case, our testing confirmed that a relatively large percentage of campus computer workstations contained one or more security vulnerabilities. In addition, since no inventory of campus workstations exists, the number of workstations to be managed is not fully known.

ITS has developed processes to provide more standardized and updated software for new workstations placed in service. However, legacy workstations built before the current procedures were developed may not be well configured and supported. In addition, ITS has made efforts to standardize support through the Support Center and the IT Request Ticket system, but support often relies on a non-ITS staff identifying the need and requesting support. We found some opportunity to improve the methodology and checklists used to re-image workstations.

The use of some type of remote management tool appears to hold the most potential for addressing existing vulnerabilies and providing a way of inventorying workstations at a campus level, given decreasing numbers of support staff due to budget cuts. ITS is presently rolling out the BigFix Enterprise Suite (BigFix) and Sophos Enterprise Console project, which appears to be capable of addressing most of the security problems identified.

Our observations and related management corrective actions are described in greater detail in section III of this report.

II. INTRODUCTION

A. Purpose

To determine if campus administration over computing processes result in properly configured and secure workstations.

B. Background

In 2007, Information Technology Services (ITS) completed a Transformation Program to consolidate as many IT staff, servers, and functions as possible. One stated goal of the transformation program was to develop a unified, consistent campus-wide approach for workstation support and management. After the consolidation a number of campus units still did not use ITS for their workstation support for a variety of reasons addressed later in this document.

The Support Center provides direct workstation support and is comprised of the Help Desk, Support Operations, and Support Depot teams. The Support Center provides the following types of computer workstation support.

- Workstation setup for new employees
- Software installation
- Upgrades and updates
- Workstation troubleshooting
- Workstation upgrades
- Workstation disposal services

Support Center services are obtained by submitting a ticket in the on-line IT request system, email, or by phoning the Help Desk. The Help Desk resolves issues directly or will escalate the ticket to the appropriate technician inside the support center or other ITS units as needed, e.g. network service, etc. For all Support Center services a ticket is created in the IT request system to track and monitor work. The unit or team that completes the work will close out the ticket when the work is completed. The current organization of the Support Center and use of the IT request system have helped to coordinate, monitor, and manage workstation support activities within ITS, although some workstation support is still provided by Local IT Specialists (LITS) who report to the Divisional Liaisons.

One staff member in the Support Depot team produces software images on a regular basis that have operating systems and software commonly needed by the Support Operations staff. The software images are available to Support Operations staff via download from the central Microsoft Windows Domain server. Regular image production minimizes the number of patches required to bring the software up to date and assures workstations have the same basic configuration.

The manager of the Support Depot team is responsible for the implementation of the BigFix remote management tool and Sophos Enterprise Console. This project is currently funded for the first 3,000 workstations. BigFix has full Microsoft

Windows and Mac Support, and can support Linux and UNIX (if those modules were implemented) and provides the ability to patch both Operating System and third party software. BigFix also has an asset discovery module that could be used to identify and inventory, and manage all workstations connecting to the campus networks.

The first stage of this project was to replace LANDesk, which was another remote management tool that was installed on approximately 800 workstations in 2008 in an attempt to improve workstations management and security that ultimately did not meet the needs of the University. LANDesk was replaced with BigFix, QuickSupport (TeamViewer) that provides remote desktop access to ITS support staff, and Sophos Enterprise Console. QuickSupport is also being used independently of BigFix and Sophos Enterprise Console to provide ITS support staff with remote assistance tools to answer client questions and resolve problems remotely.

The units we reviewed that did not use ITS Support Center Services included:

- Educational Partnership Center (EPC)/UC College Prep (UCCP)
- University Police
- Financial Aid
- School of Engineering (insecure subnet academic workstations)

Each of these units has unique situations and reasons that they do not utilize ITS Support Center Services, as listed below.

When ITS consolidation occurred, EPC/UCCP had a specific grant to fund a .5 FTE IT support position. As this grant was specific to these units, it was not possible to combine the position into the larger ITS organization and these units were largely excluded from the consolidation. They do not receive any direct support, other than that the use the ITS Software Licensing Coordinator to take advantage of the software discounts available to all University Units. Over the past year, EPC and UCCP have merged into a single unit, and as the re-organization is finalized, Student Affairs may consider alternative arrangements for general IT support and/or filling IT-related staff positions. The current .5 FTE position may not be sufficient to provide workstation support to both units.

The University Police does not normally allow ITS to access their workstations because the background checks performed and required for police officers are more stringent than the background checks performed for other critical positions at the University. The Police have one employee spend half of her time doing

workstation support and have recalled a retired Police Sergeant as a part time hourly employee to provide additional workstation support.

Financial Aid has outsourced their workstation, firewall, and server support to a local contractor since 1998. The original contact with this vendor was started so that they could obtain a Firewall, on the advice on Internal Audit, when CATS was not prepared to offer this service. They have continued to pay the contractor for support since that time and have not been part of the ITS consolidation.

There are likely other units that also do not use the ITS Support Center for workstation support, but identifying all of them was not feasible, partly because ITS does not maintain an inventory of all workstations connecting to campus networks. The Arboretum was brought to our attention late in the audit as another self-supporting unit, but our fieldwork was already complete so we did not review their workstations.

The raising of the inventorial equipment threshold to $5,000 some years ago has also made it more difficult to keep track of all University owned computers. One of the modules available in BigFix is the Asset Discovery feature that will record all computers connecting to the campus network, and identify the type of computers as much as possible. In our opinion, identification of University Workstations is a necessary first step in managing them.

C. Scope

We reviewed 22 workstations in ten units including various different types of workstations and Microsoft Windows Domains to determine if they were meeting the minimum campus network connectivity and security standards, University Policy, and industry best practices.

As the campus is in the process of implementing an ITS Support Center remote management tool (BigFix) we incorporated the use of this tool into our review. We also reviewed the reports compiled with the BigFix application documenting the vulnerabilities identified on the first 312 computers with the BigFix client installed. We reviewed and compared the policies affecting workstation configuration and security on seven Microsoft Windows Domains.

We defined different types of workstations in our initial audit planning and attempted to test at least one of each of types of the workstations, as listed below:

- Workstations managed by ITS utilizing the BigFix remote management tool.
- LANDesk Administered machines (These were replaced with BigFix during the audit and not LANDesk workstations were available for review).
- ITS manually administered workstations - Workstations that are administered in the clients office or taken back to an ITS office for service. ITS service may also be provided via the QuickSupport remote access tool. These workstations may not yet have BigFix deployed or may be out of scope of the initial BigFix deployment.
- HIPAA workstations – SHS, Benefits and Fire Dept are part of the HIPAA covered entity. Special training and check lists have been developed by ITS to configure and administer these workstation.
- Payment Card Industry workstations - Credit Card merchants are subject to Data Security Standards as dictated by the Payment Card Industry.
- Life/Safety – Police/Fire workstations.
- Non ITS managed workstations including:
  - Unit or user managed
  - Third-party (contractor) managed

We did not review any home workstations that may be used for University business purposes and only conducted limited review of other mobile devices, e.g. iPhone, iPod, BlackBerry, Etc.

D. Positives

The ITS Support Depot Group Manager responsible for the BigFix Enterprise Suite and Sophos Enterprise Console project has identified that the key to success of the project is the process, and not the tool itself. He noted there are 50 remote desktop management tools on the market. High Cost, poor technology support and user acceptance were identified as limiting factors in implementing LANDesk.

LANDesk also had technical deficiencies, but it appears BigFix was well researched and has necessary technical capabilities. The Support Depot Group Manager is implementing the patch management and related processes in stages to assure that BigFix and/or Sophos does not cause unexpected workstation problems.

While some users may expect quicker results we agree it is more important to gain trust and acceptance to assure successful wide spread deployment.

III. OBSERVATIONS REQUIRING MANAGEMENT CORRECTIVE ACTION

A. Workstation Software Vulnerabilities

We found that a large percentage of campus workstations tested had one or more vulnerabilities.

The campus should continue to pursue testing, development, and implementation of remote management tools.

Comments:

Software Vulnerabilities

We reviewed 22 workstations in ten units and found 42 software vulnerabilities. Many of the vulnerabilities could allow hackers to take complete control of the workstation. Seven of the workstations were missing multiple Microsoft Office patches or service packs, four were missing critical or important operating systems patches or service packs, and 12 workstations had 30 un-patched third party software vulnerabilities.

A report of the first 312 workstations to have the BigFix client installed further revealed that, prior to BigFix patching, over a third of these workstations had vulnerable third party software and large numbers were also missing critical operating system and Microsoft Office patches and service packs.

Seven of the workstations we reviewed were missing many critical Microsoft Office Patches. Some workstations were missing as many as 30 Microsoft Office patches. Most of the workstations that were missing Microsoft Office Patches were configured to install automatic updates, but were only installing operating system updates and not Microsoft Office updates. Microsoft provides two web pages for updating their software products. The "Windows" update web site only updates the Microsoft Windows operating system, whereas the "Microsoft" update web site updates Microsoft Windows operating system and Microsoft Office software. Although this condition was noted on both ITS and unit/user supported workstations it was more common on the unit/user supported workstations. To assure the workstation is using the "Microsoft" update web site the user/administrator must navigate through the "Windows" update site and check a box to "agree" to use the "Microsoft" update site.

Four of the workstations were missing critical or important operating system patches or service packs. Two of these workstations were missing Microsoft Service Pack 3, which did not install through the automatic update process. One was a newly built workstation that had auto update enabled and would have updated on its own. One was a workstation managed exclusively by a Graduate student.

We also reviewed an initial report of the software vulnerabilities BigFix detected on the first 312 workstations. The most common software vulnerabilities were also related to third party software. Over a third of the workstations scanned by BigFix, prior to BigFix patching, had vulnerable versions of QuickTime, Java, Adobe Flash, or Adobe Reader.

The following chart summarizes the software vulnerabilities noted in our review.

Software Vulnerabilities Noted					
Department and Number of Work-stations tested		Third party software	Trojans	Microsoft Office	Operating System
Student Health Center (HIPAA workstations)	3				
Ticket Office (PCI workstations)	3	4		2	1
Police (Unit Administered workstations)	2	8			
TAPS (ITS administered workstations)	1	0			
Educational Partnership Center (Unit administered workstations)	4	6	1	3	1
UC College Prep (Unit administered workstations)	1	0			
Dining (ITS administered workstations)	1	2			
Financial Aid (third party administered workstations)	1	1			
Internal Audit (workstations newly imaged by ITS)	2	3		1	1
SOE (ITS administered workstations)	3	5			
SOE (user administered workstations)	1	1		1	1

We also found the following specific issues affecting workstation security:

Java Run Time Environment Software Challenges

Java Run Time Environment presents some unique security challenges because it is used as middleware with other third party software. The third party software does not always certify and support the most recent release of Java. For example the version of Java currently available on the ITS download page for SCT Banner is Java 6, update 11 which has known vulnerabilities. The current release is Java

6, update 21 which appears to work with SCT Banner, but has not been tested or certified by Financial Affairs. Although BigFix is capable of patching all the third party software noted the current plan is to not patch Java until the versions compatible with enterprise applications are identified. When the necessary versions are identified and certified, BigFix will be used to patch Java to the most current version that works with the enterprise applications.

University Police Office Challenges

The two University Police workstations reviewed had a relatively large number of third party software vulnerabilities. The web browser was Firefox 2.0, which was replaced with Firefox 3.0 in June 2008 and is now unsupported by the vendor. They also used an unsupported version of Eudora as the email client. We did not find any serious malware on Police workstations, likely due to the fact that ITS has provided a hardware firewall in their network closet that blocks most internet users from seeing or attacking their workstations. The Police have one person dedicated half time to workstation support and have also brought a retired police sergeant back part time to provide additional workstation support. The retired Sergeant estimated it would take him several months just to change the Eudora users to a supported email client.

The police typically do not use ITS staff to support their workstations because the background checks performed on Police Officers who access Police data are more stringent than background checks performed on ITS and other University employees. In our opinion, BigFix might prove to be a very good solution for the Police Department in that it could be used to patch and support their workstations without giving access to restricted Police data to ITS staff. BigFix provides logs available to end users of all the actions it has taken, which should provide the police with the appropriate assurance that their restricted data is not compromised in the process. The BAS Divisional Liaison and the retired Police sergeant both agreed this should work, but the Divisional Liaison and Police Chief need to reach a final agreement and ITS may need to train the Police on the use of the BigFix software and logs.

PCI Scans of Ticket Office Systems

After noting that one of the workstations in the Ticket Office was missing Microsoft Windows operating system Service Pack 3, we asked ourselves why this had not already been detected on the requisite monthly Payment Card Industry scans of their systems. In reviewing the monthly scans, we found that only the main ticketing system in the data center was being scanned and workstations in the Ticket Office and Recital Hall were not scanned. University Relations corrected this error when it was brought to their attention.

Workstation Audit Logs

We observed that one workstation jointly administered by a third party and the unit did not have audit logging enabled, although logging was enabled on the Domain server. One supported workstation had audit logging enabled for some events, but was not configured according to Microsoft recommended best practices. In the University Relations audit, number SC-09-13, ITS agreed to "enable audit logging on all new ITS computers or computers on which the operating system is reinstalled, per security best practices". ITS implemented this agreement; however, since one of these workstations is not managed by ITS it is not as clear how consistent implementation will be achieved.

Antivirus Software not Installed on Mac Computers

Four unit administered Mac workstations did not have anti-virus software installed. The UCSC Minimum Requirements for Network Connectivity mandate "Malicious Software Protection to protect networked devices from malicious software, such as viruses, spyware, and other types of malware". The campus has anti-virus software freely available for Mac operating systems. When we made the support staff aware that this software was available, it was installed on the computers we had previously reviewed.

EPC/UCCP Challenges

We found two Trojans on an EPC laptop computer. EPC technical support already knew the computer was infected. EPC support staff thought they had removed the Trojan, but our scanning software still detected two Trojans. The Trojan reportedly opens a backdoor channel to the system to allow access by other infections. EPC has lost some of their technical staff and may no longer have enough staff to support and patch all workstations timely. BigFix may be the best solution for EPC workstation security unless additional support can be obtained. The Student Affairs Divisional Liaison will need to work with EPC to determine the best course of action.

Remote Management Tool Solutions

To address workstation security management issues ITS has purchased licenses to install the BigFix client on 3,000 workstations to determine if this tool will work and is acceptable to both ITS staff and end users. The Divisional Liaisons have been asked to identify the specific workstations in their divisions to have the BigFix client installed.

Agreements:

1. ITS Client Services and Security Support Depot manager will pursue testing, development, and implementation of appropriate remote management tools to help assure workstation administration processes

result in 3,000 properly configured and secure workstations by December 17, 2010.

2. BAS Divisional Liaison will work with the police chief, Police Department, and ITS as needed to see if Police workstations can be included in the initial implementation of BigFix by December 1, 2010.

3. Student Affairs Divisional Liaison, in consultation with the vice chancellor of Student Affairs and the ECP/UCCP executive director, will determine if the units should be re-prioritized, so that EPC/UCCP is included in the initial implementation of BigFix by December 1, 2010.

4. ITS Client Services and Security Support Depot manager will work with business partners on strategies to run non-vulnerable versions of Java JRE, including working with software vendors or advising clients on alternatives to reduce risks. ITS will track which clients need to have vulnerable versions of Java and manage BigFix Java patching accordingly October 29, 2010.

B. Workstation Inventory (*High Risk*)

UCSC does not have an inventory of workstations owned or used by the University nor does it keep an inventory of workstations that connect to the campus network.

An accurate inventory of workstations should be completed as a first step in identifying which assets needs to be protected and the appropriate risk mitigation techniques to apply.

Comments:
Business and Finance Bulleting IS-3 requires that the campus conduct a risk assessment to "…inventory and determine the nature of campus electronic information resources" and "to identify the level of security necessary for the protection of the resources". Industry standards such as the International Standards Organization IS 27002 also states, "All assets should be clearly identified and an inventory of all important assets drawn up and maintained" and "The process of compiling an inventory of assets is an important prerequisite of risk management"

UCSC has not had the technical capabilities to log and inventory all workstations connecting to the campus network. One of the specific benefits listed in the ITS Support Center Remote Management Tools: BigFix Enterprise Suite and Sophos Enterprise Console project is:

Current Asset Information
Current, accurate computer hardware and software asset information provides a clear picture of the supported desktop environment. This data will be used to inform decisions related to service levels, standards development and maintenance, service changes, software licensing, hardware and software purchasing, and many other decisions requiring accurate information about our computing environment.

Asset identification is currently limited to identifying Operating Systems and software on the first 3,000 workstations in the initial project proposal. Implementing the BigFix asset identification functionality that will periodically scan the network to identify and log any computer and hardware connected to the network that is not managed by BigFix should be implemented if the first test group proves successful. Identification and inventory of all workstations used for University Business is critical and should be a longer-term goal.

Agreement:
ITS Client Services and Security Support Depot manager, upon successful initial implementation of BigFix, will enable BigFix asset identification functionality to periodically scan the network to identify and log any computer and hardware connected to the network that is not managed by BigFix to begin building a complete inventory of workstations used for University Business by March 31, 2011.

C. Campus Software Image Distribution and Use

The campus software image that contains operating system, Microsoft Office, and commonly deployed third party software and the accompanying post-image checklist procedure is not available to the staff providing workstation support in self-supporting units or to LITS who provide workstation support. The post-image checklist used to install the software was missing an important step and was not always followed by Support Operations staff.

Comments:
The Support Deport produces software images on a regular basis. The images have operating system (Microsoft Windows or Mac) and Microsoft Office that are patched and up to date as of the date the image is produced. The images also contain patched versions of Adobe Reader, Acrobat, Java, and other commonly used third party software. The campus Software Image disk is only available to Support Center Staff. Workstation support staff in self-supporting units and LITS who re-image workstations use the original disks purchased from the

software vendors or provided when the workstations were purchased. These disks can be years old and require many more patches and/or service packs than would be required with the campus Software Image. This increases the risk of compromise since the un-patched workstations are connected to the internet while the patches are applied and ultimately takes more time to update. We verified that the Educational Partnership Center and UC College Prep both participate in the Microsoft Consolidated Campus Agreement license program which allows them to install the latest Microsoft operating system and Microsoft Office releases. We were not able determine how the Police Office paid for their software licenses, but the Campus Software Images are made using Microsoft Windows XP and Microsoft Windows 7, so ITS should be able to provide the appropriate image to match the unit's license. The Support Depot manager stated a process was being developed to verify software licenses before new software was offered to individual users via BigFix, with a focus on Microsoft and Adobe products.

The Campus Software Image installation procedure includes the use of a post-image checklist to assure workstations are configured consistently and securely. In reviewing workstations that had been freshly imaged, we noted that not all third party software was up to date. The post-image checklist did not include steps to update third party software. Although the third party software was set to auto-update, the end user must allow the update. Until the update is applied, the software is vulnerable. The workstation we reviewed had vulnerable versions of Firefox, Adobe Reader, QuickTime, and Thunderbird.

The post-image checklist does not include a step to run Microsoft Baseline Security Analyzer (MBSA). When we ran MBSA on a newly imaged workstation, we found missing Microsoft Office patches because the checklist was not followed to assure Microsoft Office updates were enabled. MBSA also checks for incomplete installations of Microsoft updates, assures audit logging is enabled, checks for weak or missing passwords, and unneeded services. Running MBSA used to be part of the standard procedure for re-imaging workstations, but at some point the procedure was re-written and this step was removed. In our opinion, the few minutes it takes to run MBSA is well worth the time to assure the workstation is fully patched and secure before it is given to the end user.

The Microsoft Windows workstations we reviewed at EPC were configured to automatically update the operating system but had not yet been configured to update Microsoft Office.

If the Campus Software Image and post-image checklists were provided to self-supporting units it would be more likely that their workstations were configured to update Microsoft Office as well as the operating system.

Agreements:

1. ITS Client Services and Security Support Depot manager will develop a plan to provide standardized imaging materials to clients or support staff who are not currently using the Support Depot to image or re-image workstations and can demonstrate proper licensing by December 1, 2010.

2. ITS Client Services and Security Support Depot manager will determine if ITS can provide workstation imaging services to units who currently are not receiving ITS services. If possible notify applicable units of the status by December 1, 2010.

3. ITS Client Services and Security Support Depot manager will update the post-image checklist to include updating third party software and to run MBSA after the image is installed by September 1, 2010.

D. Microsoft Windows Domain Policies

The campus does not have a standard configuration for Microsoft Windows Domain policies that affect workstation settings and security.

Comments:

We reviewed the policies for seven Microsoft Windows Domains. While most were consistent with Campus Network Connectivity Requirements and best practices, one Domain did not enforce password complexity in compliance with Campus Password Policy.

Detailed standardized Domain Policies may not be required, but Domain policies should be consistent to enforce University and Campus Policy to the degree possible. A standard policy, if developed, may provide for increased efficiencies and standardization if new Domains are created and policies need to be manually configured.

Agreements:

1. EPC has changed their Domain policy during the audit to require complex passwords in compliance with the Campus Password Policy implemented on May 25, 2010.

2. ITS Client Services and Security Support Depot manager will document standard Microsoft Windows Domain Policies consistent with Campus Minimum Network Connectivity Requirements for use by Windows Domain Administrators by October 31, 2010.

E. Restricted Data on Workstations

Social Security Numbers (SSN) were found on a number of workstations and laptops at EPC that originated from a UCOP formatted database used to identify potential students on a non-profit National Student Clearing House web page.

Comments:
Most of the SSNs identified appeared to originate from a database kept to track potential students. The collection of the SSN was dictated by a very specific database variable format sheet provided by UCOP. The SSN were copied from the database to other workstations and laptops. At least one workstation did not require a password to access files containing student names and SSNs. EPC was very responsive in searching for and eliminating files containing SSNs after we provided them with a tool to conduct these searches.

We contacted UCOP and questioned the need to collect this data. UCOP indicated that they were considering eliminating the collection and storage of SSNs. Subsequent to this dialogue, UCOP removed the SSNs from the list of data fields to be collected and stored, and plans to work with units throughout the UC system to redact or secure any stored SSNs.

In addition, Financial Aid requested that we scan the workstation we audited for SSN. While we did not find any SSN on this workstation we provided the SSN search logic and Financial Aid purchased the search tool so that they could continue to search all their systems to find and eliminate legacy SSN data.

Agreement:
EPC has worked with UCOP to eliminated SSNs in their database and secured all workstations as requested by UCOP implemented on July 1, 2010.

***