# SYSTEM COMPUTING SERVICES
# NETWORK SECURITY AUDIT
Internal Audit Report
April 1, 2014 through December 1, 2014

## GENERAL OVERVIEW

Network resources run the gamut from simple desktop computers to complex appliances and devices such as routers and firewalls that direct network traffic and control access to other network resources such as servers and storage devices. System Computing Services (SCS) network resources are particularly complex due to SCS being the gateway to the Internet for much of the State of Nevada. Data stored on the network has a similar range of sensitivity and confidentiality. There are federal and state regulations that govern how data is to be managed, ranging from the Family Educational Rights and Privacy Act (FERPA) and Health Information Portability and Accountability Act (HIPAA) to state laws such as Nevada Revised Statutes (NRS) 603A. Further, there are industry requirements from the Payment Card Industry (PCI) that govern an institution’s acceptance of credit cards and electronic payments. The Board of Regents also has policies and guidelines as outlined in Title 4, Chapter 1, Section 22 of the Board of Regents Handbook and Chapter 14 of the Procedures and Guidelines Manual adopted in December, 2009. The configuration and management of network devices has a significant impact on the security of the device, the network, data stored on the network, and our compliance with the laws and standards mentioned above.

## SCOPE OF AUDIT

The Internal Audit Department has completed a review of Network Security at SCS. We conducted our review between April 1, 2014 and December 1, 2014.

Our review was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included a review of SCS policies and procedures governing management, security and testing of devices that we considered significant to the overall security of SCS's network.  Our testing included, but was not limited to the following.

1. Evaluating the administration and configuration of key production servers used to support critical applications using industry standard benchmarking tools when available.
2. Reviewing the configuration and administration of key firewalls used to restrict access to and from the Internet and to control access to certain network resources and segments using industry standard benchmarking tools.
3. Testing administrative desktop and laptop computers for critical operating system patches and antivirus software.
4. Reviewing how critical data is backed up.

In all cases we used standards from recognized sources such as the National Institute for Standards and Technology (NIST), the Center for Internet Security (CIS) and others.

It should be noted that certain important network devices were not evaluated due to equipment that was being replaced at the time of the audit with a new vendor.

In our opinion we can be reasonably assured that SCS network security is functioning in a satisfactory manner. The reason for this opinion is primarily due to the monitoring and other practices implemented by the System Security function.  Their use of automated tools and continuous evaluation of various network security aspects has a positive impact on the overall security landscape.

We believe that implementation of the following recommendations would further improve the security of the SCS network and recoverability of critical data.

## SYSTEM BACKUP

System and database backups are critical to the continued functioning of a datacenter in the event of a security breach or system malfunction. SCS acts as its own backup service by utilizing its datacenters in Reno and Las Vegas. Data is replicated and systems are backed up across the network to each center. The geographic distance between each location is considered sufficient to avoid the problem of both centers being included in a common disaster. In reviewing the backup process, however, the following exceptions were noted.

1. Backup copies are vulnerable to accidental or intentional deletion by System and Data Base administrators due to current, replicated, and back-up data being online and essentially stored at a local level.

   We recommend that SCS implement the necessary changes to the backup process to alleviate the risk of deleting the backups.

   **Institution Response**

   **SCS Systems Support Services is responsible for data backups and the security of the data being stored. Changes required to mitigate the risk of deleting backups have been implemented. Copies of backup storage have been made inaccessible to all administrators except SCS Systems Support Services analysts who require write access to the storage library in order to install, configure, and maintain the storage subsystem.**

**Follow-Up Response**

**This recommendation was fully implemented at the time of the initial response. We request that this finding be closed.**

2. While data restoration is performed on a regular basis, not all areas and platforms are part of the regular restore process.

   We recommend that SCS implement a method to test the restore process across all backup areas and platforms.

   **Institution Response**

   **An automated test-restore process will be implemented and scheduled to run at regular intervals for all platforms. Tests will be run nightly to verify the restoration process on AIX, Linux, and Windows platforms. The process will be implemented by 8/31/15.**

   **Follow-Up Response**

   **SCS has procured and implemented the Automated Restore Testing (ART) utility from TSMworks to verify file restores on AIX, Linux, and Windows platforms. Tests are run nightly and results are verified on a regular basis. We request that this finding be closed.**

## NETWORK SERVER TESTING

Servers provide many critical functions for networks. The most obvious examples are network authentication and websites. Whenever a user logs into a network, a server is utilized to authenticate to the network. The authentication process also determines what network resources can be accessed and, perhaps more importantly, the types of access, such as read only or update access. Similarly, a web server is used to "serve up" a web page when someone uses a web browser to access a website.

### *Windows*

We used industry standard benchmarking tools to evaluate 24 of the higher risk Windows based servers. SCS ran the Center for Internet Security (CIS) Configuration Assessment Tool (CAT) on the 24 Windows servers. The CISCAT evaluates over 200 configuration parameters that affect server security. We also ran the Microsoft Baseline Security Analyzer (MBSA) on a subset of eight Windows servers. MBSA looks for missing updates and common security misconfigurations and provides an overall risk assessment of the server. Each of the servers tested with the MBSA tool received a "Potential Risk" rating. The benchmarking tools noted the following exceptions:

1. CISCAT identified possible security configuration changes for several parameters including:
    a. Windows firewall not implemented
    b. Certain logon parameters not implemented
    c. Restricting certain user rights to administrators
2. The MBSA tool noted the following concerns:
    a. User accounts (including generic) with non-expiring passwords.
    b. Non-interactive service accounts and certain administrator accounts with non-expiring passwords.

For items one and two, we recommend that SCS follow the guidance provided in the benchmark tool reports for correcting the various deficiencies and review the user accounts on each server to eliminate generic, test, and stale user accounts where appropriate.

**Institution Response**

**SCS Systems Support Services is responsible for server configurations, user account management, and server security. The benchmark tool report**

**recommendations were followed to apply security configuration changes and delete eligible generic, test, and stale user accounts. The reports will be reviewed on an on-going basis and used as a guide for continued application of security enhancements on Windows servers.**

1. **Security Configuration Changes**
    a. **Windows Firewall has been enabled.**
    b. **Logon parameters noted by CISCAT have been implemented.**
    c. **SCS has recently purchased a privilege management tool to reduce and manage local administrative capability granted to administrators on Windows clients. Implementation of the privilege management tool should be completed by December 2015 with additional tuning and ongoing management as required.**

2. **User Account Concerns**
    a. **The only remaining user accounts with non-expiring passwords, some of which are generically named, belong to Institutional Presidents whose leave is tracked through the SA/SCS iLeave tool. These accounts are in place to minimize inconvenience to institutional executive assistants and address difficulties with external (non-SCS/SA) staff resetting their Active Directory (AD) account's password as there is no linkage between SCS's AD environment and institutional AD environments. These accounts will no longer be necessary and will be deleted once the leave tracking component of the iNtegrate 2 project has been implemented. As an interim solution, SCS will require that leave tracking accounts be named after and assigned to the actual person performing leave tracking, provide automated password reset reminders to said persons, and assist said institutional users with changing their password over the phone via the SCS Service Desk. This method of resetting a password is not ideal due to the inherent difficulty of identity verification over the phone, with the additional side effect of Service Desk staff being privy to the external leave keepers' new passwords. The interim solution will be completed by 12/31/2015.**
    b. **Some service accounts have non-expiring passwords to avoid inadvertent downtime due to expiration. Moving forward, the designated owner of a service account with a non-expiring password will be required to schedule and perform a password reset yearly with a one month grace period. The passwords for such service accounts will be of greater length and complexity than those required by AD Group Policy for normal user accounts. Automated password reset reminders will be sent to the service account's owner. The service account owner's**

**manager and the System Security Officer will be automatically notified if the password reset does not occur in a timely fashion. Account changes to require password resets are expected to be completed by 10/31/2015.**

**Follow-Up Response**

1. **Security Configuration Changes**
   a. **This recommendation was fully implemented at the time of the initial response. We request that this finding be closed.**

   b. **This recommendation was fully implemented at the time of the initial response. We request that this finding be closed.**

   c. **Implementation of the privilege management tool should be completed by 12/31/15 with additional tuning and ongoing management as required.**

2. **User Account Concerns**
   a. **Standard password expiration has been implemented for all user accounts except those belonging to Institutional Presidents and their Executive Assistants. The ability for named Executive Assistant accounts to manage leave tracking for the Presidents is currently being tested in iLeave. Once testing is complete, named accounts will be defined for each Executive Assistant. Passwords for the Presidents and Executive Assistants will be reset on first access, then expire annually like Service Accounts. We expect all generic accounts associated with the leave tracking process to be deleted by 12/31/2015.**

   b. **Procedures and an automated tool for notifying Service Account owners, their managers, and Security have been implemented per our initial response as of 5/27/2015. Several Service Accounts with a password last set prior to that implementation date must still be changed by the account owners. We expect that these service account passwords will be changed by 12/31/2015.**

## UNIX BASED SERVERS

We used the CISCAT tool and a specialized Unix audit script to evaluate a total of 36 Unix based servers. The Unix environment supports critical applications and processes that are vital to the functioning of the institutions and the network itself.

PeopleSoft Campus Solutions and its associated database run in this environment as do the Domain Name Servers (DNS) necessary for network navigation. The benchmarking tools noted the following exceptions:

1. The CISCAT benchmark identified possible security configuration changes for several parameters including:
    a. File and directory permissions and ownership
    b. Transmission Control Protocol/Internet Protocol (TCP/IP) hardening
    c. Securing remote access
    d. Known vulnerabilities in some unused system services
2. Password parameters that did not comply with NSHE standards.
3. The switch user or super user (SU) command has potential for abuse from certain groups and/or users.

For items one through three, we recommend that SCS follow the guidance provided in the benchmark tool reports for correcting the various deficiencies.

**<u>Institution Response</u>**

**The benchmark tool reports, in addition to other operating system and security utilities, will be reviewed quarterly and used as a roadmap for continued hardening and application of security enhancements on all UNIX servers. SCS Systems Support Services is responsible for security at the operating system level as well as access to the servers. Each campus is responsible for application level file and directory security. The benchmark tool report recommendations have been followed to implement security configuration and user account changes.**

1. **Security Configuration Changes**
   **Suggestions for UNIX permissions at the operating system level, TCP/IP hardening, securing remote access, and eliminating unused system services were implemented. Security recommendations for application files have been conveyed to the campus owners. Campus owners have implemented some of these changes, but have elected not to make some changes because the files and directories in question are**

**considered non-critical. SCS will evaluate campus application file security and communicate benchmark tool recommendations on an on-going basis. SCS will also review the recommendations from various reports on a quarterly basis and make changes as needed.**

2. **Some password expiration time periods for user level accounts on Linux and AIX systems vary from the NSHE policy regarding password parameters. A business case has previously been made for reasonable extension of this limit; however SCS will work to shorten the expiration period to comply with policy standards. Adherence to policy standards is expected to be implemented by 12/31/15.**

3. **SCS has been working on the elimination of direct login to shared accounts such that users are required to login with their personal account first and then switch (SU) to the shared account. The elimination of direct logins has been completed for the Shared Instance. UNR is about 80% compliant and SCS is actively working with UNR IT to implement the remaining changes by 7/31/2015. UNLV is about 20% compliant and has indicated that the remainder of the changes would pose a significant issue to their on-going operations.**

**Follow-Up Response**

1. **This recommendation was fully implemented at the time of the initial response. We request that this finding be closed.**

2. **AIX user accounts and most AIX service accounts have been brought into compliance with NSHE password standards, however some application AIX service accounts remain non-compliant. The UNR and Shared Instances retain 3-5 service accounts with non-compliant password expirations while the UNLV Instance maintains 18-20 non-expiring service accounts. Each of the application owners has indicated that changing passwords for these service accounts would cause significant disruption to business processes. Account owners will be required to provide an exception request describing the business need for an exemption from the policy.**

   **User and service accounts created on Linux systems since June 2015 are in compliance with the NSHE password standards and several existing accounts were also brought into compliance. However, after a more in-depth review of the remaining accounts, we will be unable to bring them into compliance by the originally projected completion date of 12/31/15. Several of the remaining 200+ accounts are 10-20 years old with inaccurate or no associated contact information. These accounts are remnants of a two year project in 2009 to decommission**

**student email and transition UNIX services to newer hardware. At that time, campuses could request that specific faculty and staff accounts be kept active. We have done a cursory review of accounts and outlined a plan to perform a usage analysis in order to categorize accounts for retention or deletion, obtain or verify contact information for retained accounts, and contact account owners to confirm the continued business need for the account. Additionally, we will research and implement a password self-service process or product so that account owners can be notified of pending password expirations and change the password. We expect to bring Linux account passwords into compliance with NSHE password standards by 5/1/16.**

3. **The elimination of direct logins was completed for the Shared Instance at the time of the initial response. SCS has worked with UNR to implement and test additional changes in their development and test environments to eliminate direct logins. These changes will be implemented on UNR's production systems on 10/24/15 at which time the UNR Instance will be at 100% compliance. After reviewing the status of changes with UNLV OIT, the UNLV Instance remains at about 20% compliance and feels that any additional changes to remove direct logins would pose a significant issue to their on-going operations.**

## VMWARE

We used the CISCAT tool along with the VMware compliance checker and audit program to evaluate eight virtual machines that host the various Windows servers noted earlier.

1. VMware compliance checker noted issues with:
   a. Media Access Control (MAC) address changes
   b. Rejection of certain types of data transmit

   We recommend that SCS follow the guidance provided in the compliance checker to alleviate these issues.

**Institution Response**

**The recommended changes have been implemented on all VMware hosts and a script has been written to include these changes on any new hosts.**

**Follow-Up Response**

**This recommendation was fully implemented at the time of the initial response. We request that this finding be closed.**

VIOS AND HACMP

Virtual IO Server (VIOS) in combination with High Availability Cluster Multiprocessing (HACMP) are components of the virtualized environment for the Unix based systems mentioned previously. These systems support critical applications across all NSHE institutions. This combination of products is designed to provide continuity and fail-over capability in the event that a server or storage device fails. We used vendor hardening and best practice guides to evaluate this environment. The following exceptions were noted:

1. The VIOS systems have not had any hardening standards applied to them.
2. The capability of the HACMP fail-over process to function correctly has not been adequately and regularly tested on either the system or the application.

We recommend that SCS use the vendor hardening guide to secure the VIOS systems.

**Institution Response**

**Security best practices have been implemented and recommendations noted in the IBM hardening standard have been reviewed and applied to the VIO servers. The reports will be reviewed quarterly and changes will be implemented as appropriate on an on-going basis.**

**Follow-Up Response**

**This recommendation was fully implemented at the time of the initial response. We request that this finding be closed.**

We also recommend that SCS develop and implement a process to regularly test the functioning of the HACMP process for systems and applications.

**Institution Response**

**SCS will schedule and coordinate quarterly failover tests with each Campus Instance (UNR, UNLV, and Shared) to verify successful functioning of the automated HACMP process at the operating system level and incorporate application level restart testing as requested by each Campus.**

**Controlled failover tests were included with the upgrade of the HACMP product code which will be completed for second quarter on all HACMP systems by 5/30/15. SCS is responsible for and provides an automated failover test process for operating system level resources with each HACMP upgrade where system level resources are moved from the failed primary database server to the backup server. Operating system level resources were tested and automatic failover has been successful for all upgraded systems. Future quarterly tests irrespective of a HACMP code upgrade will be scheduled with each Campus Instance.**

**Each Campus Instance is responsible for and may elect to include a scripted restart of the application upon failover to the backup node. UNLV and UNR successfully completed a scripted restart of the application in the controlled failover tests during the HACMP upgrades. Due to the complexity of the Shared Instance applications system design, at this time the SCS IAS group finds it more prudent to manually shut-down and start-up the database and the application and web services in the event of a server or storage device failure. This manual process affords the Database Administrators at SCS the opportunity to determine a root cause of the failure and to ensure that the integrity of the database itself has not been compromised, something that is not feasible if automated start-up scripts are used. However, the SCS IAS group continues to work with the Systems Support Services group to develop and test processes which could conceivably provide for an automated start-up upon a system failure.**

**Follow-Up Response**

**Controlled failover tests for the Shared, UNR, and UNLV HA operating system environments were completed in June 2015. HA system configurations incur no changes except when they are being upgraded and**

**are designed to perform automatically a scheduled nightly test of all HA components, essentially double-checking every sub-component of HA to make sure that it has not changed since startup. While an automated HA failover when the system experiences a problem only takes a 1-3 minute pause in processing, a failover test requires 30-60 minutes of scheduled downtime due to the manual checks and balances involved in the testing process and the practice of "failing" back to the original system. Since one of the goals of system and application management is to minimize end-user downtime, production outages are complex and difficult to schedule due to competing time requirements for firmware, operating system, and application maintenance and upgrades. We feel that these factors mitigate the need for too frequent testing of a full HA failover. Since upgrade or maintenance is typically applied once or twice per year, we feel that testing incorporated in the upgrade/maintenance implementation is sufficient to test the functioning of the HACMP process. However, in the event that no upgrade or maintenance is scheduled within a year of the previous one, a controlled failover test will be scheduled such that HACMP functioning will tested at least once in any 12-month period. We request that this finding be closed.**

## FIREWALL TESTING

A firewall is a network appliance that is designed to filter network traffic entering and exiting a private network such as SCS's, or sections of a private network. It can also provide a buffer zone for those services that must be available to the Internet such as web and email servers. SCS employs numerous firewalls throughout the network to control ingress (incoming traffic) and egress (outgoing traffic) to other networks and to the Internet. We evaluated the configurations of four of the key SCS firewalls to determine whether they were properly filtering network traffic and being utilized to secure Internet accessible servers.

We noted some firewall configuration parameters were not set in accordance with the security benchmark, as provided below:

1. Not forbidding incoming traceroute
2. Not requiring fragment chain fragmentation checks

3. Excessive timeouts for some services

4. DNS guard not enabled on some firewalls

We recommend that SCS follow the guidance provided in the benchmark to mitigate these issues.

### Institution Response

1. **Traceroute/ICMP has been blocked from the Internet to all SCS/SA locations**
2. **Fragment chain fragmentation checks have been enabled.**
3. **All connection/access timeouts have been set to 20 minutes.**
4. **DNS guard has been enabled.**

### Follow-Up Response

**These recommendations were fully implemented at the time of the initial response. We request that this finding be closed.**

## DESKTOP/LAPTOP PERSONAL COMPUTERS

We evaluated 29 personal computers at SCS and NSHE facilities in Reno and Las Vegas. Each system was evaluated for appropriate operating system security patches, antivirus software version and virus signature data file. Training computers were also checked for system integrity software. We did not find any exceptions with regard to security patches, antivirus software or integrity software however we did note the following issue:

1. Each of the 29 users is granted local administrator privileges and this is the default for all users across NSHE and SCS. Local administrators have the capability to install and uninstall software on their systems. This would allow them to circumvent the installed security software and makes them more susceptible to malware from malicious email and websites.

We recommend that local administrator capability only be granted to those individuals with a job related need for this capability.

**Institution Response**

**SCS has recently purchased a privilege management tool to limit and manage local administrative capability on desktops. Implementation should be completed by December 2015 with additional tuning and ongoing management required.**

**Follow-Up Response**

**Implementation of the privilege management tool should be completed by 12/31/15 with additional tuning and ongoing management as required.**

## CHANGE CONTROL PROCESS

We evaluated the process that is used to document and communicate the running configuration, settings, and patch log of the production servers across SCS server platforms. The change control process is critical to specifically document and communicate what has been done to a server in terms of system settings, special configurations, software applications, and patch levels such that service can be restored in a timely manner in the event of a disaster, system breach, or improper update. The change control process at SCS is even more important given the complexity of the environment and lean staff within the systems function, which does not have the benefit of fully trained backup employees. During our review of the change control process, the following exceptions were noted.

1. There is no formal change control system for production server operating systems with the requisite level of detail.

   We recommend that SCS implement a formal change control process. Ideally, the process would cover all server platforms and provide the following information:

a. Run configuration

b. Testing, results and sign off

c. Change authorization

d. Patch levels

e. Specialized parameter settings

f. Server applications and usage

**Institution Response**

**SCS Systems Support Services will implement a formal change control process for production server platforms which will include the requisite detail for configuration, process, and compliance specific to the server environments as noted in the audit. We already adhere to established SCS procedures for tracking changes provided through the KACE Management Appliance as well as the Request for Change (RFCA) process followed by the SCS Operational Managers group. Systems Support Services will integrate a formalized process for hardware and software server related changes with the existing KACE and RFCA procedures by August 31, 2015.**

**Follow-Up Response**

**We agree that a formal change control process would be beneficial in the implementation of server operating system changes. Due to higher priority projects and lack of staff resources, we were unable formalize an acceptable process by the originally expected date. However, after much discussion and cursory research of automated systems, we have a better understanding of how to develop a manual process that includes more detailed configuration, use, testing, and authorization information to better track and document changes. We will not pursue an automated utility or process at this time, but have noted the preference for this type of solution and will research the associated feasibility and costs as time permits. We expect complete documenting a manual process by 12/31/15.**

2. Draft policies have been developed for one server platform that address security and configuration settings. The policies are a good start and cover much needed information but they are only in draft form.

   We recommend that SCS complete policies for all server platforms and that the policies be formally implemented.

**Institution Response**

**SCS Systems Support Services will work with the SCS Security Officer to formalize server policies that address security and configuration settings for server platforms. Accepted policies will then be implemented and exceptions to policies tracked through the SCS Security Office. We expect to document policies and exception requests to these policies by 12/31/15.**

**Follow-Up Response**

**A comprehensive draft security policy has been submitted to senior management for review. Sub-policies specific to server systems are expected to be completed by 12/31/15.**

## POLICIES, PROCEDURES AND BEST PRACTICES

We reviewed the SCS information technology (IT) policies and procedures and other processes at SCS that have an impact on security including: passwords, security training, contingency planning, incident handling, and risk assessment. The following exceptions were noted:

1. SCS' written policies do not cover all of the necessary topics and the existing policies are weak in some areas. International Standards Organization (ISO) specifications provide an excellent reference for policy development.

   We recommend that SCS complete and adopt a comprehensive set of information security policies.

   **Institution Response**

   **SCS will initiate a policy review and develop a comprehensive set of information security policies.**

   **Follow-Up Response**

   **A comprehensive draft security policy has been submitted to senior management for review.**

2. SCS has not completed an IT risk assessment or contingency plan as noted in the NSHE Procedures and Guidelines Manual, Chapter 14, Section 1.2. National Institute of Standards and Technology (NIST) Special Publications 800-30 and 800-34 address these topics.

   We recommend that SCS perform a risk assessment so that a contingency plan can be created.

   **Institution Response**

   **The NSHE Procedures and Guidelines Manual, Chapter 14, Section 1.2 requires "appropriate risk assessment provisions to identify vulnerabilities and threats to institutional information resources and major enterprise systems, including but not limited to scheduled network and system vulnerability scans." To this end, SCS has had a 3rd party security assessment performed in 2010 against all enterprise systems. In 2013 we had another targeted assessment performed against all enterprise database systems. In 2015, we are engaged with a 3rd party to perform a penetration test against enterprise systems. Additionally, SCS conducts weekly vulnerability scans against all desktop and servers. Reporting of vulnerabilities on desktop systems has been in place for several years. Weekly reports on all servers will be provided starting this April.**
   **The costs and resources necessary to conduct an additional "Risk Assessment" based on NIST Risk Management Framework (RMF) or other recognized methodology (OCTAVE, FAIR, TARA) will be examined.**

   **Follow-Up Response**

   **Server vulnerability reports are provided automatically on a weekly basis to the Systems group.**

3. SCS does not perform background checks when hiring personnel into sensitive IT positions. NSHE and the State of Nevada have standards that require background checks when hiring people for certain sensitive positions. Federal Information System Controls Audit Manual (FISCAM) SM-7.1 also recommends background checks be performed on outside contractors.

We recommend that SCS implement a background check policy for sensitive positions.

**<u>Institution Response</u>**

**SCS will investigate the current contracts within NSHE and leverage what the other institutional IT and Human Resources departments have already put in place. SCS will then create a policy and begin background checks for sensitive positions by December 30, 2015.**

**<u>Follow-Up Response</u>**

**There are ongoing discussions with System HR and legal counsel as well as the campuses on the broader issue of background checks for a variety of positions (not just positions related to IT). Moreover, given the interrelated nature of IT systems across the NSHE institutions, and the even closer inter-relationships with the forthcoming implementation of iNtegrate 2, SCS acknowledges the need for a baseline policy. However, SCS does not wish to establish such a policy in isolation as other background check models are likely needed and are being discussed. If a more comprehensive System solution is not forthcoming by April, SCS will propose and seek implementation of a program of background checks no later than June 30, 2016.**

The Internal Audit Department would like to thank System Computing Services management and staff for their cooperation and assistance during this review.

Reno, Nevada
February 5, 2015

Grant Dintiman

Grant Dintiman
IT Auditor

Scott Anderson

Scott Anderson
Director of Internal Audit