NEVADA STATE COLLEGE
PEOPLESOFT SECURITY AUDIT
Internal Audit Report
February 1, 2013 to May 30, 2013

GENERAL OVERVIEW

PeopleSoft Campus Solutions is the software system implemented across all NSHE institutions as part of the iNtegrate Project to replace the outgoing Student Information System known as SIS. The iNtegrate Project began in 2008 and completed in late 2011. Truckee Meadows Community College (TMCC) and the University of Nevada Las Vegas (UNLV) were the institutions picked to pilot the systems before it was rolled out to the remaining campuses. In mid-2010, TMCC and UNLV went live with the new system with all students enrolled in or applying to TMCC or UNLV using the new system. Nevada State College (NSC) went live with the admissions module in the fall of 2010 with all modules live by the end of 2011. PeopleSoft Campus Solutions is considered part of an Enterprise Resource Planning (ERP) system, with the Campus Solutions portion covering the major functions of student services consisting of the following five modules or functions: Recruiting and Administration; Student Records; Student Financials; Financial Aid and Academic Advising.

SCOPE OF AUDIT

The Internal Audit Department has completed a review of PeopleSoft Campus Solutions Security at Nevada State College (NSC). We conducted our review between February 1, 2013 and May 30, 2013. Our audit included a review of policies and procedures governing PeopleSoft security administration and tests of individuals' access to sensitive data as determined by representatives of the key functional areas. In particular, we were concerned with data that would fall under the auspices of the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standards (PCI DSS).

In our opinion, we can be reasonably assured that access to sensitive data in NSC's PeopleSoft Campus Solutions system is properly controlled and that PeopleSoft security administration is functioning in a satisfactory manner. However, implementation of the following recommendations would further improve security and simplify security administration in the future.

SECURITY ADMINISTRATION – ROLES AND PERMISSIONS

User access to data within PeopleSoft is primarily controlled by assigning roles to a user. In turn, roles have permission lists assigned to them that define what pages can be accessed and how the data on the page can be accessed. Data access can vary from display only at the low end to the ability to correct data at the high end. Permission lists can access from tens to hundreds of data items. Users can have multiple roles and roles can have multiple permission lists. It is also possible to assign a permission list directly to a user. NSC has access to 187 roles and 300 permission lists defined for use by any of the NSHE institutions that operate within the shared instance of the PeopleSoft Campus Solutions database and another 12 roles and 13 permission lists defined specifically for NSC. The development of the roles and permission lists was driven by the implementation consultants with the help of key functional area leads at the time of the iNtegrate project. We noted the following concerns with regard to the documentation of roles and permissions that was created as a part of the iNtegrate project.

1. There are no narrative descriptions that define what job functions roles and permission lists are designed to support, what data a permission list can access and the manner of that access – display only or update and so forth.
2. The existing documentation for roles and permission lists is inadequate for an ongoing security administration function and is becoming more obsolete as time passes and the employees involved in the original project move on to other positions.

We recommend that NSC work with System Computing Services (SCS) and their fellow institutions to develop narrative descriptions for both roles and permission lists. The narratives should provide information on the job functions supported, the data or pages they can access and the manner in which they are designed to access the data.

Institution Response

NSC agrees with this recommendation.

Correction

The existing documentation for roles and permission lists will become more obsolete as time passes. It is critical that we have a system in place to update the roles and permissions as operations and staff change. This will be addressed first at a system level to ensure consistency with other colleges and then at the institutional level.

System-Level Coordinated Effort

As part of the Shared Instance, NSC will coordinate its documentation efforts to complement the work being done by System Computing Services (SCS). SCS has developed a plan and timeline for a re-architecture of the Shared Instance security infrastructure. Chris Piekarz, Senior Security Analyst for SCS, presented this plan to the iNtegrate Shared Instance Advisory (iSIA) group where it was passed on May 23rd, 2013. This rebuild will impact how NSC will proceed with documenting roles and permission lists.

NSC Documentation

Narrative descriptions defining job functions for roles and permission lists, including data accessible under these constructs and level of access will be developed in the following manner:

- **For roles and permission lists that NSC does not expect to change as a result of the Shared Instance rebuild, NSC will begin a documentation effort. This documentation will be completed within one year from the date of this response.**
- **For roles and permission lists that will be rebuilt, NSC will create the documentation for that role / permission list within one month of its migration to production by System Computing Services.**
- **iNtegrate co-project leads Brian Chongtai and Andrea Martin will lead and facilitate the efforts above in coordination with the functional leads from Admissions, Advising, Financial Aid, Student Records, and Student Financials.**

Prevention & Monitoring
Once established, NSC will routinely document and update narrative descriptions for roles and permission lists as job functions evolve and change.

Follow-Up: NSC's Director of Information Technology, Brian Chongtai, has taken responsibility for this item. NSC is working with System Computing Services and the other Shared Instance institutions. Efforts are ongoing but will require additional time since total resolution is not merely an NSC issue. The completion date is September 2014.

ROLE AND PERMISSION LIST USAGE AND DESIGN PHILOSOPHY

Security design is an important part of the implementation of any system. Since this is a new system that will likely be in use for the foreseeable future, the design foundation is critical to long-term ease of use, maintenance and proper security functioning. There are competing objectives in the design of roles and permission lists with the tradeoffs being in scalability, flexibility and system performance. We evaluated role and permission list design against PeopleSoft's own recommendations on design and against published design criteria from authorities in the field. Design criteria from these sources indicate that, in general, roles should not overlap in their use of system features and similarly, permission lists should be mutually exclusive in their assignment of system pages. Further, the average user should have between 10-20 permission lists for optimal system performance. With these in mind, we noted the following concerns.

1. Our analysis of roles and permission lists noted that the implementation consultants did not follow the security design guidelines identified above. We found overlapping permission lists and roles as well as many users with substantially more permission lists than the guideline indicates.

We recommend that NSC work with SCS and their fellow institutions to evaluate the design of these components and begin a process of migrating roles and permission lists toward the design philosophy noted above.

Institution Response

NSC agrees with the recommendation.

Correction

As part of the Shared Instance, NSC will coordinate with SCS and the other NSHE institutions to implement a rebuild of security components in line with a new design philosophy.

System-Level Rebuild

SCS has recently developed a re-architecture of the shared instance security infrastructure and an execution plan for that re-architecture. Chris Piekarz, Senior Security Analyst for SCS, presented this plan on May 23rd, 2013. Mr. Piekarz has also shared his ideas for the new design philosophy with Grant Dintiman, NSHE Internal Auditor. Mr. Dintiman is in agreement with the execution of a plan around this philosophy.

Since the rebuilding of the shared instance security infrastructure represents a significant commitment of resources, the plan was reviewed by the iSIA with approval given to proceed in order to comply with this audit finding.

NSC Migration to the Shared Instance Design Philosophy

As the new roles and permission lists are developed by SCS, NSC will assist in testing and developing narratives as described in audit item number one. This will be completed by iNtegrate co-project leads Brian Chongtai and Andrea Martin with functional leads from Admissions, Advising, Financial Aid, Student Records, and Student Financials. Migration to the Shared Instance design philosophy will be accomplished as follows:

- **If it is found the new roles and permission lists meet its security needs, NSC will replace its current security with that developed for the shared version.**

- **Where it is found the shared version does not match its needs, NSC will build new roles and permission lists that adhere to the shared instance design philosophy.**

Follow-Up/Prevention & Monitoring: **NSC's Director of Information Technology, Brian Chongtai, has taken responsibility for this item. NSC is working with System Computing Services and the other Shared Instance institutions. Efforts are ongoing but will require additional time since total resolution is not merely an NSC issue. The completion date is June 2014.**

2. We noted one NSC specific role and 5 shared instance roles not assigned to any user profiles. There were no unassigned permission lists. Unused roles and/or permission lists obfuscate the security picture because it cannot be determined that they are not used or are invalid without research.

   We recommend that NSC work with SCS and their fellow institutions and evaluate unassigned roles to determine their need and eliminate any that are not necessary.

Institution Response

NSC agrees with this recommendation.

Correction
NSC has evaluated the one unassigned role as suggested by the auditor and has requested from SCS that it be removed. Review of unnecessary shared instance roles will occur during the System-level re-architecture of the shared instance security infrastructure.

Prevention & Monitoring
NSC will actively monitor institution specific roles and permission lists during security changes to ensure that unused roles and/or permission lists are eliminated if they are no longer deemed necessary.

Follow-Up: **NSC's Director of Information Technology, Brian Chongtai, has taken responsibility for this item. The recommendation has been fully implemented. Mr. Chongtai and his staff have implemented a proactive process whereby all roles and permission lists are regularly monitored and updated. Appropriate changes are being made in a timely and consistent manner.**
NSC respectfully requests that this item be closed.

SENSITIVE DATA ACCESS

We evaluated user access to 83 different pages that were deemed to contain sensitive data across the main functional areas of the PeopleSoft Campus Solutions system. These areas deal with financial aid, student admissions and records, student financials, academic advising and outreach. We compared the list of departmental employees to the list of employees with access according to our queries of the PeopleSoft system. We asked the department heads to evaluate non-departmental users with access rights in their functional area. Users with access rights in excess of what they should have are considered over provisioned. We noted the following:

1. Fifty two individuals were over provisioned with access to Student Records (34) and Registrar data (18). Sixty three individuals were over provisioned with access to Financial Aid data. Twenty four individuals were over provisioned with access to Academic Advising data. Four individuals were over provisioned with access to Student Financial data.

We recommend that NSC adjust these users as necessary and conduct regular reviews of user roles to ensure role assignments are appropriate.

Institution Response

NSC agrees with this recommendation.

Correction
iNtegrate co-project leads Brian Chongtai and Andrea Martin have met with each functional area to review security and completed adjusting security access as needed for Admissions, Academic Advising, Financial Aid, Student Financials, and Student Records.

Prevention & Monitoring
Within six months after the completion of the System-level security infrastructure re-architecture, iNtegrate co-project leads Brian Chongtai and Andrea Martin will work with each functional lead to develop a standardized set of security roles to

apply to defined positions within the institution. If, during a security request, a role is requested that falls outside of the standardized set, approvals will be required of the respective functional area prior to that security being granted. Documentation of these exceptions will be maintained by the NSC security coordinator.

<u>Follow-Up:</u> NSC's Director of Information Technology, Brian Chongtai, has taken responsibility for this item. The recommendation has been fully implemented. Mr. Chongtai and his staff have established a standardized set of security roles and applied them to defined positions within the institution. An approved process to address requests that fall outside of this set has been developed and implemented, and appropriate documentation will be maintained in Mr. Chongtai's office.

NSC respectfully requests that this item be closed.

We took a more detailed look at Social Security Number (SSN) and Date of Birth (DOB) data due to their increased sensitivity. PeopleSoft provides the capability to mask SSN and the birth year in DOB on selected high use screens, however there are many more screens that do not mask the data. We observed the following issues.

1. Approximately 250 individuals have unintended access to SSN data through access to screens with unmasked SSN data.
2. Even though the option exists to mask the birth year on selected high use screens, that option has not been implemented.

We recommend that NSC evaluate users with access to unmasked SSN data and ensure that they have a job related need for such access. Further, we suggest that NSC work with other institutions in the shared instance and consider masking birth year on the high use screens.

Institution Response

NSC agrees with this recommendation.

<u>Correction</u>
NSC values the trust placed in us by our students, faculty, and staff to protect Personally Identifiable Information (PII). We will honor that trust by restricting

access to PII except in those cases where it is deemed necessary to serve our constituents.

Masking Social Security Numbers

Masking of SSN is done at the system level. Currently, PeopleSoft's delivered masking mechanism is used on only two pages, RELATIONSHIPS and SCC_BIO_DEMO_PERS. Further masking of additional pages can only be accomplished by a modification. A modification is a technical term to describe programming changes at the system level. These typically require work by SCS and outside consultants. The delivered masking currently masks SSN only on the Search/Match page, with the default being to mask SSN for everyone on this page. To see an unmasked SSN, a person must be specifically provided with an additional role.

NSC Review of Unmasked SSN Access

iNtegrate co-project leads Brian Chongtai and Andrea Martin have evaluated users with access to unmasked Social Security Number data and examined whether there was a job-related need to see this information. There are a limited number of users who have a job-related need to see unmasked SSN and all other users not requiring this level of access were removed prior to the end of December 2013.

Masking Year in Date of Birth

Chris Piekarz, SCS Senior Security Analyst, has brought the issue of using the delivered masking mechanism for birth year on high use screens to the attention of Ginger Holladay-Houston, SCS Director of Information and Application Services. Consequently, on May 30th, 2013 SCS applied a mask in PeopleSoft for the year portion of date of birth (DOB) on the Search/Match page.

Prevention & Monitoring

With the automatic masking of both SSN and DOB provided through system-level security NSC can now monitor and grant specific access to those individuals who require this access for job-related functions. For all PeopleSoft security requests, application coordinators now review, document, and approve requests for access to unmasked SSN or DOB data.

Follow-Up: NSC's Director of Information Technology, Brian Chongtai, has taken responsibility for this item. NSC is now monitoring access to sensitive student data and provides specific access only to those employees whose job-related duties require it. There has been established a formal process to request, review and approve all such requests, and a regular review of individuals with such access has been implemented.

NSC respectfully requests that this item be closed.

STUDENT ADMINISTRATION and CONTRIBUTOR RELATIONS (SACR) SECURITY

The community and state colleges utilize a single shared database for their implementation of PeopleSoft Campus Solutions. Each institution needs to maintain some separation of their data from the other institutions and this is partially done with a host of parameters that are defined through SACR security tables and settings. SACR parameters are defined for an individual and thus restrict data on some pages by user and not by the user's assigned roles. For example, institution is one SACR parameter, so if an individual is assigned the NSC01 institution code, in general, they can only access NSC records and not other institutions in the database. We noted the following issues with SACR settings.

1. SACR parameters had not been properly implemented at NSC and other institutions to prevent cross institution grade and enrollment changes.

We recommend that NSC work with SCS to research and implement SACR parameters and settings to prevent cross institution data changes.

Institution Response

NSC agrees with this recommendation.

Correction
iNtegrate functional project lead Andrea Martin has worked with SCS to research and implement SACR security parameters and settings to prevent cross institution grade and enrollment changes. This effort was completed on May 7th, 2013.

Prevention & Monitoring
With the new SACR security parameters and settings in place, grade and enrollment changes by other shared instance institutions are no longer possible to perform.

Follow-Up: NSC's Director of Information Technology, Brian Chongtai, has taken responsibility for this item. The recently established SACR security parameters and

settings are in place and are controlling the integrity of NSC student records. Mr. Chongtai and his staff continue to monitor and manage this area in a proactive manner and are confident that the matter is totally resolved.

NSC respectfully requests that this item be closed.

The Internal Audit Department would like to thank the Information Technology Services staff and other college employees for their cooperation and assistance during this review.

Reno, Nevada
May 22, 2013

SIGNATURE ON FILE
Grant Dintiman
IT Auditor

Sandra K Cardinal
Sandra K. Cardinal
Assistant Vice Chancellor for Internal Audit

NEVADA STATE
COLLEGE

January 14, 2014

Mr. Scott Anderson
Internal Audit Manager
Nevada System of Higher Education
2601 Enterprise Road
Reno, Nevada 89512

RE: Nevada State College Sponsored PeopleSoft Security Audit February 1, 2013 – May 30, 2013

Dear Scott:

Attached are NSC's follow-up responses to the findings detailed in the above-mentioned audit.

<u>AUDIT</u>: Nevada State College PeopleSoft Security Audit

<u>AUDIT PERIOD</u>: February 1, 2013 – May 30, 2013

<u>RECOMMENDATIONS</u>: 6

<u>COMPLETE IMPLEMENTATION OF RECOMMENDATIONS</u>: 4

<u>IMPLEMENTATION OF RECOMMENDATIONS IN PROGRESS</u>: 2

NBR.	RECOMMENDATION	AGREE	IMPLEMENTED
1.	Narrative Description	Yes	Ongoing efforts with SCS and other institutions continue. Expected completion is September 2014.
2.	Security Design	Yes	Ongoing efforts with SCS and other institutions continue. Expected completion is June 2014.

3.	Unassigned Roles	Yes	Yes
4.	Security Access	Yes	Yes
5.	SSN Masking	Yes	Yes
6.	SACR Parameters	Yes	Yes

Thank you and your staff for your continued assistance and for all of the efforts of your staff.

Sincerely,

Buster

Harry E. Neel, Jr.
Senior Vice President for Finance and Administration

cc: Brian Chongtai
Andrea Martin
Kevin Butler
Grant Dintiman