SENSITIVE DATA SECURITY AND PROTECTION

SYSTEMWIDE

Audit Report 11-56
June 12, 2012

Members, Committee on Audit

Henry Mendoza, Chair
William Hauck   Steven M. Glazer
Glen O. Toney

Staff

University Auditor: Larry Mandel
Senior Director: Michael Caldera
IT Audit Manager: Greg Dove
Senior Auditor: Gordon Eng

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY
# CONTENTS

Executive Summary .......................................................................................................................... 1

Introduction ......................................................................................................................................... 3  
  Background .................................................................................................................................... 3  
  Purpose .......................................................................................................................................... 4  
  Scope and Methodology .................................................................................................................. 5

## OBSERVATIONS, RECOMMENDATIONS,  
AND MANAGEMENT RESPONSES

Information Security Governance ........................................................................................................ 6

Information Security Awareness Training........................................................................................... 7

Network Security .................................................................................................................................. 8  
  Data Leakage .................................................................................................................................. 8  
  Unsecure Workstations ..................................................................................................................... 9

Application System Access .................................................................................................................. 10
APPENDICES

APPENDIX A: Personnel Contacted
APPENDIX B: Management Response
APPENDIX C: Chancellor’s Acceptance

ABBREVIATIONS

CO  Chancellor’s Office
CSU  California State University
CIO  Chief Information Officer
FERPA Family Educational Rights and Privacy Act
ISO  Information Security Officer
IT  Information Technology
ITS  Information Technology Services
ICSUAM Integrated California State University Administrative Manual
EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor during the last quarter of 2010, the Board of Trustees, at its January 2011 meeting, directed that Sensitive Data Security and Protection be reviewed. The Office of the University Auditor had previously reviewed some aspects of sensitive data in the 2008 and 2009 audits of Information Security.

We visited six campuses from April 18, 2011, through December 9, 2011, and audited the procedures in effect at that time. Campus-specific findings and recommendations have been discussed and reported individually.

Our study and evaluation revealed certain conditions that, in our opinion, would result in inappropriate access or disclosure of sensitive data if not corrected. Specifically, the campuses had not implemented adequate controls over the following areas: security governance, network security, awareness training, and application access. These conditions, along with other weaknesses, are described in the executive summary and body of this report. In our opinion, due to the effect of the weaknesses described above, the operational and administrative controls over sensitive data in effect as of December 9, 2011, taken as a whole, were not sufficient to meet the objectives stated in the “Purpose” section of this report.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

Our audit did not examine all controls over sensitive data, but was designed to assess management controls, increase awareness of the topic, and assess regulatory compliance for significant sensitive data categories that are prevalent in the California State University environment.

The following summary provides management with an overview of conditions requiring attention. Areas of review not mentioned in this section were found to be satisfactory. Numbers in brackets [ ] refer to page numbers in the report.

INFORMATION SECURITY GOVERNANCE [6]

The organizational structure and general oversight of the campus information security function did not provide consistent executive level support for ensuring that security initiatives were effectively implemented throughout the campus, and broad inconsistencies and omissions were identified within the various information security programs.

INFORMATION SECURITY AWARENESS TRAINING [7]

The online security awareness training program had not been updated to maintain relevance with changing security threats and campus security concerns.
NETWORK SECURITY [8]

Campuses had not adequately addressed the risk of protected data being transmitted in an unprotected format or stored on unsecured media devices. In addition, sensitive data stored in PeopleSoft could be accessed from non-campus-owned workstations that were not secure or reliable.

APPLICATION SYSTEM ACCESS [10]

Most faculty were designated as advisors at every campus visited, which in combination with the “drop in advising” function, allowed all faculty unlimited access to view any student’s grades at any time.
INTRODUCTION

BACKGROUND

Integrated California State University Administrative Manual (ICSUAM) §8000.0, Information Security Policy, dated April 19, 2010, represents the most recent and specific guidance to campuses regarding the security and protection of sensitive data. It provides direction for managing and protecting the confidentiality, integrity, and availability of California State University (CSU) information assets and defines the organizational scope of information security throughout the system.

The policy states that the Board of Trustees is responsible for protecting the confidentiality, integrity, and availability of CSU information assets. Unauthorized modification, deletion, or disclosure of information assets can compromise the mission of the CSU, violate individual privacy rights, and possibly constitute a criminal act.

According to ICSUAM §8000.0, it is the collective responsibility of all users to ensure:

- The confidentiality of information that the CSU must protect from unauthorized access.
- The integrity and availability of information stored on or processed by CSU information systems.
- Compliance with applicable laws, regulations, and CSU or campus policies governing information security and privacy protection.

The policy further states that auxiliary organizations, external businesses, and organizations that use campus information assets must also follow the CSU Information Security Policy.

State Administrative Manual §5300 defines information security as the protection of information and information systems and equipment from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction. Pursuant to Government Code §11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, procedures, and filing requirements issued by the Office of Information Security and Privacy Protection in the California Office of Information Security.

At the CSU campuses, the information security officer has overall responsibility for the security and protection of sensitive data, which extends to all campus departments, colleges, and auxiliary organizations.
Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration and control of sensitive data; to determine the adequacy of controls over the related processes; and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the overall audit objective, specific goals included determining whether:

- Certain essential administrative and managerial internal controls are in place, including delegations of authority and responsibility, oversight committees, executive-level reporting, and documented policies and procedures.
- A management framework is established to initiate and control the implementation of information security within the organization, and management direction and support for information security is communicated in accordance with business requirements and relevant laws and regulations.
- All assets are accounted for and have a nominated owner/custodian who is responsible for achieving and maintaining appropriate protection of organizational assets, and information is appropriately classified to indicate the expected degree of protection.
- Security responsibilities are addressed with employees prior to the start of employment so that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work.
- Responsibilities and procedures for the management of information processing and service delivery are defined, and technical security controls are integrated within systems and networks.
- Access rights to systems, applications, and business processes surrounding sensitive data are controlled by means of user identification and authentication, based on business and security requirements.
- Formal event reporting and escalation procedures are in place for information security events and weaknesses, and communication is consistent and effective, allowing for timely corrective action.
- The information systems’ design, configuration, operation, use, and management are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.
- Contractual language addressing a third party’s responsibility for protecting sensitive data is appropriate.
SCOPE AND METHODOLOGY

The proposed scope of the audit, as presented in Action Item, Agenda Item 2 of the January 25 and 26, 2011, meeting of the Committee on Audit, stated that sensitive data security and protection would include review and compliance with Trustee policy, federal and state directives, and campus policies and procedures; procedures for handling confidential information; communication and employee training; encryption; tracking and monitoring of access to sensitive data; and retention practices for key records. If the sensitive data is maintained by a third party, we would review the involvement of campus information security personnel in the decision process; documentation of campus expectations for handling and securing the data; contract language covering security expectations; and monitoring of third-party performance.

Our study and evaluation were conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors and included the audit tests we considered necessary in determining that operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the administrative, compliance, operational, and technical controls over the security and protection of sensitive data. Specifically, we reviewed and tested:

- Information security policies and procedures.
- Information security organizational structure and management framework.
- Information asset management accountability and classification.
- Human resources security responsibilities.
- Administrative and technical security procedures.
- Access and configuration controls over networks, systems, applications, business processes, and data.
- Incident response, escalation, and reporting procedures.
- Compliance with relevant statutory, regulatory, and contractual security requirements.
- Third-party contractual language regarding handling of sensitive data.

Our testing and methodology was designed to provide a managerial level review of key security practices over sensitive data. Our review did not examine all categories of sensitive data; selected emerging technologies were excluded from the scope of the review. Our testing approach was designed to provide a view of the security used to protect only key computing and business processes.

During the course of the audit, we visited six campuses: Fullerton, Los Angeles, Sacramento, San Diego, San Luis Obispo, and Sonoma. We interviewed campus personnel and audited procedures in effect at the time of the audit.
OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

INFORMATION SECURITY GOVERNANCE

The organizational structure and general oversight of the campus information security function did not provide consistent executive level support for ensuring that security initiatives were effectively implemented throughout the campuses, and broad inconsistencies and omissions were identified within the various information security programs.

We found several omissions and irregularities at the campuses reviewed, including the following:

- Campuses did not always have a process to identify and report all security incidents, especially when computers were procured and maintained outside of the campus information technology department.

- Security initiatives were not always consistently reported to campus executive management, and information security reporting did not always contain sufficient information to assist executive decision-making.

- The security of sensitive data stored on paper documents was not assessed by the information security department at some campuses.

- Campus-initiated risk assessments and gap analyses were not always considered in security planning.

- Background checks for student assistants with access to level one sensitive data were not performed at some campuses.

- Faculty employees had not completed security training at some campuses.

- Security initiatives identified in prior audits had not been completed at some campuses. Specifically, Internet-accessible web servers had not been placed on a separate network segment from other internal production servers.

- The system access evaluation process did not include a review of accessibility to student grades or Social Security numbers at some campuses, and existing access was not always appropriate.

Integrated California State University Administrative Manual (ICSUAM) §8015, Organizing Information Security, dated April 19, 2010, states that each campus must develop, implement, and document the organizational structure that supports the campus’ information security program. The organizational structure must define the functions, relationships, responsibilities, and authorities of individuals or committees that support the campus information security program.

The campus chief information officers (CIO) stated that the campuses considered their organizational reporting structure to be consistent with that of the chancellor’s office (CO), but acknowledged that
appropriate procedures to keep the campus presidents and cabinets informed and involved in information security were not as robust as they could be. The systemwide information security officer (ISO) stated that the CSU information security policy had been recently implemented but that the specific standards were still in draft form.

Lack of appropriate oversight for the information security function could create conflicting priorities, lead to suppressed discoveries, and result in inadequate or conflicting budgetary decisions for projects.

**Recommendation 1**

We recommend that the CO review information security governance and security reporting structures at every campus to ensure that information security initiatives are brought to the president’s cabinet regularly so that vice presidents for each division are aware of and supportive of the implementation of information security initiatives. We also recommend that specific guidance for the scope and breadth of the information security program be provided to the campuses.

**Management Response**

We concur. The CO will review the information security governance and security reporting structures at every campus. We will recommend a reporting format, which will ensure that information security initiatives are brought to the president’s cabinet to ensure awareness and to garner support for the implementation of information security initiatives. Additionally, the CO will provide campuses an information security program, which will include specific scope and guidance.

Target completion date: December 31, 2012

**INFORMATION SECURITY AWARENESS TRAINING**

The online security awareness training program had not been updated to maintain relevance with changing security threats and campus security concerns.

ICSUAM §8035.100, *Information Security Awareness and Training*, dated April 19, 2010, states that each campus must implement a program for providing appropriate information security awareness and training to employees appropriate to their access to campus information assets. The campus information security awareness program must promote campus strategies for protecting information assets containing protected data. All employees with access to protected data and information assets must participate in appropriate information security awareness training. When appropriate, information security training must be provided to individuals whose job functions require specialized skill or knowledge in information security.

The CO ISO stated that the online security training program was to be refreshed on an as-needed basis, but it had not been revised since the original implementation.
Failure to provide employees with relevant information security awareness training increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.

**Recommendation 2**

We recommend that the CO regularly update the online security awareness training program to ensure that the program remains relevant to the current information security risk environment.

**Management Response**

We concur. The CO will regularly update the online security awareness training program to ensure that the content remains relevant and current to our systemwide risk environment.

Target completion date: November 30, 2012

**NETWORK SECURITY**

**DATA LEAKAGE**

Campuses had not adequately addressed the risk of protected data being transmitted in an unprotected format or stored on unsecured media devices.

We found that the campuses did not have methods to prevent data from being sent from the internal campus networks in an unprotected format or from being stored on alternative media devices that were not appropriately secured, such as iPhones or USB drives.

ICSUAM §8010.00, *Establishing an Information Security Program*, dated April 19, 2010, states in part that the campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The program should, among other things: a) provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g., paper or electronic); and b) develop risk management strategies to identify and mitigate threats and vulnerabilities.

The campus CIOs stated that it is expensive to prevent sensitive data from leaking to other devices and storage media, and they had been focused on first ensuring that such data was protected internally.

Failure to prevent sensitive data from being sent externally in an unprotected format, or from being copied to and stored on unprotected devices, increases the risk of mismanagement of protected data, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.
Recommendation 3

We recommend that the CO assess the risk of accidental exposure of sensitive data and evaluate methods that might ensure that sensitive data is protected from being transmitted in an unprotected format or stored on unsecured devices.

Management Response

We concur. The CO will assess the risk of accidental exposure of sensitive data and evaluate methods that might ensure that sensitive data are protected from being transmitted in an unprotected format or stored on unsecured devices.

Target completion date: December 31, 2012

UNSECURE WORKSTATIONS

Sensitive data stored in PeopleSoft could be accessed from non-campus-owned workstations that were not secure or reliable.

We found that the methods used by campuses to provide access to the PeopleSoft system did not ensure that such access originated only from secure computers that had not been compromised.

ICSUAM §8010.00, Establishing an Information Security Program, dated April 19, 2010, states in part that the campus information security program must implement a risk-based, layered approach that uses preventative, detective, and corrective controls sufficient to provide an acceptable level of information security and must be reviewed at least annually. The program should, among other things, a) provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held or transmitted (e.g., paper or electronic); and b) develop risk management strategies to identify and mitigate threats and vulnerabilities.

The campus CIOs stated that one of the objectives of PeopleSoft was to provide access to the systems anywhere and anytime, to support student and employee self-service, and that security training should minimize the possibility of employee login credentials being compromised by access from unsecured computers.

Lack of adequate security over the individual workstations used to access CSU systems could lead to compromise of employee authentication credentials, which increases campus exposure to security breaches and could compromise compliance with statutory information security requirements.

Recommendation 4

We recommend that the CO examine security solutions that would help prevent employees from accessing the CSU systems at unprotected and unsecured workstations.
Management Response

We concur. The CO will evaluate security solutions to help prevent employees from accessing the CSU systems at unprotected and unsecured workstations.

Target completion date: December 31, 2012

APPLICATION SYSTEM ACCESS

Most faculty were designated as advisors at every campus visited, which in combination with the “drop in advising” function, allowed all faculty unlimited access to view any student’s grades at any time.

ICSUAM §8060, Access Control, dated April 19, 2010, states that access to campus information assets containing protected data as defined in the CSU Data Classification Standard may be provided only to those having a need for specific access in order to accomplish an authorized task.

The campus provosts stated that they were unaware of any specific guidance limiting access by faculty with advising responsibility; that all faculty were given Family Educational Rights and Privacy Act (FERPA) training; and that broad advising capability had been granted to better assist students with advice toward completing degree programs.

Improper segregation of employee access could lead to unauthorized or inappropriate exposure to sensitive data, and can adversely affect campus compliance with existing regulations regarding protection of such data.

Recommendation 5

We recommend that the CO reassess access privileges assigned to faculty and staff with advising responsibility and limit access to only those student grades that are required to provide specific advice. We also recommend that the CO expand the annual evaluation process of system access to include appropriateness of advising capabilities.

Management Response

The most recent upgrade of Peoplesoft (Version 9.0) allows campuses to utilize greater security controls in providing access to student academic records for the purposes of academic advisement. Campuses should continue to include information regarding FERPA compliance to individuals providing academic advisement. Further, campuses should develop data security policies that appropriately limit access to student records. Unlimited access should be parsed only as required. Full-time faculty and professional staff may be granted access to advising as necessary. Part-time faculty, graduate assistants, and other staff should be permitted advising capabilities only by written approval of department chairs. All approvals should be subject to annual review and review based upon changes in employment status. Campuses are to confirm with the chancellor’s office before the
end of the calendar year that modifications to campus student systems necessary to implement these policy changes have been completed. The CO will communicate these expectations to the campuses.

Target completion date: September 1, 2012
### APPENDIX A: PERSONNEL CONTACTED

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Office of the Chancellor</strong></td>
<td></td>
</tr>
<tr>
<td>Benjamin F. Quillian</td>
<td>Executive Vice Chancellor and Chief Financial Officer</td>
</tr>
<tr>
<td>Ephraim P. Smith</td>
<td>Executive Vice Chancellor and Chief Academic Officer</td>
</tr>
<tr>
<td>Bruce Briggs</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>Lori Erdman</td>
<td>Chief of Staff, Business and Finance (At time of review)</td>
</tr>
<tr>
<td>Christine Helwick</td>
<td>General Counsel</td>
</tr>
<tr>
<td>William Perry</td>
<td>Information Security Officer</td>
</tr>
<tr>
<td>Sabrina Sanders</td>
<td>Assistant Director, Student Program</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>California State University, Fullerton</strong></td>
<td></td>
</tr>
<tr>
<td>Mildred Garcia</td>
<td>President (Currently)</td>
</tr>
<tr>
<td>Milton A. Gordon</td>
<td>President (At time of review)</td>
</tr>
<tr>
<td>Silas Abrego</td>
<td>Vice President for Student Affairs</td>
</tr>
<tr>
<td>Ryan Alcantara</td>
<td>Associate Vice President for Student Affairs</td>
</tr>
<tr>
<td>Amy Alspaugh</td>
<td>Assistant to the Associate Vice President of Academic Affairs</td>
</tr>
<tr>
<td>Welson Badal</td>
<td>Director, Administration and Finance Technology (IT)</td>
</tr>
<tr>
<td>William Barrett</td>
<td>Interim Vice President for Administration and Finance/Chief Financial Officer</td>
</tr>
<tr>
<td>John Beisner</td>
<td>Director, University Risk Management</td>
</tr>
<tr>
<td>Kerry Boyer</td>
<td>Director, IT Information Security</td>
</tr>
<tr>
<td>Pat Carroll</td>
<td>Executive Assistant to the President</td>
</tr>
<tr>
<td>Amir Dabirian</td>
<td>Vice President, IT</td>
</tr>
<tr>
<td>Nancy Dority</td>
<td>Assistant Vice President of Enrollment Services</td>
</tr>
<tr>
<td>Naomi Goodwin</td>
<td>Assistant Vice President for Administration and Finance</td>
</tr>
<tr>
<td>Willie Hagan</td>
<td>Vice President, Administration and Finance/Chief Financial Officer</td>
</tr>
<tr>
<td>(At time of review)</td>
<td></td>
</tr>
<tr>
<td>Bahram Hatefi</td>
<td>Director of Internal Audit (At time of review)</td>
</tr>
<tr>
<td>Rommel Hildago</td>
<td>Assistant Vice Director for IT and Senior Director for Infrastructure Services</td>
</tr>
<tr>
<td>Elizabeth Housewright</td>
<td>Associate University Librarian</td>
</tr>
<tr>
<td>Terry Jarmon</td>
<td>IT Asset Security and Reprographics Manager</td>
</tr>
<tr>
<td>Denise Johnson</td>
<td>Director, Human Resource Operations</td>
</tr>
<tr>
<td>Chris Manriquez</td>
<td>Associate Vice President, IT</td>
</tr>
<tr>
<td>Tariq Marji</td>
<td>Chief Financial Officer, CSU, Fullerton, Auxiliary Services Corporation</td>
</tr>
<tr>
<td>Mary Jo Medyn</td>
<td>Assistant to Vice President of Academic Affairs</td>
</tr>
<tr>
<td>Ron Morris</td>
<td>IT Systems Administrator, Associated Students California State University, Fullerton, Inc.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Frank Mumford</td>
<td>Executive Director, CSU, Fullerton, Auxiliary Services Corporation</td>
</tr>
<tr>
<td>Steve Murray</td>
<td>Acting Vice President of Academic Affairs</td>
</tr>
<tr>
<td>Willie Peng</td>
<td>Assistant Director, Infrastructure Services</td>
</tr>
<tr>
<td>Blanca Rodriguez</td>
<td>Payroll Director</td>
</tr>
<tr>
<td>Fred Sanchez</td>
<td>Executive Director, Associated Students California State University, Fullerton, Inc.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Ira Unterman</td>
<td>Chief Financial Officer, CSU Fullerton Philanthropic Foundation and Executive Director for Advancement Operations</td>
</tr>
<tr>
<td>California State University, Los Angeles</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>James M. Rosser</td>
<td>President</td>
</tr>
<tr>
<td>Joseph Aguirre</td>
<td>Executive Director, University-Student Union</td>
</tr>
<tr>
<td>Van Andranigian</td>
<td>IT Coordinator, Administrative Technology</td>
</tr>
<tr>
<td>Kevin Brady</td>
<td>Director, Risk Management and Environmental, Health and Safety</td>
</tr>
<tr>
<td>Lisa Chavez</td>
<td>Vice President for Administration and Chief Financial Officer</td>
</tr>
<tr>
<td>Annie Ekshian</td>
<td>Supervisor, Property Management Office</td>
</tr>
<tr>
<td>Gay Galgano</td>
<td>Director, Payroll Services</td>
</tr>
<tr>
<td>Jose Gomez</td>
<td>Associate Vice President, Administration and Finance</td>
</tr>
<tr>
<td>Tanya Ho</td>
<td>University Internal Auditor</td>
</tr>
<tr>
<td>Robert Hoffmann</td>
<td>Assistant Director, Operations and Access Management, Information Technology Services (ITS)</td>
</tr>
<tr>
<td>Steve Jones</td>
<td>Associate Dean, Undergraduate Studies</td>
</tr>
<tr>
<td>Tammie Leung</td>
<td>Director of Outreach and Recruitment, Office of Admissions and Recruitment</td>
</tr>
<tr>
<td>Vince Lopez</td>
<td>Director, Office of Admissions and Recruitment</td>
</tr>
<tr>
<td>Karen Melick</td>
<td>Director, Administrative Technology</td>
</tr>
<tr>
<td>Sheryl Okuno</td>
<td>Director, IT Security and Compliance</td>
</tr>
<tr>
<td>Rhoda Posey</td>
<td>Associate Director, Center for Student Financial Aid</td>
</tr>
<tr>
<td>Peter Quan</td>
<td>Vice President and Chief Information Officer (CIO), ITS</td>
</tr>
<tr>
<td>Chris Rapp</td>
<td>Director, ITS IT Infrastructure Services</td>
</tr>
<tr>
<td>Salvador Rodriguez</td>
<td>Senior Internal Auditor</td>
</tr>
<tr>
<td>Lisa Sanchez</td>
<td>Assistant Vice President, Human Resources Management</td>
</tr>
<tr>
<td>Dan Thomas</td>
<td>Risk Management Analyst, Environmental, Health and Safety Office, Division of Administration and Finance</td>
</tr>
<tr>
<td>Rowena Tran</td>
<td>Assistant Director, University-Student Union</td>
</tr>
<tr>
<td>Susie Varela</td>
<td>Director, Human Resource Management</td>
</tr>
<tr>
<td>Intef Weser</td>
<td>Executive Director, Associated Students, Incorporated</td>
</tr>
<tr>
<td>Joan Woosley</td>
<td>Director of Recruitment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>California State University, Sacramento</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Alexander Gonzalez</td>
<td>President</td>
</tr>
<tr>
<td>Tejeshwar Chowdary</td>
<td>Director and Information Technology Coordinator, Student Affairs</td>
</tr>
<tr>
<td>Mike Christensen</td>
<td>Associate Vice President of Risk Management Services</td>
</tr>
<tr>
<td>Leslie Davis</td>
<td>Executive Director, University Union and The Well</td>
</tr>
<tr>
<td>Emiliano Diaz</td>
<td>Director, Admissions and Outreach</td>
</tr>
<tr>
<td>Jill Farrell</td>
<td>Business Office Manager, University Union and The Well</td>
</tr>
<tr>
<td>Dennis Geyer</td>
<td>University Registrar</td>
</tr>
<tr>
<td>Larry Gilbert</td>
<td>Vice President and CIO</td>
</tr>
<tr>
<td>Yavette Hayward</td>
<td>Senior Management Auditor</td>
</tr>
<tr>
<td>Ming-Tung “Mike” Lee</td>
<td>Interim Vice President and Chief Financial Officer, Administration and Business Affairs</td>
</tr>
<tr>
<td>Dena Lemus</td>
<td>Admissions Counselor, Admissions and Outreach</td>
</tr>
<tr>
<td>Cindy Martinez</td>
<td>Enrollment Systems Analyst, Records and Campus Community</td>
</tr>
<tr>
<td>Lynn Maynard</td>
<td>Assistant Director of Financial Aid Systems Operations</td>
</tr>
<tr>
<td>Kathi McCoy</td>
<td>Director of Auditing Services (At time of review)</td>
</tr>
<tr>
<td>Ed Mills</td>
<td>Associate Vice President, Enrollment Services</td>
</tr>
</tbody>
</table>
APPENDIX A: PERSONNEL CONTACTED

California State University, Sacramento (cont.)

Mark Montalvo  Director of Finance and Administration, Associated Students
Jason Musselman  Network Security Analyst
Helen Norris  Associate Vice President, Administrative Computing Systems
Kristine Novak  Assistant Registrar
Andy Schloss  Director of Hardware and Software Support
Andrew Singletary  Information Technology Manager, University Union and The Well
Kirt Stout  Director of Risk Management and Business Continuity Planning
Elizabeth Sublett  Interim Associate Vice President, Human Resource Services
Gerald Tubo  Information Technology Manager, Associated Students of California State University, Sacramento
David Wagner  Vice President of Human Resources
Jeff Williams  Information Security Officer
Patricia Worley  Executive Director, Associated Students of California State University, Sacramento
Craig Yamamoto  Financial Aid Director

San Diego State University

Elliot Hirshman  President
Edith Benkov  Associate Vice President, Faculty Affairs
Scott Burns  Associate Vice President, Financial Operations
Mikhail Burstein  Director, Student Information Management System
Valerie Carter  Director, Audit and Tax
Bernice Casillas  Manager, Student Accounts and Cashiering
David Del Rio  Assistant Director, Business Services
Cathy Garcia  Manager, Contract and Procurement Management
Sandy Jorgensen-Funk  Director, Counseling and Psychological Services
Alicia Koukis  Assistant Director, Information Systems
Gene LeDuc  Information Technology Security Officer
Catherine Love  Assistant Director, Employment, Classification and Training Manager
Rich Pickett  Senior Director and CIO, Enterprise Technology Services
Kimberlee Reilly  Assistant Controller
Jessica Rentto  Interim Associate Vice President, Administration
Jennifer Rikard  Co-Coordinator of ASPIRE Program, Counseling and Psychological Services
John Ross  Academic Affairs Information Technology Coordinator
Sally Roush  Vice President, Business and Financial Affairs
Joanne Stroud  Administrative Manager, Student Health Services
Rayanne Williams  Registrar, Enrollment Services
Felecia Vlahos  Information Security Officer

California Polytechnic State University, San Luis Obispo

Jeffrey D. Armstrong  President
Donna Amos  Associate Director, Admissions, Recruitment, Financial Aid
Debbie Arseneau  Associate Registrar, Office of the Registrar
Marc Benadiba  Associate Director Payroll, Fiscal Services, Payroll Services
APPENDIX A: PERSONNEL CONTACTED

California Polytechnic State University, San Luis Obispo (cont.)

Chris Blackburn  Administrative Analyst, Human Resources
Marty Braggs  Director, Health and Counseling Services
Ed Bruns  Network Analyst, Network Administration, ITS
Chris Call  Information Security Coordinator, Administration and Finance
Anthony Colvard  Information Technology Consultant, Associated Students, Incorporated of California Polytechnic State University at San Luis Obispo

Ken Delmese  Property Clerk II, Fiscal Services, Property
Don Duke  Operating Systems Analyst, ITS, LAN Server Services
Julie Dupuy  Administrative Analyst, Academic Records, System Management
Brad Fely  Administrative Analyst, Office of the Registrar
Beth Gallagher  Executive Director, Human Resources
Mark Goble  Information Technology Consultant, Health and Counseling Services
Joyce Haretani  Associate Director, Human Resources
Larry Kelley  Vice President, Administration and Finance
Lois Kelly  Director of Financial Aid
Lorlie Leetham  Director of Fiscal Services, Administration and Finance
Scott Loosley  Associate Director for Operations, Facility Services
Dee Louie  Accountant II, Fiscal Services, Financial Reporting
Johanna Madjedi  Associate Vice Provost, ITS
Jim Maraviglia  Associate Vice Provost, Admissions, Recruitment, and Financial Aid
David Mason  Network Analyst, Documents and Technical Services
Ryan Matteson  Security and Architecture, Office of the CIO
Theresa May  Interim Director, Information Services Infrastructure, ITS
Mike Miller  Vice Provost for Information Services, CIO

Greg Porter  Operating Systems Analyst, Central Systems Administration, ITS
Rick Ramirez  Associate Vice President, Administration and Finance
Gage Sahl  Warehouse Worker, Facility Services, Moving and Surplus
Katy Schrempp  Administrative Analyst, Admissions, Recruitment, and Financial Aid
Lisa Shealy  Information Technology Consultant, Central Systems Administration, ITS

Cem Sunata  Registrar
Terry Vahey  Director, Administration and Finance Department Tech Services and Information Security Officer

Richard Walls  Interim Director Communication and Computing Services, ITS

Sonoma State University

Ruben Armiñana  President
Brian Biggs  Analyst/Programmer, IT
Barry Blackburn  Information Security Officer
Brent Boyer  Associate Director, Disability Services
Brandon Dudley  Director, Library Technology
Peter Flores  Common Management System Security Administrator
Laurence Furukawa-Schlereth  Vice President of Administration and Finance
Andru Luvisi  Operating System Security Specialist
Roger Mamer  Systems Specialist, Computer Sciences
Sonoma State University (cont.)
Robin Marshall          Director, Workstation Services and Security
Ruth McDonnell          Deputy Controller, Contracts and Procurement
Sally Sacchetto         Director of Faculty Personnel
Georgia Schwartz        Medical Director
Kathleen Spitzer        Managing Director, Employee Services
Jean Sugiyama           Network Analyst
Stephanie Thibault      Instructional Technology Technician, Biology
Jason Wenrick           Interim CIO
Lisa Wyatt              Director of Counseling, Psychological Services
MEMORANDUM

DATE: September 6, 2012

TO: Larry Mandel
    University Auditor

FROM: Benjamin F. Quillian
      Executive Vice Chancellor and
      Chief Financial Officer

Ephraim P. Smith
Executive Vice Chancellor and
Chief Academic Officer


In response to the "Incomplete Draft" report dated June 12, 2012, we are providing the enclosed revised management responses.

Should you have any questions, please feel free to contact either of us.

BFQ:mpr

Attachment

c: Bruce Briggs, Assistant Vice Chancellor and Chief Information Officer
   Eric Forbes, Assistant Vice Chancellor, Student Academic Support
   Nathan Evans, Director, Enrollment Management Services
   William Perry, Chief Information Management and Security Officer
SENSITIVE DATA SECURITY AND PROTECTION

SYSTEMWIDE

Audit Report 11-56

INFORMATION SECURITY GOVERNANCE

Recommendation 1

We recommend that the CO review information security governance and security reporting structures at every campus to ensure that information security initiatives are brought to the president’s cabinet regularly so that vice presidents for each division are aware of and supportive of the implementation of information security initiatives. We also recommend that specific guidance for the scope and breadth of the information security program be provided to the campuses.

Management Response

We concur. The CO will review the information security governance and security reporting structures at every campus. We will recommend a reporting format, which will ensure that information security initiatives are brought to the president’s cabinet to ensure awareness and to garner support for the implementation of information security initiatives. Additionally, the CO will provide campuses an information security program, which will include specific scope and guidance.

Target completion date: December 31, 2012

INFORMATION SECURITY AWARENESS TRAINING

Recommendation 2

We recommend that the CO regularly update the online security awareness training program to ensure that the program remains relevant to the current information security risk environment.

Management Response

We concur. The CO will regularly update the online security awareness training program to ensure that the content remains relevant and current to our systemwide risk environment.

Target completion date: November 30, 2012
NETWORK SECURITY

DATA LEAKAGE

Recommendation 3

We recommend that the CO assess the risk of accidental exposure of sensitive data and evaluate methods that might ensure that sensitive data is protected from being transmitted in an unprotected format or stored on unsecured devices.

Management Response

We concur. The CO will assess the risk of accidental exposure of sensitive data and evaluate methods that might ensure that sensitive data are protected from being transmitted in an unprotected format or stored on unsecured devices.

Target completion date: December 31, 2012

UNSECURE WORKSTATIONS

Recommendation 4

We recommend that the CO examine security solutions that would help prevent employees from accessing the CSU systems at unprotected and unsecured workstations.

Management Response

We concur. The CO will evaluate security solutions to help prevent employees from accessing the CSU systems at unprotected and unsecured workstations.

Target completion date: December 31, 2012

APPLICATION SYSTEM ACCESS

Recommendation 5

We recommend that the CO reassess access privileges assigned to faculty and staff with advising responsibility and limit access to only those student grades that are required to provide specific advice. We also recommend that the CO expand the annual evaluation process of system access to include appropriateness of advising capabilities.

Management Response

The most recent upgrade of Peoplesoft (Version 9.0) allows campuses to utilize greater security controls in providing access to student academic records for the purposes of academic advisement. Campuses should continue to include information regarding FERPA compliance to individuals providing academic advisement. Further, campuses should develop data security policies that
appropriately limit access to student records. Unlimited access should be parsed only as required. Full-time faculty and professional staff may be granted access to advising as necessary. Part-time faculty, graduate assistants, and other staff should be permitted advising capabilities only by written approval of department chairs. All approvals should be subject to annual review and review based upon changes in employment status. Campuses are to confirm with the Chancellor’s Office before the end of the calendar year that modifications to campus student systems necessary to implement these policy changes have been completed. The CO will communicate these expectations to the campuses.

Target completion date: September 1, 2012
September 14, 2012

MEMORANDUM

TO: Mr. Larry Mandel
   University Auditor

FROM: Charles B. Reed
       Chancellor

SUBJECT: Draft Final Report 11-56 on
         Sensitive Data Security and Protection, Systemwide

In response to your memorandum of September 14, 2012, I accept the response as submitted with the draft final report on Sensitive Data Security and Protection, Systemwide.

CBR/amd