

**AUXILIARY ORGANIZATIONS**  
**CALIFORNIA STATE UNIVERSITY,**  
**LONG BEACH**

**Audit Report 09-16**  
**November 12, 2009**

---

**Members, Committee on Audit**

Melinda Guzman, Chair  
Raymond W. Holdsworth, Vice Chair  
Herbert L. Carter Carol R. Chandler  
Kenneth Fong Margaret Fortune  
George G. Gowgani William Hauck  
Henry Mendoza

---

**Staff**

University Auditor: Larry Mandel  
Senior Director: Janice Mirza  
Audit Manager: Gary Miller  
Senior Auditors: Kwabena Boakye and Dominick Owens  
Internal Auditor: Caroline Lee

---

**BOARD OF TRUSTEES**  
**THE CALIFORNIA STATE UNIVERSITY**

---

## CONTENTS

Executive Summary .....	1
Introduction.....	6
Background .....	6
Purpose.....	7
Scope and Methodology .....	8

---

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

### **CAMPUS**

Information Technology .....	11
Protected Data Assessment.....	11
User Access Reviews.....	12
Information Security Training .....	13

### **CALIFORNIA STATE UNIVERSITY, LONG BEACH FOUNDATION**

Facilities Agreements .....	15
Operational Compliance .....	15
Cash Receipts and Handling.....	16
Property and Equipment .....	18
Trusts and Other Liabilities .....	20
Auxiliary Programs.....	21
Information Technology .....	24
Password and Data Security .....	24
System Backups .....	25
Environmental Controls .....	26
Disposition of Protected Data.....	27
Remote Server Access .....	28

### **FORTY-NINER SHOPS, INC**

Operating, Administrative and Facilities Agreements.....	30
Operational Compliance .....	32
Risk Management .....	32
Employees.....	32

---

CONTENTS

Segregation of Duties..... 33

Petty Cash and Change Funds ..... 34

    Petty Cash ..... 34

    Change Funds..... 35

Property and Equipment ..... 36

Information Technology ..... 37

    Password Security ..... 37

    System Backups ..... 38

    System Security and Environmental controls ..... 39

    Disposition of Protected Data ..... 40

    Data Confidentiality Forms ..... 41

**ASSOCIATED STUDENTS, CALIFORNIA STATE UNIVERSITY, LONG BEACH**

Operating and Administrative Agreements ..... 43

Segregation of Duties..... 44

Cash Receipts and Handling..... 45

Purchasing and Accounts Payable ..... 46

Property and Equipment ..... 48

Information Technology ..... 49

    Password and Data Security ..... 49

    System Backups ..... 51

    Vendor Master File ..... 52

## **APPENDICES**

APPENDIX A:	Personnel Contacted
APPENDIX B:	Statement of Internal Controls
APPENDIX C:	Campus Response
APPENDIX D:	Chancellor's Acceptance

---

## **ABBREVIATIONS**

A/R	Accounts Receivable
AS	Associated Students, California State University, Long Beach
CFO	Chief Financial Officer
CSU	California State University
CSULB	California State University, Long Beach
DMZ	Demilitarized Zone
EO	Executive Order
FASB	Financial Accounts Standards Board
Foundation	California State University, Long Beach Foundation
HR	Human Resources
OMB	Office of Management and Budget
RFIN	Resolution of the Committee on Finance
PCI DSS	Payment Card Industry Data Security Standard
Shops	Forty-Niner Shops, Inc.
Telnet	Telecommunication Network
VPN	Virtual Private Network

---

## EXECUTIVE SUMMARY

In July 1981, the Board of Trustee policy concerning auxiliary organizations was adopted in the Resolution of the Committee on Finance (RFIN) 7-81-4. Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, required that the Office of the University Auditor conduct internal compliance/internal control reviews of auxiliary organizations, and the Board of Trustees instructed that such reviews be conducted on a triennial basis pursuant to procedures established by the chancellor.

California State University, Long Beach (CSULB) management is responsible for establishing and maintaining an adequate system of internal compliance/internal control and assuring that each of its auxiliary organizations similarly establishes such a system. This responsibility, in accordance with California Code of Regulations, Title 5, Section 42402 et seq. and Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations et seq.*, includes requiring the documentation of internal control, communicating requirements to employees, and assuring that its system of internal compliance/internal control is functioning as prescribed. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of control procedures.

The objectives of a system of internal compliance/internal control are to provide management with reasonable, but not absolute, assurance that:

- ▶ Auxiliary operations are conducted in accordance with policies and procedures established in the State Administrative Manual, Education Code, Title 5, and Trustee policy.
- ▶ Assets are adequately safeguarded against loss from unauthorized use or disposition.
- ▶ Transactions are executed in accordance with management's authorization and recorded properly to permit the timely preparation of reliable financial statements.

We visited the CSULB campus and its auxiliary organizations from May 26, 2009, through June 26, 2009, and made a study and evaluation of the system of internal compliance/internal control in effect as of June 26, 2009. This report represents our triennial review.

Our study and evaluation at the *California State University, Long Beach Foundation* revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the auxiliary did not maintain adequate control over the following areas: cash receipts and handling, property and equipment, trusts and other liabilities, and information technology. These conditions, along with other weaknesses, are described in the executive summary and in the body of the report. In our opinion, except for the effect of the weaknesses described above, accounting and administrative control in effect as of June 26, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *Forty-Niner Shops, Inc.* revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the auxiliary did not maintain adequate control over the following areas: petty cash and change funds, property and equipment, and information technology. These conditions, along with other weaknesses, are described in the executive

summary and in the body of the report. In our opinion, except for the effect of the weaknesses described above, accounting and administrative control in effect as of June 26, 2009, taken as a whole, was sufficient to meet the objectives stated above.

Our study and evaluation at *Associated Students, California State University, Long Beach* revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the auxiliary did not maintain adequate control over property and equipment and information technology. These conditions, along with other weaknesses, are described in the executive summary and in the body of the report. In our opinion, except for the effect of the weaknesses described above, accounting and administrative control in effect as of June 26, 2009, taken as a whole, was sufficient to meet the objectives stated above.

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.

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

## **CAMPUS**

### **INFORMATION TECHNOLOGY [11]**

The California State University, Long Beach Foundation (Foundation), Forty-Niner Shops, Inc. (Shops) and Associated Students, California State University, Long Beach (AS) did not perform a periodic, detailed assessment and inventory of protected information residing on their systems, and the protected information was not classified into security levels. Further, the Foundation, Shops, and AS did not perform periodic, documented management reviews of user access privileges within all systems and applications containing protected data, and personnel with access to protected data were not required to complete information security awareness training.

## **CALIFORNIA STATE UNIVERSITY, LONG BEACH FOUNDATION**

### **FACILITIES AGREEMENTS [15]**

Certain use agreements between California State University, Long Beach Foundation (Foundation) and third parties did not include an indemnification provision to specifically indemnify the CSU Trustees, the campus, and the State of California.

## **OPERATIONAL COMPLIANCE [15]**

The Foundation had not developed a written risk management policy.

## **CASH RECEIPTS AND HANDLING [16]**

Foundation cash receipts were not always timely processed and adequately safeguarded.

## **PROPERTY AND EQUIPMENT [18]**

Foundation administration of the physical inventory process did not ensure current inventory procedures, clear definition and communications of roles and responsibilities, and prompt follow-up of missing assets. Further, an agreement with a third-party for inventory services did not include insurance and indemnification provisions.

## **TRUSTS AND OTHER LIABILITIES [20]**

Certain campus program revenues were inappropriately deposited to, and held in custody by, the Foundation.

## **AUXILIARY PROGRAMS [21]**

Foundation administration of sponsored programs did not ensure the completion and timely submission of program deliverables, completion of current conflict of interest forms, and a timely closeout process for grants and contracts.

## **INFORMATION TECHNOLOGY [24]**

Password controls and data security were not always adequate for Foundation systems, and backups for Foundation systems with protected data were not encrypted when stored locally or when in transit to the off-site storage facility managed by a third party. In addition, the Foundation server room had a water-sprinkler system, which is an inappropriate type of fire suppression for a room storing critical servers/systems. Further, the Foundation did not wipe hard drives to ensure secure disposition of protected data, and remote access to Foundation servers was not always secure.

## **FORTY-NINER SHOPS, INC.**

## **OPERATING, ADMINISTRATIVE AND FACILITIES AGREEMENTS [30]**

Certain business arrangements among the Forty-Niner Shops, Inc. (Shops), the campus, and other entities were not supported by complete and/or timely written agreements.

## **OPERATIONAL COMPLIANCE [32]**

Shops had not developed a written risk management policy. Further, the Shops' revocation of post-employment health benefits for full-time employees hired after January 1, 2009, was in conflict with requirements for the comparability of employee salaries, wages, and benefits with campus staff performing substantially similar services.

## **SEGREGATION OF DUTIES [33]**

Certain duties and responsibilities related to accounts receivable were not adequately segregated at Shops accounting office.

## **PETTY CASH AND CHANGE FUNDS [34]**

Shops petty cash policy did not specify a threshold for petty cash purchases, and Shops petty cash was inappropriately supplemented. In addition, administration of the vault fund at Shops was not adequate. This is a repeat finding from the prior Auxiliary Organizations audit.

## **PROPERTY AND EQUIPMENT [36]**

Administration of Shops property and equipment did not ensure proper accountability and identification.

## **INFORMATION TECHNOLOGY [37]**

Password controls were not always adequate for Shops systems, and backups for Shops systems were not securely stored locally in a fireproof safe, nor were the backups stored at any off-site location. In addition, certain critical Shops systems were not stored in the data center, and the data center was not equipped with a fire suppression device. Further, Shops did not wipe hard drives to ensure secure disposition of protected data, and Shops personnel with access to critical systems and protected data were not required to complete data confidentiality forms.

## **ASSOCIATED STUDENTS, CALIFORNIA STATE UNIVERSITY, LONG BEACH**

### **OPERATING AND ADMINISTRATIVE AGREEMENTS [43]**

Certain written agreements between the Associated Students, California State University, Long Beach (AS) and third parties did not include proper indemnification provisions, were not executed in a timely manner, or lacked contractual terms to address information security and data confidentiality.

### **SEGREGATION OF DUTIES [44]**

Certain duties and responsibilities related to payroll processing were not adequately segregated at AS.

### **CASH RECEIPTS AND HANDLING [45]**

Administration of cash receipts at AS did not ensure adequate accountability over pre-numbered receipts and the prompt changing of a safe combination after a change in personnel with safe access.

### **PURCHASING AND ACCOUNTS PAYABLE [46]**

Certain AS cash disbursements were not appropriately authorized and/or supported by sufficient and appropriate documentation.

### **PROPERTY AND EQUIPMENT [48]**

Administration of AS property and equipment was deficient. Both concerns were noted in the prior Auxiliary Organizations audit.

### **INFORMATION TECHNOLOGY [49]**

Password controls and data security were not always adequate for AS systems, and backups for AS systems with protected data were not encrypted when stored locally or when in transit to the off-site storage facility managed by a third party. In addition, access to add/edit vendor data in the AS vendor master file was not adequately controlled and resulted in an inadequate segregation of duties.

---

## INTRODUCTION

### **BACKGROUND**

Education Code §89900 states, in part, that the operation of auxiliary organizations shall be conducted in conformity with regulations established by the Trustees.

Education Code §89904 states, in part, that the Trustees of the California State University (CSU) and the governing boards of the various auxiliary organizations shall:

- ▶ Institute a standard systemwide accounting and reporting system for businesslike management of the operation of such auxiliary organizations.
- ▶ Implement financial standards that will assure the fiscal viability of such various auxiliary organizations. Such standards shall include proper provision for professional management, adequate working capital, adequate reserve funds for current operations and capital replacements, and adequate provisions for new business requirements.
- ▶ Institute procedures to assure that transactions of the auxiliary organizations are within the educational mission of the state colleges.
- ▶ Develop policies for the appropriation of funds derived from indirect cost payments.

The Board of Trustee policy concerning auxiliary organizations was originally adopted in July 1981 in the Resolution of the Committee on Finance (RFIN) 7-81-4. Executive Order 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, represents policy of the Trustees addressing CSU auxiliary organization activity and governing the internal management of the system. CSU auxiliary organizations are required to comply with Board of Trustee policy (California Code of Regulations, Title 5, Section 42402 and Education Code, Section 89900).

This executive order requires that the Office of the University Auditor will perform an internal compliance/internal control review of auxiliary organizations. The review will be used to determine compliance with law, including statutes in the Education Code and rules and regulations of Title 5, and compliance with policy of the Board of Trustees and of the campus, including appropriate separation of duties, safeguarding of assets, and reliability and integrity of information. According to Board of Trustee instruction, each auxiliary organization shall be examined on a triennial basis pursuant to procedures established by the chancellor.

The California State University, Long Beach Foundation (Foundation) was established in 1956 as a non-profit public benefit corporation. The Foundation serves the university's educational mission by supporting and engaging in research, entrepreneurship, community service, endowment administration, sponsored programs post-award administration, and the acquisition of private resources. The Foundation is governed by a board of directors committed to developing philanthropic resources to support the university's mission. A recent example of this is the purchase of Brook's College, which is located approximately one mile from the campus and has been renamed the Residential Learning College. This

location includes three residential/classroom/office buildings, with 177,000 total square feet, including 50,000 square feet of classroom and office space, and approximately 550 beds for student housing. The Foundation completed renovation of this property during audit fieldwork and opened it to students in August 2009 to function as a living and learning environment.

The Forty-Niner Shops, Inc. (Shops) was established in 1953 as a non-profit public benefit corporation. Shops is governed by a ten-member board of directors comprised of representatives from university administration, faculty, students and the community, and was incorporated to: establish, maintain, and operate a general book and supply store, and cafeteria and restaurant on campus; build, construct, lease, or purchase buildings necessary to carry out its purposes; apply funds and property received to further the educational services of the university; and perform other functions related to university activities. Currently, Shops owns and operates the main campus bookstore as well as a satellite bookstore located off-campus in Belmont Shores that was opened in December 2007. Shops also owns and operates several dining concepts and convenience stores, operates several national brand restaurants, contracts with third parties for the operation of several other national brand restaurants, and operates residential dining services. In addition, Shops operates the ID card services program for students via an agreement with the university.

The Associated Students, California State University, Long Beach (AS) was established in 1949 as the associated student body organization and was later incorporated as a non-profit corporation in 1956 to provide programs and services integral to the campus' educational mission. AS promotes and maintains student self-government and essential activities closely related to, but not normally included as a part of, the regular instruction program of the university. AS is charged with developing student leadership; fulfilling the recreational and social needs of the students; overseeing building, constructing, leasing or purchasing of buildings; applying funds and property received to further the educational services and/ or welfare of the students; and performing other functions related to university student activities. Currently, AS owns and operates the University Student Union, and operates the Isabel Patterson Child Development Center, a recycling center, an intramural sports and wellness program, the Beach Pride Center, and several media outlets that provide students with experience in television and radio production and publishing.

## **PURPOSE**

The principal audit objectives were to determine compliance with the Education Code, Title 5, and directives of the Board of Trustees and the Office of the Chancellor and to assess the adequacy of controls and systems. Specifically, we sought assurances that:

- ▶ Legal and regulatory requirements are complied with.
- ▶ Accounting data is provided in an accurate, timely, complete, or otherwise reliable manner.
- ▶ Assets are adequately safeguarded from loss, damage, or misappropriation.
- ▶ Duties are appropriately segregated consistent with appropriate control objectives.
- ▶ Transactions, accounting entries, or systems output is reviewed and approved.
- ▶ Management does not intentionally override internal controls to the detriment of control objectives.
- ▶ Accounting and fiscal tasks, such as reconciliations, are prepared properly and completed timely.

- ▶ Deficiencies in internal controls previously identified were corrected satisfactorily and timely.
- ▶ Management seeks to prevent or detect erroneous recordkeeping, inappropriate accounting, fraudulent financial reporting, financial loss, and exposure.

## **SCOPE AND METHODOLOGY**

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 accounting and administrative controls are in place and operative. The management review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor policies, letters, and directives. For those audit tests that required annualized data, fiscal years 2006/07 and 2007/08 were the primary periods reviewed. In certain instances, we were concerned with representations of the most current data; in such cases, the test period was July 1, 2008, to June 26, 2009. Our primary focus was on internal compliance/internal control.

Specifically, we reviewed and tested:

- ▶ Formation of the auxiliary.
- ▶ Functions the auxiliary performs on the campus.
- ▶ Creation and operation of the auxiliary's board.
- ▶ Establishment of policies and procedures based upon sound business practices.
- ▶ Maintenance of "arms-length" in business transactions between the auxiliary and the campus.
- ▶ Campus oversight of auxiliary operations.

Additionally, for the period reviewed, we examined other aspects of compliance of the campus and each auxiliary with the Education Code and Title 5 as they relate to the operation of CSU auxiliary organizations. Individual codes and regulations added to the scope of our review were identified through an assessment of risk. Similarly, internal controls were included within our scope based upon risk. Therefore, the scope of our review varied from auxiliary to auxiliary.

A preliminary survey of CSU auxiliaries at each campus was used to identify risks. Risk was defined as the probability that an event or action would adversely affect the auxiliary and/or the campus. Our assessment of risk was based upon a systematic process, using professional judgments on probable adverse conditions and/or events that became the basis for development of our final scope. We sought to assign higher review priorities to activities with higher risks. As a result, not all risks identified were included within the scope of our review.

Based upon this assessment of risks, we specifically included within the scope of our review the following:

### California State University, Long Beach Foundation

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements

California State University, Long Beach Foundation (cont.)

- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Auxiliary Programs
- ▶ Information Technology

Forty-Niner Shops, Inc.

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control
- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Auxiliary Programs
- ▶ Information Technology

Associated Students, California State University, Long Beach

- ▶ Operating and Administrative Agreements
- ▶ Facilities Agreements
- ▶ Corporate Governance
- ▶ Fiscal Compliance
- ▶ Operational Compliance
- ▶ Program Compliance
- ▶ Campus Oversight and Control

Associated Students, California State University, Long Beach (cont.)

- ▶ Segregation of Duties
- ▶ Cash Receipts and Handling
- ▶ Petty Cash and Change Funds
- ▶ Investments
- ▶ Fees, Revenues, and Receivables
- ▶ Purchasing and Accounts Payable
- ▶ Personnel and Payroll
- ▶ Property and Equipment
- ▶ Trusts and Other Liabilities
- ▶ Auxiliary Programs
- ▶ Information Technology

Campus

- ▶ Campus Oversight and Control

We have not performed any auditing procedures beyond June 26, 2009. Accordingly, our comments are based on our knowledge as of that date. Since the purpose of our comments is to suggest areas for improvement, comments on favorable matters are not addressed.

---

# OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

## CAMPUS

### INFORMATION TECHNOLOGY

#### PROTECTED DATA ASSESSMENT

The California State University, Long Beach Foundation (Foundation), Forty-Niner Shops, Inc. (Shops) and Associated Students, California State University, Long Beach (AS) did not perform a periodic, detailed assessment and inventory of protected information residing on their systems, and the protected information was not classified into security levels.

Executive Order (EO) 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates periodic assessment and inventory of protected information residing on systems.

The California State University, Long Beach (CSULB) *Records Management Standard* identifies three classification levels of information based on the value, legal requirements, sensitivity, and criticality assigned to them. These levels are: Level 1 – Confidential; Level 2 – Internal Use or Enterprise; and Level 3 – Public. This standard applies to all records, regardless of medium held by CSULB and all employees of CSULB and CSULB auxiliary organizations.

The executive management of these auxiliaries stated that management was unaware of the requirement to complete such a detailed assessment and classification of protected information.

Inadequate accountability over information assets, especially those containing critical and/or personal confidential information or with accessibility to such protected information, increases the risk of loss and inappropriate use of auxiliary resources and exposure to information security breaches.

#### **Recommendation 1**

We recommend that the auxiliaries perform an initial, and then annual, assessment and inventory of protected data on all systems to determine the existence of any protected data, the classification of

such data into applicable security levels, and the need for appropriate logical and physical security measures.

### **Campus Response**

We concur.

The Foundation currently does an annual assessment and inventory of protected data, and will also include classification of this data by January 31, 2010.

ASI will perform an initial, and then annual, assessment and inventory of protected data on all systems to determine the existence of any protected data, the classification of such data into applicable security levels, and the need for appropriate logical and physical security measures. Estimated date of completion is April 30, 2010.

Shops will review all internal system data and assess for content falling under the protected data category. A new policy and procedure will be drafted to define the applicable data security classification and the appropriate security thereof. Estimated date of completion is January 31, 2010.

### **USER ACCESS REVIEWS**

The Foundation, Shops, and AS did not perform periodic, documented management reviews of user access privileges within all systems and applications containing protected data.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the California State University (CSU) system. Section 8.10, *Computer Controls*, states that auxiliary organizations should establish written policies and practices creating levels of security linked to job responsibilities and data sensitivity.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates a periodic, documented review of user access privileges within all systems and applications containing protected data.

The executive management of these auxiliaries stated that management reviews of user access privileges were completed on an informal ad hoc basis, but were not consistently documented for all systems. The executive directors further stated that they were unaware of the requirement to document management reviews of user access privileges.

Failure to periodically perform a documented review of user access to systems and applications containing protected data increases the risk of inappropriate access.

### **Recommendation 2**

We recommend that all auxiliaries conduct periodic, documented management reviews of user access for all systems and applications containing protected data, at least annually.

### **Campus Response**

We concur.

The Foundation will conduct and document management review of user access annually beginning January 31, 2010.

ASI will begin conducting annual, documented management reviews of user access for all systems and applications containing protected data. This review will be conducted in conjunction with the assessment and inventory of protected data. Estimated date of completion is April 30, 2010.

Shops will formalize its user access policy to include a standardized corporate review instead of leaving the responsibility with the respective operation. The policy will include an annual audit/review component as part of the process. Estimated date of completion is January 31, 2010.

## **INFORMATION SECURITY TRAINING**

Foundation, Shops, and AS personnel with access to protected data were not required to complete information security awareness training.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates periodic information security awareness training for all employees with access to protected data.

The executive management of each auxiliary stated that the auxiliaries had implemented some forms of employee education regarding information security policies and requirements, although this may not have provided comprehensive coverage of information security risks. They added that the *Workplace Answers* module for information security awareness training was anticipated to be made available to, and required of, all campus and auxiliary employees.

Failure to provide employees with information security awareness training increases the risk of mismanagement of protected data, which increases auxiliary and campus exposure to security breaches and could compromise compliance with statutory information security requirements.

**Recommendation 3**

We recommend that the auxiliaries develop and implement an action plan for providing information security awareness training to all employees with access to protected data.

**Campus Response**

We concur.

The Foundation has provided the online security training program by Workplace Answers to its employees.

All ASI employees with access to protected data have completed the Workplace Answers online information security training. In addition, ASI will develop and implement an action plan for providing training to new employees prior to their gaining access to confidential data. Estimated date of completion is January 31, 2010.

In collaboration with the CSU campuses, the chancellor's office developed a web-based information security awareness training course designed to provide the campus community members with guidance on securing our information resources. This web-based course was extended to the Forty-Niner Shops to help safeguard auxiliary information as well as university data. This training course was provided to Shops personnel during the month of August 2009 and administered through the campus information security office.

## **CALIFORNIA STATE UNIVERSITY, LONG BEACH FOUNDATION**

### **FACILITIES AGREEMENTS**

Certain use agreements between the California State University, Long Beach Foundation (Foundation) and third parties did not include an indemnification provision to specifically indemnify the CSU Trustees, the campus, and the State of California.

Our review of four off-site use agreements disclosed that all four lacked an indemnification provision to specifically indemnify the CSU Trustees, the campus, and the State of California.

EO 849, *California State University Insurance Requirements*, dated February 5, 2003, states that auxiliary organizations shall agree to indemnify, defend, and save harmless the State of California, the Trustees of the CSU, the campus, and the officers, employees, volunteers, and agents of each of them from any and all loss, damage, or liability that may be suffered or incurred by state, caused by, arising out of, or in any way connected with the operations of the auxiliary.

The Foundation associate executive director stated that the use agreements reviewed reflect those that have been in place for several years and were executed on a standard lease form supplied by the lessor.

The absence of an appropriate indemnification provision subjects both the auxiliary and CSU to potential liability.

#### **Recommendation 4**

We recommend that the Foundation ensure that all future use agreements include appropriate indemnification provisions.

#### **Campus Response**

We concur. The Foundation will ensure appropriate indemnification is included in all future use agreements. Corrective action on this issue is complete.

### **OPERATIONAL COMPLIANCE**

The Foundation had not developed a written risk management policy.

EO 715, *California State University Risk Management Policy*, dated October 27, 1999, delegated authority and responsibility to the campus president to implement campus risk management policies consistent with the CSU Risk Management Policy guidelines. This includes an ongoing process to identify risks, analyze the frequency and severity of the potential risks, and select the best management techniques to manage the risks.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.7, *Risk Management*, states that auxiliary organizations should develop programs to manage risk related to activities in which the organizations are engaged.

The Foundation chief financial officer (CFO) stated that the Foundation followed the university's risk management policy and further addressed risk management in its insurance and lease management policy. He further stated that he did not realize that there was a need for a separate written risk policy.

The absence of a comprehensive risk management policy increases the risk that all current risk-related activities may not be adequately evaluated.

### **Recommendation 5**

We recommend that the Foundation develop and adopt a written risk management policy, including procedures to actively identify, analyze, quantify, and manage risk.

### **Campus Response**

We concur. The Foundation currently utilizes the risk management policy of the campus and will develop and adopt its own risk management policy. Estimated date of completion is April 30, 2010.

## **CASH RECEIPTS AND HANDLING**

Foundation cash receipts were not always timely processed and adequately safeguarded.

We found that:

- ▶ Checks collected off-site by sponsored project directors were not immediately submitted to the Foundation for deposit. Specifically, we found seven checks totaling \$2,212 dated from January 6, 2009, to May 22, 2009, located in the cashier's office inbox on June 5, 2009. The submission delays ranged from 14 to 150 days from the date on which the checks were written.
- ▶ Checks and credit card receipts collected off-site by sponsored project directors were transported to the Foundation cashier's office by student assistants and other project staff in unsecured envelopes. These receipts contained personal contact information, which consisted of the cardholders' name, address, credit card number, and expiration date.

CSULB Foundation *Cash Receipts Policy #11-000.1* states that deposits to the Foundation shall be prepared daily by each project director to ensure accurate and timely recording of funds.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system.

Section 8.9.1, *Cash*, states that the auxiliary should receive cash in a consistent manner utilizing systems that ensure integrity of existing internal controls.

CSULB Foundation *Cash Receipts Policy #11-000.1* states that the project director or other authorized employee (staff) shall hand carry deposits to the Foundation in a locked security bag and only relinquish possession of funds to the Foundation cashier or designated Foundation employee.

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive standard that mandates 12 core requirements intended to help organizations proactively protect customer account data. Requirement 3 mandates the protection of stored cardholder data, and requirement 9 mandates the restriction of physical access to cardholder data.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates adequate administration and safeguarding of cash receipts and sensitive information.

The Foundation CFO stated that even though the Foundation cash-handling policy was posted online and in the cashier's window, not all project staff was complying with these requirements. He further stated that management was unaware of the unsecured deposits in transit that contained personal confidential information.

Inadequate administration of cash receipts and protection of personal information increases the risk of loss from inappropriate acts and the unauthorized access to, and disclosure of, personal information.

### **Recommendation 6**

We recommend that the Foundation:

- a. Reiterate existing cash-handling policies to all project staff and increase enforcement efforts to ensure that all receipts are processed in a timely manner.
- b. Furnish locked security bags to all project directors to ensure that receipts are adequately safeguarded until deposited.

### **Campus Response**

We concur. These recommendations were completed during fieldwork. An e-mail was sent to all project directors reminding them of the cash-handling policies, and locked security bags have been provided to all projects transporting sensitive material. Corrective action on this issue is complete.

## PROPERTY AND EQUIPMENT

Administration of the physical inventory process at the Foundation required improvement.

We reviewed the 2008 physical inventory and found that:

- ▶ Inventory procedures were not updated to include the role of the third-party service provider, and roles and responsibilities were not clearly defined or communicated for all Foundation departments (i.e., information systems and technology, accounts payable, grants and contracts) and sponsored project directors involved in the review and final disposition of inventory variances.
- ▶ 240 assets were not located during the physical inventory count, and adequate follow-up was not performed to determine the disposition of these assets. For example, the Foundation did not receive responses from sponsored project directors regarding the disposition of 142 (59%) of the 240 missing assets.
- ▶ A purchase order instead of a service agreement was used for a third-party service provider that performed the physical inventory counts. In addition, the purchase order did not reference the CSU general provisions. As a result, insurance and indemnification provisions were not addressed.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should establish a written system that ensures physical inspection of property and equipment on a service life schedule and proper recording of property and equipment.

EO 849, *California State University Insurance Requirements*, dated February 5, 2003, states that auxiliary organizations shall require certain levels of general liability insurance and agree to indemnify, defend, and save harmless the State of California, the Trustees of the CSU, the campus, and the officers, employees, volunteers, and agents of each of them from any and all loss, damage, or liability that may be suffered or incurred by state, caused by, arising out of, or in any way connected with the operations of the auxiliary.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient administration of the physical inventory process and that business arrangements for services include appropriate insurance and indemnification provisions.

The Foundation associate director of information systems and technology stated that including the role of the third-party service provider and the roles and responsibilities of all departments and sponsored project directors involved in the physical inventory process was not considered when the fixed assets procedures were updated. He further stated that the Foundation had not adequately followed up on the missing assets or its initial attempts to contact sponsored project directors concerning the missing assets due to other priorities. He added his belief that the use of a service agreement or referencing the CSU general provisions was not necessary for this type of service.

Insufficient administration of property and equipment increases the risk that property may be lost or stolen, and misrepresented in the financial statements, while the absence of appropriate insurance and indemnification provisions for services subjects both the auxiliary and CSU to potential liability.

### **Recommendation 7**

We recommend that the Foundation:

- a. Update its inventory procedures to include the role of the third-party service provider, and clearly define and communicate roles and responsibilities for all Foundation departments and sponsored project directors involved in the physical inventory process.
- b. Promptly resolve disposition of the missing assets, including follow-up with the sponsored project directors.
- c. Ensure that all future agreements with third parties for inventory services include appropriate insurance and indemnification provisions.

### **Campus Response**

We concur:

- a. Inventory procedures will be updated and the roles for all Foundation departments, and sponsored project directors involved in the physical inventory process will be defined and communicated by April 30, 2010.
- b. All the items that were not found during the initial physical inventory were cleared during audit fieldwork. Corrective action on this issue is complete.
- c. Purchase orders now contain a link to CSU terms and conditions, so future agreements with vendors will contain that information. Corrective action on this issue is complete.

## TRUSTS AND OTHER LIABILITIES

Certain campus program revenues were inappropriately deposited to, and held in custody by, the Foundation.

The Foundation financial statements as of June 30, 2009, indicated that the Foundation administered and maintained 584 custodial trust accounts totaling \$32.1 million. We reviewed 50 of these accounts and found that state funds were being inappropriately held by the Foundation in 40 accounts.

EO 919, *Policy Governing Non-General Fund Receipts*, dated October 15, 2004, states that each CSU campus shall administer their non-General Fund receipts to ensure that the funds are held in proper accounts. EO 919 also states that, as a matter of CSU policy, auxiliaries may not accept state funds with the intent of administering them as an agent of the university. Payment for services is the only instance where state funds may be accepted into an auxiliary organization's account. Further, the entity that is responsible for any losses that might arise from the event or activity that generated the receipts shall be the entity wherein receipts are held.

Although EO 1000, *Delegation of Fiscal Authority and Responsibility*, dated July 1, 2007, indicates that it supersedes EO 919, the areas noted above are acknowledged by systemwide administrators to still be in effect and will be addressed by the forthcoming Integrated CSU Administrative Manual.

The Foundation CFO stated that a review of custodial trust accounts had been initiated after the athletics administration audit to determine whether any state funds were being inappropriately held but had not yet been completed due to resource constraints.

The campus' required oversight of state funds is limited when funds are deposited outside the custody of the CFO.

### **Recommendation 8**

We recommend that the Foundation:

- a. Complete a review of all custodial trust accounts and determine, within 60 days, which accounts contain state funds.
- b. Certify that none of the following specific and similar monies reside in Foundation trust accounts:
  - Gifts to the university, its units and programs.
  - Contracts and grants awarded to the university.
  - Pre-award indirect cost recovery reimbursements.
  - Foundation net operating surplus designated for use by the campus.
  - Fees for continuing education courses provided by the university.

- Fees for university events, workshops, conferences, institutes, special projects, and programs.
  - Reimbursements for services and products provided to auxiliary enterprises and organizations paid from General Fund and/or CSU operating fund monies.
  - Rental fees for university facilities, except those facilities that have been leased to the auxiliary by the campus.
  - Student fees and other general fees pursuant to the CSU student fee policy.
  - Monies held by the Foundation via contract with the campus.
- c. Submit to the Office of the University Auditor, within 60 days, a list of those trust accounts which have been deemed appropriate to remain in the custody of the Foundation and comprehensive documentation to support the sources of funds for those trust accounts.
- d. Move those state funds identified in “a” above to campus accounts within six months.

### **Campus Response**

We concur:

- a. The review of accounts will be completed by January 26, 2010.
- b. The review will certify that none of the listed accounts reside in Foundation trust accounts by January 26, 2010.
- c. The list of trust accounts deemed appropriate to remain in the custody of the Foundation with corresponding documentation will be submitted to the Office of the University Auditor by January 26, 2010.
- d. A plan will be developed to move state funds from the Foundation to campus accounts. During this time while state funds are retained at the Foundation, the state will have full control over the funds. Estimated date of completion is April 30, 2010.

### **AUXILIARY PROGRAMS**

Foundation administration of sponsored programs required improvement.

We reviewed ten grants and contracts files and found that:

#### Process Controls

Sponsored program deliverables, including periodic technical, performance, and patent reports, or evidence of completion and timely submission to sponsors was not required to be submitted to the office of grants, contracts and foundation programs and retained in the project files.

### Processing Exceptions

- ▶ Three files did not contain evidence of periodic technical reports that were required to be submitted to the contracting agency.
- ▶ The final report deliverables in one project file were not submitted to the contracting agency in a timely manner.
- ▶ One file did not contain a current conflict of interest form. The most recent conflict of interest form contained in the file was completed in October 2003.
- ▶ The grants and contracts closeout process was not always timely. We reviewed five projects with end dates that ranged from October 2006 to June 2008 and found that three projects were closed from 108 to 616 days after the project end date. The other two projects reviewed had not been closed as of the completion of audit fieldwork, which ranged from 177 to 377 days after the project end date.

EO 890, *Administration of Grants and Contracts in Support of Sponsored Programs*, dated January 7, 2004, 3.2.1 *Administration of Sponsored Programs*, states that the sponsored program administrator is legally responsible and accountable to the sponsor for the use of funds provided and the performance of the sponsored program.

Office of Management and Budget (OMB) Circular A-110, *Uniform Administrative Requirements for Grants and Agreements With Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations*, §.51(a), indicates that recipients are responsible for managing and monitoring each project, program, sub-award, function, or activity supported by the award. Section .71(a) states that recipients shall submit, within 90 calendar days after the date of completion of the award, all financial, performance, and other reports as required by the terms and conditions of the award.

CSULB Office of University Research *Standard Operating Procedure for Conflict of Interest Forms for Principal Investigators* states, in part, that principal investigators with proposals for funding from all other sources (i.e., non-exempt and not funded by the National Science Foundation or National Institutes of Health) must file the an annual update of form 700-U.

The director of grants, contracts and foundation programs stated that the office of grants, contracts and foundation programs did not require evidence of the submission of deliverables to the sponsor or feel the need to continuously monitor the completion and timeliness of interim deliverables because project directors are made aware of their responsibilities during their project orientation. She further stated that the office procedures did not require technical reports to be retained on file by other than the project director, and the failure to update the conflict of interest form was due to oversight. She also stated that when the project director did not complete and submit the final patent report in a timely manner, her office elevated it to the dean's office. She added that the closeout process did not appear timely due to pending project extensions and extenuating circumstances.

Inadequate administration of sponsored programs increases the risk of non-compliance with OMB requirements and exposes the auxiliary organization to penalties and disallowances for non-compliance with contracts and grants terms.

**Recommendation 9**

We recommend that the Foundation:

- a. Update its existing post-award administration procedures and implement a process that requires grants and contracts administrators to track the submission of deliverables.
- b. Reiterate the importance of timely submission of deliverables and implement a process to ensure compliance.
- c. Ensure that conflict of interest forms are kept current.
- d. Enforce its existing procedures to ensure that projects are closed out timely, within 90 days.

**Campus Response**

We concur:

- a. The policy will be reiterated to grants and contracts administrators.
- b. The Foundation will reiterate with project directors the importance of timely submission with the 120/90/60/45/30-day notices. This process is included in the current close-out checklist.
- c. The Foundation's procedures are to keep the conflict of interest forms current, and this will be reiterated with administrators.
- d. The Foundation will reiterate with administrators the importance of closing out projects on a timely basis.

Estimated date of completion is January 31, 2010.

## INFORMATION TECHNOLOGY

### PASSWORD AND DATA SECURITY

Password controls and data security were not always adequate for Foundation systems.

We found that:

- ▶ The password security parameter was inadequate for the IFAS system, as the minimum password length was six characters instead of the minimum eight characters required by the campus and leading information security industry guidelines.
- ▶ The IFAS system, including all modules from Finance, Grants Management, Payroll and Human Resources (HR) containing protected data, was not encrypted. Furthermore, an Internet-accessible device (web server) was located within the same network segment as critical internal resources (IFAS and reporting servers). Normally, these Internet-accessible devices are segmented into a demilitarized zone (DMZ) such that if these devices are compromised, there is separation among other internal network resources. Although this web server was enabled with only http and https, this web server had not been scanned for vulnerability assessment and verification of security to remain on this network segment with critical resources.

The CSULB *Password Standard* states that to the extent that the password complexity is supported by the respective device, passwords shall contain at least eight characters. This standard applies to all individuals who have or are responsible for an account or any form of access that supports or requires a password on any CSU system, has access to the CSULB network, or stores any non-public CSULB information.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates strong controls over password parameters and system security.

The Foundation associate director of information systems and technology stated that the password length of six characters was the default setting that had not been changed. He added that encryption was not yet available for IFAS, although an enhancement ticket was set up by Bi-Tech for implementation in the near future. He further stated that the Foundation had attempted, but was unsuccessful in moving the web server to the DMZ when the system was initially set up.

Insufficient password controls and security parameters may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems; all of which increase the risk of unauthorized access to auxiliary systems and confidential data.

### **Recommendation 10**

We recommend that the Foundation:

- a. Set effective password security parameters for IFAS in accordance with campus and security industry guidelines.
- b. Apply encryption controls to all Foundation computers, databases, and file servers that house protected or sensitive data.
- c. Implement a formal DMZ between internal network resources and Internet-accessible devices.

### **Campus Response**

We concur:

- a. The password length requirement was changed to eight characters during audit fieldwork.
- b. Currently, the application vendor has indicated that the encryption feature is not currently available, but an enhancement request has been created. The Foundation has implemented preventative and detective controls, which were discussed with the auditors. It was agreed that these controls protect sensitive data with the best available technology. The campus and the Foundation both accept the risks inherent in not encrypting sensitive information.
- c. The web server was moved to the DMZ during audit fieldwork.

Corrective action on this issue is complete.

## **SYSTEM BACKUPS**

Backups for Foundation systems with protected data were not encrypted when stored locally or when in transit to the off-site storage facility managed by a third-party.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound

business practices. Sound business practice mandates the encryption of protected data contained on auxiliary systems and backups.

The Foundation associate director of information systems and technology stated that the Foundation had not encrypted backups because the time required to encrypt data was not considered to be cost beneficial.

Inadequate security of system backups increases the risk of inappropriate access to protected data and the possible ramifications of required public notifications should backups be lost when unencrypted.

### **Recommendation 11**

We recommend that the Foundation encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure.

### **Campus Response**

We concur. The Foundation will implement a method to encrypt system backups. Estimated date of completion is February 28, 2010.

## **ENVIRONMENTAL CONTROLS**

The Foundation server room had a water-sprinkler system, which is an inappropriate type of fire suppression for a room storing critical servers/systems.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that fire suppression devices appropriate for electrical equipment be maintained within the premises of server rooms.

The Foundation associate director of information systems and technology stated that the server room had a water-sprinkler system because of building code requirements imposed before the room was designated as the server room.

Failure to maintain appropriate fire suppression devices in the server room increases the risk of unsuccessful suppression of a fire and/or damage to critical systems, which may expose employees to dangerous conditions and result in the loss of critical systems.

### **Recommendation 12**

We recommend that the Foundation evaluate the feasibility of another means of fire suppression or consider relocation of Foundation servers to the campus data center.

### **Campus Response**

We concur. The Foundation has begun to evaluate the feasibility of alternative fire suppression methods in the main server room. Should such alternative methods prove impracticable or cost prohibitive, the relocation of Foundation servers will be evaluated. Estimated date of completion is April 30, 2010.

### **DISPOSITION OF PROTECTED DATA**

The Foundation did not wipe hard drives to ensure secure disposition of protected data.

We found that hard drives of old machines were not destroyed or wiped clean and were retained in a storage closet.

The CSULB *Records Management Standard* states that to protect the confidentiality of information and the related privacy rights of CSULB students, faculty, staff, donors, patrons, vendors, and others, Level 1 and Level 2 information contained in all software and/or computer files, storage media devices, and hard copy must be sanitized prior to disposal. The sanitization process ensures that recovery of information is not possible. Several methods can be used to sanitize media; however, the two major types of sanitization are clearing and destroying. This standard applies to all records, regardless of medium held by CSULB and all employees of CSULB and CSULB auxiliary organizations.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the secure disposition of protected data contained in auxiliary files and systems.

The Foundation associate director of information systems and technology stated that the Foundation had not disposed of these machines due to oversight, but had a process of performing low-level reformats of hard drives before removing them from the computer and storing the reformatted disks in an information technology office storage closet to which physical access was controlled.

Inadequate control over equipment assets, especially those containing protected data, increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

### **Recommendation 13**

We recommend that the Foundation implement a process to ensure that hard-drive wiping is performed and sufficiently documented.

### **Campus Response**

We concur. A Media Sanitation section was added to the Information Privacy and Security Policy. A Media Sanitation Log was created. A section on destroying obsolete media was added to the Records Retention Policy and Procedures. A “Method of Media Sanitation” was added to the Retired Fixed Asset Form. Corrective action on this issue is complete.

## **REMOTE SERVER ACCESS**

Remote access to Foundation servers was not always secure.

Telecommunication Network (Telnet), an unsecure remote access protocol that allows users to connect to remote computers and transmits data in clear text, was enabled on the IFAS application/database server to permit remote access by the vendor for performing system updates. In addition, the athletics department also accessed IFAS for data entry purposes via Telnet remote access.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates securing remote access to auxiliary systems.

The Foundation associate director of information systems and technology stated that the Foundation had not considered this to be a significant risk because remote access to IFAS was limited.

Failure to properly secure remote access to auxiliary servers increases the risk that an attacker who is able to monitor network traffic could capture sensitive information or authentication credentials and, therefore, gain access to network resources and exploit vulnerabilities that could lead to the loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

**Recommendation 14**

We recommend that the Foundation replace Telnet remote access with a more secure remote access protocol (such as secure shell) or enforce internal firewall restrictions on Telnet such that it could only be accessed once a virtual private network (VPN) connection has been established.

**Campus Response**

We concur. Remote access is now secured via secure shell (SSH). Corrective action on this issue is complete.

## **FORTY-NINER SHOPS, INC.**

### **OPERATING, ADMINISTRATIVE AND FACILITIES AGREEMENTS**

Certain business arrangements among the Forty-Niner Shops, Inc. (Shops), the campus, and other entities were not supported by complete and/or timely written agreements.

We found that:

- ▶ The arrangement with a third-party service provider for payroll services was not supported by a written agreement. Further, the ADP payroll system, which contains protected employee data for Shops payroll, was hosted off-site by the service provider. The lack of a service agreement for this off-site hosting service also resulted in information security and confidentiality terms not being addressed.
- ▶ The residential dining meal plan agreements for fiscal years 2007/08 and 2008/09 were not signed until approximately five months after the inception dates.
- ▶ Seven of fifteen vendor agreements reviewed did not include an indemnification provision to specifically indemnify the CSU Trustees, the campus, and the State of California.
- ▶ Two facilities lease agreements, one between Shops and a private trust for the off-campus store and the other a sublease agreement with a bank for the operation of an automated teller machine on campus, did not specifically indemnify the CSU Trustees, the campus, and the State of California. This is a repeat finding from the prior Auxiliary Organizations audit.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that business arrangements be supported by complete, written agreements that are executed in a timely manner.

EO 849, *California State University Insurance Requirements*, dated February 5, 2003, states that auxiliary organizations shall agree to indemnify, defend, and save harmless the State of California, the Trustees of the CSU, the campus, and the officers, employees, volunteers, and agents of each of them from any and all loss, damage, or liability that may be suffered or incurred by state, caused by, arriving out of, or in any way connected with the operations of the auxiliary.

The Shops controller/CFO stated that the auxiliary had an approved sales order on file from the payroll service provider, which he thought was sufficient. He also stated that the residential dining meal plan agreements were signed late due to ongoing negotiations over contract terms, and added that certain vendors required the auxiliary to sign standard franchise agreements that did not include the CSU-required indemnification provision. He further stated that the auxiliary had assumed a

standard assigned lease for the off-campus store and failure to include a proper indemnification provision in the automated teller machine operator's sublease was due to oversight.

The absence of complete and/or timely written agreements and appropriate indemnification provisions, as well as information security and confidentiality terms for services involving protected data, increases the risk of misunderstandings and miscommunications regarding rights and responsibilities, and subjects the auxiliary and CSU to potential liability.

**Recommendation 15**

We recommend that Shops:

- a. Establish a written agreement with the payroll service provider and for all vendor service agreements relating to access to protected records or data, consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities and the confidentiality of data.
- b. Ensure that all future agreements are executed prior to inception.
- c. Ensure that all future agreements include an appropriate indemnification provision.

**Campus Response**

We concur. Shops will:

- a. Work with the payroll service provider (ADP) to establish a service agreement and ensure that all vendor service agreements relating to access for protected data contain the proper CSU general provisions for information security.
- b. Ensure proper execution deadlines are met for all future agreements and escalate through campus management as is appropriate.
- c. Enforce the inclusion of appropriate indemnification language in all future agreements.

Estimated date of completion is May 31, 2010.

## **OPERATIONAL COMPLIANCE**

### **RISK MANAGEMENT**

Shops had not developed a written risk management policy.

EO 715, *California State University Risk Management Policy*, dated October 27, 1999, delegated authority and responsibility to the campus president to implement campus risk management policies consistent with the CSU Risk Management Policy guidelines. This includes an ongoing process to identify risks, analyze the frequency and severity of the potential risks, and select the best management techniques to manage the risks.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.7, *Risk Management*, states that auxiliary organizations should develop programs to manage risk related to activities in which the organizations are engaged.

The Shops controller/CFO stated that the auxiliary was unaware of the requirement for a risk management policy.

The absence of a comprehensive risk policy increases the likelihood that all current risk-related activities may not be adequately evaluated.

#### **Recommendation 16**

We recommend that Shops develop and adopt a written risk management policy, including procedures to actively identify, analyze, quantify, and manage risk.

#### **Campus Response**

We concur. Shops' management has drafted a risk management policy which has been presented to the board of directors on December 11, 2009, for initial review and comment. Upon approval, the policy will be implemented accordingly. Estimated date of completion is May 31, 2010.

## **EMPLOYEES**

The Shops' revocation of post-employment health benefits for full-time employees hired after January 1, 2009, was in conflict with requirements for the comparability of employee salaries, wages, and benefits with campus staff performing substantially similar services.

Title 5 §42405 states that the governing board of each auxiliary organization shall provide salaries, working conditions, and benefits for its full-time employees which are comparable to those provided campus employees performing substantially similar services. For those full-time employees who perform services that are not substantially similar to the services performed by campus employees,

the salaries established shall be at least equal to the salaries prevailing in other educational institutions in the area or commercial operations of like nature.

The Shops controller/CFO stated that due to new accounting regulatory requirements and dwindling retail margins, the auxiliary cannot afford to provide salaries, wages, and benefits comparable to the campus.

Failure to provide comparable benefits for similar positions increases the risk that the auxiliary may be expending inappropriate amounts on salaries, wages, and benefits for employees who perform substantially similar services as employees for the campus and may expose the auxiliary and campus to potential liability.

### **Recommendation 17**

We recommend that Shops reinstate post-employment health benefits for its full-time employees to ensure the comparability of salaries, wages, and benefits for its full-time employees in relation to those provided campus employees performing substantially similar services.

### **Campus Response**

The university has explored the full context of Recommendation 17 with Shops' management and its governing board. The compensation comparability standard raised in the finding applies only to the full-time employees holding positions substantially similar to those positions within the CSU system. That standard for only those positions extends to employee salaries, working conditions, and benefits in total, i.e., the total of these factors must be competitive with CSU employment in the same class. Shops approached with considerable diligence and deliberation the action to end post-employment medical coverage for hires beginning January 1, 2009. The magnitude of the future financial obligation for such coverage, coupled with the statutory *self-supporting* standard for auxiliary commercial operations, required prudent and timely action (FASB 106 and Education Code Section 89905). Absent, however, was a formal internal compensation policy framework and plan within which Shops acted that would more fully demonstrate compliance with Education Code Section 89900(c) and Title 5 Section 42405. The university will work closely with Shops' management and the board of directors to assure the adoption of a clear policy and plan that supports the action taken on this issue. Estimated date of completion is May 31, 2010.

## **SEGREGATION OF DUTIES**

Certain duties and responsibilities related to accounts receivable were not adequately segregated at Shops accounting office.

We noted that one employee:

- ▶ Established customer credit profiles in the accounting system.
- ▶ Created and mailed accounts receivable invoices and monthly statements.

- ▶ Posted accounts receivable payments to customer accounts.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.4, *Receivables*, states that the auxiliary should establish a written internal controls system that ensures billing, cash collection, customer inquiries, and subsidiary reconciliations are conducted separately and with due regard for the receivable duties.

The Shops controller/CFO stated that duties were not adequately segregated due to limited resources and staffing constraints.

Inadequate segregation of duties increases the risk that errors and irregularities will not be detected in a timely manner.

### **Recommendation 18**

We recommend that Shops appropriately segregate certain accounts receivable duties in its accounting office or institute mitigating procedures approved by the campus CFO.

### **Campus Response**

We concur. Shops agrees to further segregate the accounts receivable (A/R) function to be compliant with the recommendation. The Shops A/R activities consist of less than a full-time task which is being further divided amongst staff. The A/R policy and procedure has been revised accordingly to address specific segregation of duties. Corrective action on this issue is complete.

## **PETTY CASH AND CHANGE FUNDS**

### **PETTY CASH**

Administration of petty cash at Shops required improvement.

We found that:

- ▶ The petty cash policy did not specify a dollar threshold for petty cash purchases.
- ▶ The Shops petty cash fund of \$2,500 was inappropriately supplemented to cover petty cash purchases of \$3,435 in May 2008. The source of the supplement was unclear and occurred without authorization.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient administration of petty cash.

The Shops controller/CFO stated that it was the auxiliary's common practice to limit petty cash purchases to \$200; however, this practice was not formally documented in its written petty cash policy. He added that supplementing petty cash with funds from other sources was due to oversight.

Inadequate administration of petty cash increases the risk of loss or misappropriation of funds.

### **Recommendation 19**

We recommend that Shops:

- a. Update its petty cash policy to include a dollar threshold.
- b. Reiterate to staff petty cash policies and procedures and prohibit supplements to petty cash funds with funds from other sources.

### **Campus Response**

We concur:

- a. The Shops petty cash policy is under revision with a stipulated threshold of \$200.
- b. The revised policy will include new language around the refunding process and prohibition of supplements. Staff will also be informed of the policy updates.

Estimated date of completion is May 31, 2010.

### **CHANGE FUNDS**

Administration of the vault fund at Shops was not adequate.

We found that:

- ▶ A specific vault fund amount had not been established.
- ▶ The vault fund was commingled with cash collected from daily sales such that the general ledger record of cash on hand did not reconcile to the actual cash on hand.
- ▶ Shops did not perform periodic, independent cash counts of the vault fund. This is a repeat finding from the prior Auxiliary Organizations audit.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient administration of the vault fund.

The Shops controller/CFO stated that daily vault fund needs for retail operations fluctuate such that a specified vault fund amount and a separate vault fund general ledger account had not been considered. He further stated that lack of independent cash counts of the vault fund was due to oversight.

Inadequate administration of the vault fund increases the risk of loss or misappropriation of funds.

### **Recommendation 20**

We recommend Shops:

- a. Establish a specific vault fund amount.
- b. Maintain the vault fund separate from cash collected from daily sales and periodically reconcile the general ledger record of cash on hand to actual cash on hand.
- c. Perform periodic, documented independent cash counts of the vault fund.

### **Campus Response**

We concur:

- a. Shops is currently drafting a separate vault policy that will specify stated cash balances for the various economic cycles that occur during the school year.
- b. As part of the new policy, vault funds will remain isolated from daily sales activity and reconciled accordingly.
- c. Policy will include independent (other than cash room) audit of the vault funds.

Estimated date of completion is May 31, 2010.

## **PROPERTY AND EQUIPMENT**

Administration of Shops property and equipment did not ensure proper accountability and identification.

We found that Shops did not perform an independent physical inventory of all property and equipment during the last three years. Custodians were asked to confirm the property and equipment in their custody; however, there was no independent verification of the confirmations provided by the custodians. This is a repeat finding from the prior Auxiliary Organizations audit.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should establish a written system that ensures physical inspection of property and equipment on a service life schedule.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates sufficient administration of property and equipment.

The Shops controller/CFO stated that the failure to perform an independent physical inventory of property and equipment was due to limited resources and staffing constraints.

Insufficient administration of property and equipment increases the risk that property may be lost or stolen, and misrepresented in the financial statements.

### **Recommendation 21**

We recommend that Shops promptly perform an independent physical inventory of its property and equipment, including reconciliation to the general ledger, and establish procedures to conduct periodic, independent physical counts on a regular basis.

### **Campus Response**

We concur. Shops updated its fixed asset/property control policy to include a formally established physical audit and reconciliation process. Estimated date of completion is January 31, 2010.

## **INFORMATION TECHNOLOGY**

### **PASSWORD SECURITY**

Password controls were not always adequate for Shops systems.

We found that:

- ▶ The password security length parameter was inadequate for all Shops systems, including those containing protected data, as the minimum password length was six characters instead of the

minimum eight characters required by the campus and leading information security industry guidelines.

- ▶ Active Directory was not enabled with password complexity requirements.

The CSULB *Password Standard* states that, to the extent that the password complexity is supported by the respective device, passwords shall contain at least eight characters, and contain characters from each of the following four groups: uppercase letters, lowercase letters, numerals and symbols. This standard applies to all individuals who have or are responsible for an account or any form of access that supports or requires a password on any CSU system, has access to the CSULB network, or stores any non-public CSULB information.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates strong controls over password parameters.

The Shops data processing manager stated that the password length of six characters was the default setting that had not been changed, and the lack of complexity requirements was due to oversight.

Insufficient password controls may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems, all of which increase the risk of unauthorized access to auxiliary systems and confidential data.

### **Recommendation 22**

We recommend that Shops set effective password security parameters for all Shops systems, including Active Directory in accordance with campus and security industry guidelines.

### **Campus Response**

We concur. Shops will revisit its password security parameters for each of its systems and move towards a standardized process in accordance with proposed guidelines for those systems falling short. Estimated date of completion is May 31, 2010.

## **SYSTEM BACKUPS**

Backups for Shops systems were not securely stored locally in a fireproof safe, nor were the backups stored at an off-site location.

We found that backups for Shops systems were stored in the data center outside of the fireproof safe and were not transferred to an off-site location.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates secure local and off-site storage of system backups for disaster recovery purposes.

The Shops data processing manager stated that the system backups were not stored in a fireproof safe due to oversight, but that Shops was in the process of evaluating and selecting a means for remote backup with an off-site third-party vendor.

Inadequate storage of system backups increases the risk that auxiliary systems will not be recovered in the event of a disaster.

### **Recommendation 23**

We recommend that Shops promptly store system backups in a fireproof safe and contract with an off-campus backup storage facility for the regular storage of system backups.

### **Campus Response**

We concur. Shops is currently evaluating several system backup options and will implement the best value solution upon assessment completion. Estimated date of completion is May 31, 2010.

## **SYSTEM SECURITY AND ENVIRONMENTAL CONTROLS**

Certain critical Shops systems were not stored in the data center, and the data center was not equipped with a fire suppression device.

We found that:

- ▶ The Symantec anti-virus and the NBC back-office database servers were stored in the information technology office (outside of Shops data center), which did not provide for adequate security and environmental controls.
- ▶ The Shops data center was not equipped with a fire suppression device.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates adequate security over critical systems and that fire suppression devices appropriate for electrical equipment be maintained within the premises of data centers.

The Shops data processing manager stated that the cited servers were temporarily stored in the information technology office to permit easy access for testing purposes. He further stated that a fire suppression device was missing from the Shops data center due to oversight.

Failure to store critical systems within the protected confines of the data center, and maintain appropriate fire suppression devices, increases the risk of unauthorized access to the critical systems and unsuccessful suppression of a fire and/or damage to critical systems, which may expose employees to dangerous conditions and result in the loss of critical systems.

#### **Recommendation 24**

We recommend that Shops:

- a. Relocate the critical servers to the Shops data center.
- b. Install a fire suppression device appropriate for electrical equipment in the data center.

#### **Campus Response**

We concur:

- a. The antivirus server in question was relocated to the data center during the time of audit. The NBC server will be moved as part of a system upgrade and VM migration scheduled for January 31, 2010.
- b. A fire suppression device was installed in the data center. Corrective action on this issue is complete.

#### **DISPOSITION OF PROTECTED DATA**

Shops did not wipe hard drives to ensure secure disposition of protected data.

We found that hard drives of old machines were not destroyed or wiped clean and were retained and stored in the Shops data center.

The CSULB *Records Management Standard* states that to protect the confidentiality of information and the related privacy rights of CSULB students, faculty, staff, donors, patrons, vendors, and others, Level 1 and Level 2 information contained in all software and/or computer files, storage media devices, and hard copy must be sanitized prior to disposal. The sanitization process ensures that recovery of information is not possible. Several methods can be used to sanitize media; however, the two major types of sanitization are clearing and destroying. This standard applies to all records, regardless of medium held by CSULB and all employees of CSULB and CSULB auxiliary organizations.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the secure disposition of protected data contained in auxiliary files and systems.

The Shops controller/CFO stated that the hard drives were stored without proper data wiping as a result of oversight, and there were only a few disposed machines because of the lack of computer turnover in recent years due to the cycle of the technology replacement service program.

Inadequate control over equipment assets, especially those containing protected data, increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

### **Recommendation 25**

We recommend that Shops implement a process to ensure that hard-drive wiping is performed and sufficiently documented.

### **Campus Response**

We concur. Shops will implement a formal process for hard-drive wiping/destruction in accordance with the above recommendation. Currently, new vendors are being targeted for performing this function due to bankruptcy of the initial vendor. Estimated date of completion is January 31, 2010.

## **DATA CONFIDENTIALITY FORMS**

Shops personnel with access to critical systems and protected data were not required to complete data confidentiality forms.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that employees complete a data confidentiality form prior to being granted access to critical systems and protected data.

The Shops controller/CFO stated that Shops had not required the completion of data confidentiality forms because it was unaware of this requirement.

Failure to obtain data confidentiality forms from employees with access to critical systems and protected data increases the risk of inappropriate disclosure of data and auxiliary exposure to liability for any such disclosures.

#### **Recommendation 26**

We recommend that Shops:

- a. Establish a policy requiring data confidentiality forms from all employees prior to granting them access to critical systems and protected data.
- b. Obtain completed forms from personnel who currently have access to such systems and data.

#### **Campus Response**

We concur. Shops will implement a process requiring the use of data confidentiality forms and will ensure that these forms are completed for personnel with access to such systems and data. Estimated date of completion is January 31, 2010.

**ASSOCIATED STUDENTS,**  
**CALIFORNIA STATE UNIVERSITY, LONG BEACH**

**OPERATING AND ADMINISTRATIVE AGREEMENTS**

Certain written agreements between the Associated Students, California State University, Long Beach (AS) and third parties did not include proper indemnification provisions, were not executed in a timely manner, or lacked contractual terms to address information security and data confidentiality.

We found that:

- ▶ Nine agreements did not indemnify the State of California.
- ▶ One agreement did not indemnify the State of California, CSU Trustees, and the campus and was not signed until 120 days after the inception date.
- ▶ One agreement with a third-party service provider for the secure disposal of AS hard drives that may contain protected data lacked contractual terms to address information security and data confidentiality.

EO 849, *California State University Insurance Requirements*, dated February 5, 2003, states that auxiliary organizations shall agree to indemnify, defend, and save harmless the State of California, the Trustees of the CSU, the campus, and the officers, employees, volunteers, and agents of each of them from any and all loss, damage, or liability that may be suffered or incurred by state, caused by, arriving out of, or in any way connected with the operations of the auxiliary.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that business arrangements be supported by complete, written agreements that are executed in a timely manner.

The AS executive director stated that the agreements were prepared by AS's legal counsel, using an outdated template that did not include the updated CSU indemnification provisions. He also stated that the agreement signed after its inception date was the renewal of an existing agreement that expired during the summer when authorized signers were unavailable and added that the contract was executed in order to preserve revenue flow. He further stated that the AS had a practice to sanitize all hard drives known to contain confidential data prior to delivery to the third-party and therefore did not see a need for the contractual terms to address information security and data confidentiality.

The absence of complete and/or timely written agreements with appropriate indemnification provisions and contractual terms for information security and data confidentiality increase the risk of misunderstandings and miscommunications regarding rights and responsibilities, subjects the

auxiliary and CSU to potential liability, and may compromise compliance with statutory information security requirements.

### **Recommendation 27**

We recommend that AS:

- a. Ensure that all future agreements include an appropriate indemnification provision.
- b. Ensure that all future agreements are executed prior to inception.
- c. Amend the cited agreement for the secure disposal of AS hard drives to include appropriate provisions for information security and data confidentiality responsibilities and indemnification, and consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities and the confidentiality of data for all vendor service agreements relating to access to protected records or data, or update its own standard agreement to include such references.

### **Campus Response**

We concur. ASI has provided its legal counsel with an updated template containing the appropriate indemnification provisions. Addenda to the existing agreements have been executed to correct the indemnification clause. A tickler file has been established to provide advance notice of agreement expiration dates so that extensions or renewals are executed prior to inception. A Confidential Information Addendum has been executed with the current provider of e-waste disposal services. We will further consider adapting the CSU General Provisions of Information Technology Acquisitions for our purchasing purposes. Corrective action on this item is complete.

## **SEGREGATION OF DUTIES**

Certain duties and responsibilities related to payroll processing were not adequately segregated at AS.

We found that the person who processed personnel action forms could also process payroll, while the person who processed payroll could also process personnel action forms.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.6, *Payroll*, states that the auxiliary should establish a written internal controls system that

ensures payroll preparation is segregated from the general ledger function and other payroll functions such as hiring authorization, timekeeping, and distribution of checks.

The AS executive director stated that in order to minimize the number of staff with access to confidential personnel data, the HR manager and payroll technician were assigned as backups for each other and only performed each other's duties when necessitated by extended absences.

Inadequate segregation of duties increases the risk that errors and irregularities will not be detected in a timely manner.

### **Recommendation 28**

We recommend that AS appropriately segregate certain payroll processing functions or institute mitigating procedures approved by the campus CFO.

### **Campus Response**

We concur. The payroll and human resource functions have been segregated. The accounting manager now serves as the backup for payroll. The ASI director of administrative services now serves as the backup for human resources. Corrective action on this item is complete.

## **CASH RECEIPTS AND HANDLING**

Administration of cash receipts at AS required improvement.

We found that:

- ▶ Pre-numbered receipts at the Child Development Center were not periodically reconciled to the receipt book (with carbon copies) or to the cash receipts journal by an independent person.
- ▶ The safe combination at the Recycling Center was not changed after a change in personnel that had access to the safe.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.1, *Cash*, states that the auxiliary should receive cash in a consistent manner utilizing systems that ensure integrity of existing internal controls.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates adequate administration and safeguarding of cash receipts.

The AS executive director stated that management was unaware of the cash-handling activities taking place at the Child Development Center, and the change of personnel with access to the safe at the Recycling Center was not reported to management as required.

Inadequate administration of cashiering receipts increases the risk of loss or misappropriation of funds.

### **Recommendation 29**

We recommend that AS:

- a. Periodically perform an independent reconciliation of pre-numbered receipts to the receipt book (with carbon copies) or to the cash receipts journal at the Child Development Center.
- b. Promptly change the safe combination at the Recycling Center and reiterate to staff that future changes in personnel with safe access should be promptly reported.

### **Campus Response**

We concur. The Child Development Center director has been assigned the responsibility of reconciling the pre-numbered receipts to the cash receipts journal at the Child Development Center. ASI's policy of changing safe combinations after changes in personnel has been reiterated with the Recycling Center supervisor. Corrective action on this item is complete.

## **PURCHASING AND ACCOUNTS PAYABLE**

Certain AS cash disbursements were not appropriately authorized and/or supported by sufficient and appropriate documentation.

We reviewed 40 cash disbursements and five travel reimbursements and found that:

- ▶ In two instances, the employees requesting the expenditure were not listed as authorized requesters on the signature authorization cards.
- ▶ In one instance, neither the employee requesting the expenditure nor the employee approving the expenditure were listed as an authorized requester/approver on the signature authorization card.
- ▶ In one instance, the employee approving the expenditure was not listed as an authorized approver on the signature authorization card.
- ▶ In one instance, the disbursement was not supported by either a packing slip or second copy of the purchase order from the requesting department, signed by department personnel showing that the item had been received.

- ▶ In one instance, an employee was reimbursed twice for breakfast and lunch and at amounts above the allowed maximums. In the same instance, a travel authorization form and conference agenda were not provided to accounts payable.
- ▶ In four instances, actual receipts for car rental, air travel, hotel, conference registration, or other items purchased were not provided. Instead, credit card statements or e-mail confirmations were provided to accounts payable.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.1, *Cash*, states that the auxiliary should disburse cash in a consistent manner utilizing systems that ensure integrity of existing internal controls, with annual management review.

The *AS Policy on Travel Expenses and Allowances* states that meals and incidentals will be permitted up to the daily maximum of \$55, and maximum reimbursement amounts are authorized as follows: breakfast for \$10, lunch for \$15, dinner for \$25, and incidentals for \$5. It further states that a travel authorization form must be completed and approved each time an employee travels off-campus on official AS business.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates that all cash disbursements be properly authorized and fully supported.

The AS executive director stated that AS's policies and forms had not been updated to reflect actual practice. He further stated that payment of the employee's lodging was based on the total hotel receipt, which included meals that had been billed to the room, and that the same meals were subsequently included on the employee's expense report in error. He added that purchases of airline travel and car rentals were performed online, and accounts payable had accepted the email confirmations in lieu of actual receipts, which are not always saved by the student travelers.

Lack of appropriate authorization and/or insufficient and appropriate supporting documentation increases the risk of errors, irregularities, and misappropriation of funds.

### **Recommendation 30**

We recommend that AS:

- a. Update existing policies and procedures, as warranted, to reflect current practices.
- b. Reiterate to staff existing cash disbursement policies and procedures regarding appropriate authorization, sufficient and appropriate supporting documentation, and daily maximum meal allowances.

### **Campus Response**

We concur. ASI will update its signature authorization policies to reflect actual practice whereby we accept in limited cases substitute signatures when primary signatories are not available. We will also provide training to reiterate to staff our existing cash disbursement policies and procedures. Estimated date of completion is January 31, 2010.

## **PROPERTY AND EQUIPMENT**

Administration of AS property and equipment was deficient. Both concerns were noted in the prior Auxiliary Organizations audit.

We found that:

- ▶ Six of the twenty assets selected for physical inspection lacked an identification tag. These assets ranged in acquisition cost from \$1,651 to \$29,900.
- ▶ Two assets noted as lost on the 2007 physical inventory count did not have a missing item report or a memo explaining the circumstances surrounding the lost property.

The *AS Policy on Business Property* states that all capitalized assets, with the exception of software, which falls into the category of equipment, will be tagged and added to the AS inventory when it is received and installed. It also states that for items that are lost, destroyed, or stolen, a missing item report must be completed and attached to the disposal form.

The *AS Property Transfer/Disposal Form* states that a copy of the memo sent to the director of administrative services explaining the circumstances surrounding the lost, damaged, or destroyed property should be attached.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.7, *Property and Equipment*, states that the auxiliary should reconcile physical inventories to the general ledger on a timely basis with review by management. It further states that the auxiliary should establish a written system that ensures physical inspection of property and equipment on a service life schedule, proper recording of property and equipment when received, and for labeling of equipment.

The AS executive director stated that all of the items selected for physical verification were present; but due to age or the area where the assets were stored, it is likely that the tags had fallen off. He further stated that the two missing items had no residual book value, and the staff member processing the disposal mistakenly concluded that a missing item report was not required.

Insufficient administration of property and equipment increases the risk that property may be lost or stolen, and misrepresented in the financial statements.

### **Recommendation 31**

We recommend that AS:

- a. Ensure that all equipment is tagged.
- b. Ensure the completion of a missing item report or memo explaining the circumstances surrounding any lost property.

### **Campus Response**

We concur. In accordance with our policy on business property, ASI will conduct a complete physical inventory of its fixed assets. Any missing tags will be replaced and Missing Item Reports will be completed for any items reported as lost, destroyed, or stolen. Procedures for reporting missing items will be reiterated with staff through follow-up training. Estimated date of completion is May 31, 2010.

## **INFORMATION TECHNOLOGY**

### **PASSWORD AND DATA SECURITY**

Password controls and data security were not always adequate for AS systems.

We found that:

- ▶ Password security parameters were inadequate for the ABRA HR and Private Advantage child care systems, as there were no complexity requirements, no password expiration, no restriction for reuse of passwords or access after repeated failed attempts, and no automatic sign-off of users after a period of no use. Further, the minimum password length was four characters instead of the minimum eight characters required by the campus and leading information security industry guidelines.
- ▶ Password security parameters were inadequate for the MAS financial system, as password expiration was set at 180 days, which exceeds leading information security industry guidelines; and there were no restrictions for reuse of passwords or automatic sign-off of users after a period of no use.
- ▶ The ABRA HR, Private Advantage child care, and MAS financial systems, which stored protected data, were not encrypted.

The CSULB *Password Standard* states that to the extent that the password complexity is supported by the respective device, passwords shall contain at least eight characters, and contain characters from each of the following four groups: uppercase letters, lowercase letters, numerals and symbols, and must be significantly different from previous passwords. This standard applies to all individuals

who have or are responsible for an account or any form of access that supports or requires a password on any CSU system, has access to the CSULB network, or stores any non-public CSULB information.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates strong password and login parameters and encryption of any protected/sensitive data residing on auxiliary systems.

The AS executive director stated that the encryption and full security capabilities referred to in the finding are not available features for the commercially purchased software systems used by AS. He further stated that due to the assignment of certain rights and restrictions to its users, management believed that the present securities were adequate for the MAS financial system.

Inadequate password controls may compromise the authentication credentials of user account privileges that are embedded into applications and operating systems; all of which increase the risk of unauthorized access to auxiliary systems and confidential data. Failure to encrypt protected and/or sensitive data could require the auxiliary to notify all affected parties in the event of a breach of security and potentially damage the auxiliary's reputation.

### **Recommendation 32**

We recommend that AS:

- a. Set effective password and login security parameters for the ABRA, Private Advantage, and MAS systems in accordance with campus and leading information security industry guidelines and perform an assessment of password security parameters for all other AS systems.
- b. Apply encryption controls to the ABRA, Private Advantage, and MAS systems and all other AS computers, databases, and file servers that house protected and/or sensitive data.

### **Campus Response**

We concur with qualifications. Currently, the vendors of the ABRA, Private Advantage, and MAS systems do not support the password and login parameters recommended by the auditors, and ASI does not have adequate resources at this time to replace these systems. Likewise, the recommended encryption controls are not supported by the vendors of these systems. The campus and the ASI both accept the risks inherent in not encrypting sensitive personnel information and not applying certain password and login security parameters.

ASI has the following preventative and detective controls in place. It was agreed that these controls protect sensitive data with the best available technology.

- All desktops have been set to automatically lock-out after ten minutes of inactivity.
- All desktops have been set to lock-out after five unsuccessful login attempts.
- Password complexity for the Windows operating system meets the requirements stated in the CSULB Password Standard.
- Password expiration for the Windows operating system is being reset to expire every 90 days for all users with access to the MAS, Private Advantage, and ABRA systems.

In addition, the following is being implemented:

- The server on which the MAS, Private Advantage, and ABRA databases reside is being moved behind the campus hardware firewall.
- The Private Advantage software is being replaced by a new program with better encryption and password complexity capabilities.

Estimated date of completion for these actions is March 31, 2010.

## **SYSTEM BACKUPS**

Backups for AS systems with protected data were not encrypted when stored locally or when in transit to the off-site storage facility managed by a third party.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

Title 5 §42401 and §42402 indicate that the campus president shall require that auxiliary organizations operate in conformity with policy of the Board of Trustees and the campus. One of the objectives of the auxiliary organizations is to provide fiscal procedures and management systems that allow effective coordination of the auxiliary activities with the campus in accordance with sound business practices. Sound business practice mandates the encryption of protected data contained on auxiliary systems and backups.

The AS executive director stated that AS had encryption software available for this purpose, but had not implemented it due to workload issues.

Inadequate security of system backups increases the risk of inappropriate access to protected data and the possible ramifications of required public notifications should backups be lost when unencrypted.

### **Recommendation 33**

We recommend that AS encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure.

### **Campus Response**

We concur. ASI has started encrypting system backups with protected data. Corrective action on this item is complete.

## **VENDOR MASTER FILE**

Access to add/edit vendor data in the AS vendor master file was not adequately controlled and resulted in an inadequate segregation of duties.

We found that users granted the “AP” user role were able to add/edit vendor data in the AS vendor master file and also able to approve and process invoice payments, as well as perform all other accounts payable functions.

EO 698, *Board of Trustees Policy for The California State University Auxiliary Organizations*, dated March 3, 1999, states that the review of auxiliary organizations will be used to determine appropriate separation of duties, safeguarding of assets, and reliability and integrity of information.

The *Compilation of Policies and Procedures for California State University Auxiliary Organizations* sets sound business practice guidelines for auxiliary organizations operating within the CSU system. Section 8.9.1, *Cash*, states that the auxiliary should establish a written internal controls system that ensures cash receipts and disbursements are conducted with appropriate segregation of duties.

The AS executive director stated that a significant portion of AS vendors are actually students to whom AS issues reimbursements. He added that the accounts payable technician had been given the ability to set-up new vendors in order to expedite the processing of these payments. He further stated that AS believed mitigating detective controls were sufficient to address any concerns.

Failure to maintain adequate control over access to the vendor master file increases the risk of fraudulently misdirected payments.

### **Recommendation 34**

We recommend that AS ensure that users with accounts payable processing duties are restricted from add/edit access to the vendor master file.

**Campus Response**

We concur. We have eliminated access to the vendor master file for all users assigned to the accounts payable role. Corrective action on this item is complete.

---

## **APPENDIX A: PERSONNEL CONTACTED**

<u>Name</u>	<u>Title</u>
<b>CAMPUS</b>	
F. King Alexander	President
John Fugatt	Manager, Student Account Services/Cashiering
Maryann Rozanski	Director, Safety, Risk Management and Information Security
Aysu Spruill	Director, Internal Auditing Services
Mary Stephens	Vice President, Administration and Finance
Sharon Taylor	Associate Vice President, Financial Management
<b>CALIFORNIA STATE UNIVERSITY, LONG BEACH FOUNDATION</b>	
Denise Bell	Director, Grants, Contracts and Foundation Programs
Sydney Dawes	Grants and Contracts Administrator
Patti Folsom	Grants and Contracts Administrator
Stephanie Moreno	Associate Director, Human Resources and Administrative Services
Tina Mow	Grants and Contracts Administrator
Brian Nowlin	Associate Executive Director
Greg Raitz	Associate Director, Information Systems and Technology
Alan Ray	Chief Financial Officer
Arlene Reyes	Director, Finance and Accounting
Helen Santana	Supervisor, Parking Operations
Sandra Shereman	Senior Director, Sponsored Programs/Business Development
John Taylor	Payroll Manager
<b>FORTY-NINER SHOPS, INC.</b>	
Camile Alvarez	Payroll Clerk
Margie Benitez	Manager, Nugget Grill and Pub
Kristin Bonetati	Manager, Gifts and Soft Goods
Sandy Brant	Accounts Receivable Clerk
Marylou Cajucom	Cash Room Supervisor
Jason Eisenmann	Receiving Lead
Nancy Green	Director, Human Resources
Salvador Guardado	Manager, Outpost Grill
Patrick Joyce	Manager, Convenient Stores
Jenny Lew	Associate Director, Dining Services
Tess Monzon	Senior Accountant
Edgar Ortiz	Computer Store Sales Associate
Don Penrod	Chief Executive Officer/General Manager
Chano Rios	Data Entry Coordinator
Elizabeth Sanchez	Accountant
Paul Sharar	Manager, Starbucks-Library
Donna Soto	Manager, ID Card Services
Julie Thorpe	Textbook Buyer
Russell Tompkins	Data Processing Manager
Robert de Wit	Controller/Chief Financial Officer
Majid Zahedi	Network Engineer

**ASSOCIATED STUDENTS, CALIFORNIA STATE UNIVERSITY, LONG BEACH**

Marfi Barnes	Human Resources Coordinator
Scott Christopherson-Schorn	Associate Director, Facility Operations
Dave Edwards	Associate Executive Director
Debra Gammage-Wilson	Manager, Human Resources
Richard Haller	Executive Director
Lee Johnson	Recycling Coordinator
David Kleen	Information Technology Manager
Marcy Le Beau	Accounting Manager
Rhonda Marikos	Director, Isabel Patterson Child Development Center
Lisa Molina de la Loza	Assistant Director, Commercial Services
Judy Musselman	Business Services Coordinator
Stewart Ohanesian	Expenditure Technician
Elizabeth Post	Accounts Receivable Technician
Elizabeth Sierra-Leeds	Building Supervisor I
Martiz Ware	Director, Administrative Services

## **STATEMENT OF INTERNAL CONTROLS**

### **A. INTRODUCTION**

Internal accounting and related operational controls established by the State of California, the California State University Board of Trustees, and the Office of the Chancellor are evaluated by the University Auditor, in compliance with professional standards for the conduct of internal audits, to determine if an adequate system of internal control exists and is effective for the purposes intended. Any deficiencies observed are brought to the attention of appropriate management for corrective action.

### **B. INTERNAL CONTROL DEFINITION**

Internal control, in the broad sense, includes controls that may be characterized as either accounting or operational as follows:

#### 1. Internal Accounting Controls

Internal accounting controls comprise the plan of organization and all methods and procedures that are concerned mainly with, and relate directly to, the safeguarding of assets and the reliability of financial records. They generally include such controls as the systems of authorization and approval, separation of duties concerned with recordkeeping and accounting reports from those concerned with operations or asset custody, physical controls over assets, and personnel of a quality commensurate with responsibilities.

#### 2. Operational Controls

Operational controls comprise the plan of organization and all methods and procedures that are concerned mainly with operational efficiency and adherence to managerial policies and usually relate only indirectly to the financial records.

### **C. INTERNAL CONTROL OBJECTIVES**

The objective of internal accounting and related operational control is to provide reasonable, but not absolute, assurance as to the safeguarding of assets against loss from unauthorized use or disposition, and the reliability of financial records for preparing financial statements and maintaining accountability for assets. The concept of reasonable assurance recognizes that the cost of a system of internal accounting and operational control should not exceed the benefits derived and also recognizes that the evaluation of these factors necessarily requires estimates and judgment by management.

#### **D. INTERNAL CONTROL SYSTEMS LIMITATIONS**

There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal accounting and related operational control. In the performance of most control procedures, errors can result from misunderstanding of instruction, mistakes of judgment, carelessness, or other personal factors. Control procedures whose effectiveness depends upon segregation of duties can be circumvented by collusion. Similarly, control procedures can be circumvented intentionally by management with respect to the executing and recording of transactions. Moreover, projection of any evaluation of internal accounting and operational control to future periods is subject to the risk that the procedures may become inadequate because of changes in conditions and that the degree of compliance with the procedures may deteriorate. It is with these understandings that internal audit reports are presented to management for review and use.

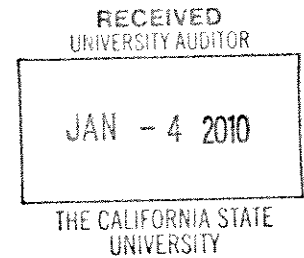


CALIFORNIA STATE UNIVERSITY, LONG BEACH

DIVISION OF ADMINISTRATION AND FINANCE

December 24, 2009

Mr. Larry Mandel  
University Auditor  
California State University  
401 Golden Shore  
Long Beach, California 90802



Re: Response to Auxiliary Organizations Audit #09-16

Dear Larry:

Please find enclosed California State University, Long Beach's response to the above report. The campus is committed to addressing and resolving the issues identified in the audit report.

Please let me know if we can provide you with any additional information.

Sincerely,

A handwritten signature in black ink, appearing to read "Mary Stephens".

Mary Stephens  
Vice President for Administration and Finance

Enclosure

IA-0229

- c: F. King Alexander, President
- Robert de Wit, Controller/Chief Financial Officer, Forty-Niner Shops
- Dave Edwards, Associate Executive Director, Associated Students, Inc.
- Richard Haller, Executive Director, Associated Students, Inc.
- Ted Kadowaki, Associate Vice President, Budget and University Services
- Brian Nowlin, Associate Executive Director, Foundation
- Don Penrod, Chief Executive Officer/General Manager, Forty-Niner Shops
- Alan Ray, Chief Financial Officer, Foundation
- Aysu Spruill, Director, Internal Auditing Services

**AUXILIARY ORGANIZATIONS  
CALIFORNIA STATE UNIVERSITY,  
LONG BEACH**

**Audit Report 09-16**

**CAMPUS**

**INFORMATION TECHNOLOGY**

**PROTECTED DATA ASSESSMENT**

**Recommendation 1**

We recommend that the auxiliaries perform an initial, and then annual, assessment and inventory of protected data on all systems to determine the existence of any protected data, the classification of such data into applicable security levels, and the need for appropriate logical and physical security measures.

**Campus Response**

We concur.

The Foundation currently does an annual assessment and inventory of protected data, and will also include classification of this data by January 31, 2010.

ASI will perform an initial, and then annual, assessment and inventory of protected data on all systems to determine the existence of any protected data, the classification of such data into applicable security levels, and the need for appropriate logical and physical security measures. Estimated date of completion is April 30, 2010.

The Shops will review all internal system data and assess for content falling under the protected data category. A new policy and procedure will be drafted to define the applicable data security classification and the appropriate security there off. Estimated date of completion is January 31, 2010.

**USER ACCESS REVIEWS**

**Recommendation 2**

We recommend that all auxiliaries conduct periodic, documented management reviews of user access for all systems and applications containing protected data, at least annually.

### **Campus Response**

We concur.

The Foundation will conduct and document management review of user access annually beginning January 31, 2010.

ASI will begin conducting annual, documented management reviews of user access for all systems and applications containing protected data. This review will be conducted in conjunction with the assessment and inventory of protected data. Estimated date of completion is April 30, 2010.

The Shops will formalize its user access policy to include a standardized corporate review instead of leaving the responsibility with the respective operation. The policy will include an annual audit/review component as part of the process. Estimated date of completion is January 31, 2010.

## **INFORMATION SECURITY TRAINING**

### **Recommendation 3**

We recommend that the auxiliaries develop and implement an action plan for providing information security awareness training to all employees with access to protected data.

### **Campus Response**

We concur.

Foundation has provided the online security training program by Workplace Answers to its employees.

All ASI employees with access to protected data have completed the Workplace Answers on-line information security training. In addition, ASI will develop and implement an action plan for providing training to new employees prior to their gaining access to confidential data. Estimated date of completion is January 31, 2010.

In collaboration with the CSU campuses, the Chancellor's Office developed a web-based information security awareness training course designed to provide the campus community members with guidance on securing our information resources. This web-based course was extended to the Forty-Niner Shops to help safeguard auxiliary information as well as university data. This training course was provided to Shops personnel during the month of August 2009 and administered through the campus Information Security Office.

**CALIFORNIA STATE UNIVERSITY, LONG BEACH FOUNDATION**

**FACILITIES AGREEMENTS**

**Recommendation 4**

We recommend that the Foundation ensure that all future use agreements include appropriate indemnification provisions.

**Campus Response**

We concur. The Foundation will ensure appropriate indemnification is included in all future use agreements. Corrective action on this issue is complete.

**OPERATIONAL COMPLIANCE**

**Recommendation 5**

We recommend that the Foundation develop and adopt a written risk management policy, including procedures to actively identify, analyze, quantify, and manage risk.

**Campus Response**

We concur. The Foundation currently utilizes the risk management policy of the campus and will develop and adopt its own risk management policy. Estimated date of completion is April 30, 2010.

**CASH RECEIPTS AND HANDLING**

**Recommendation 6**

We recommend that the Foundation:

- a. Reiterate existing cash-handling policies to all project staff and increase enforcement efforts to ensure that all receipts are processed in a timely manner.
- b. Furnish locked security bags to all project directors to ensure that receipts are adequately safeguarded until deposited.

**Campus Response**

We concur. These recommendations were completed during fieldwork. An e-mail was sent to all project directors reminding them of the cash-handling policies and locked security bags have been provided to all projects transporting sensitive material. Corrective action on this issue is complete.

## PROPERTY AND EQUIPMENT

### Recommendation 7

We recommend that the Foundation:

- a. Update its inventory procedures to include the role of the third-party service provider, and clearly define and communicate roles and responsibilities for all Foundation departments and sponsored project directors involved in the physical inventory process.
- b. Promptly resolve disposition of the missing assets, including follow-up with the sponsored project directors.
- c. Ensure that all future agreements with third parties for inventory services include appropriate insurance and indemnification provisions.

### Campus Response

We concur.

- a. Inventory procedures will be updated and the roles for all Foundation departments and sponsored project directors involved in the physical inventory process will be defined and communicated by April 30, 2010.
- b. All the items that were not found during the initial physical inventory were cleared during audit fieldwork. Corrective action on this issue is complete.
- c. Purchase orders now contain a link to CSU terms and conditions, so future agreements with vendors will contain that information. Corrective action on this issue is complete.

## TRUSTS AND OTHER LIABILITIES

### Recommendation 8

We recommend that the Foundation:

- a. Complete a review of all custodial trust accounts and determine, within 60 days, which accounts contain state funds.
- b. Certify that none of the following specific and similar monies reside in Foundation trust accounts:
  - Gifts to the university, its units and programs.
  - Contracts and grants awarded to the university.
  - Pre-award indirect cost recovery reimbursements.
  - Foundation net operating surplus designated for use by the campus.
  - Fees for continuing education courses provided by the university.

- Fees for university events, workshops, conferences, institutes, special projects, and programs.
  - Reimbursements for services and products provided to auxiliary enterprises and organizations paid from General Fund and/or CSU operating fund monies.
  - Rental fees for university facilities, except those facilities that have been leased to the auxiliary by the campus.
  - Student fees and other general fees pursuant to the CSU student fee policy.
  - Monies held by the Foundation via contract with the campus.
- c. Submit to the Office of the University Auditor, within 60 days, a list of those trust accounts which have been deemed appropriate to remain in the custody of the Foundation and comprehensive documentation to support the sources of funds for those trust accounts.
- d. Move those state funds identified in “a” above to campus accounts within six months.

### **Campus Response**

We concur.

- a. The review of accounts will be completed by January 26, 2010.
- b. The review will certify that none of the listed accounts reside in Foundation trust accounts by January 26, 2010.
- c. The list of trust accounts deemed appropriate to remain in the custody of the Foundation with corresponding documentation will be submitted to the Office of the University Auditor by January 26, 2010.
- d. A plan will be developed to move state funds from the Foundation to campus accounts. During this time while state funds are retained at the Foundation, state will have full control over the funds. Estimated date of completion is April 30, 2010.

## **AUXILIARY PROGRAMS**

### **Recommendation 9**

We recommend that the Foundation:

- a. Update its existing post-award administration procedures and implement a process that requires grants and contracts administrators to track the submission of deliverables.
- b. Reiterate the importance of timely submission of deliverables and implement a process to ensure compliance.
- c. Ensure that conflict of interest forms are kept current.
- d. Enforce its existing procedures to ensure that projects are closed out timely, within 90 days.

**Campus Response**

We concur.

- a. The policy will be reiterated to Grants & Contracts administrators.
- b. The Foundation will reiterate with project directors the importance of timely submission with the 120/90/60/45/30-day notices. This process is included in the current close-out checklist.
- c. The Foundation's procedures are to keep the conflict of interest forms current and this will be reiterated with administrators.
- d. The Foundation will reiterate with administrators the importance of closing out projects on a timely basis.

Estimated date of completion is January 31, 2010.

**INFORMATION TECHNOLOGY****PASSWORD AND DATA SECURITY****Recommendation 10**

We recommend that the Foundation:

- a. Set effective password security parameters for IFAS in accordance with campus and security industry guidelines.
- b. Apply encryption controls to all Foundation computers, databases, and file servers that house protected or sensitive data.
- c. Implement a formal DMZ between internal network resources and Internet-accessible devices.

**Campus Response**

We concur.

- a. The password length requirement was changed to eight characters during audit fieldwork.
- b. Currently, the application vendor has indicated that the encryption feature is not currently available, but an enhancement request has been created. The Foundation has implemented preventative and detective controls, which were discussed with the auditors. It was agreed that these controls protect sensitive data with the best available technology. The campus and the Foundation both accept the risks inherent in not encrypting sensitive information.
- c. The web server was moved to the DMZ during audit fieldwork.

Corrective action on this issue is complete.

## **SYSTEM BACKUPS**

### **Recommendation 11**

We recommend that the Foundation encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure.

### **Campus Response**

We concur. The Foundation will implement a method to encrypt system backups. Estimated date of completion is February 28, 2010.

## **ENVIRONMENTAL CONTROLS**

### **Recommendation 12**

We recommend that the Foundation evaluate the feasibility of another means of fire suppression or consider relocation of Foundation servers to the campus data center.

### **Campus Response**

We concur. The Foundation has begun to evaluate the feasibility of alternative fire suppression methods in the main server room. Should such alternative methods prove impracticable or cost prohibitive, the relocation of Foundation servers will be evaluated. The estimated date of completion is April 30, 2010.

## **DISPOSITION OF PROTECTED DATA**

### **Recommendation 13**

We recommend that the Foundation implement a process to ensure that hard-drive wiping is performed and sufficiently documented.

### **Campus Response**

We concur. A Media Sanitation section was added to the Information Privacy and Security Policy. A Media Sanitation Log was created. A section on destroying obsolete media was added to the Records Retention Policy and Procedures. A "Method of Media Sanitation" was added to the Retired Fixed Asset Form. Corrective action on this issue is complete.

## **REMOTE SERVER ACCESS**

### **Recommendation 14**

We recommend that the Foundation replace Telnet remote access with a more secure remote access protocol (such as secure shell) or enforce internal firewall restrictions on Telnet such that it could only be accessed once a virtual private network (VPN) connection has been established.

**Campus Response**

We concur. Remote access is now secured via secure shell (SSH). Corrective action on this issue is complete.

**FORTY-NINER SHOPS, INC.**

**OPERATING, ADMINISTRATIVE AND FACILITIES AGREEMENTS**

**Recommendation 15**

We recommend that Shops:

- a. Establish a written agreement with the payroll service provider and for all vendor service agreements relating to access to protected records or data, consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities and the confidentiality of data.
- b. Ensure that all future agreements are executed prior to inception.
- c. Ensure that all future agreements include an appropriate indemnification provision.

**Campus Response**

We concur.

- a. The Shops will work with the payroll service provider (ADP) to establish a service agreement and ensure that all vendor service agreements relating to access for protected data contain the proper CSU general provisions for information security.
- b. The Shops will ensure proper execution deadlines are met for all future agreements and escalate through campus management as is appropriate.
- c. The Shops will enforce the inclusion of appropriate indemnification language in all future agreements.

Estimated date of completion is May 31, 2010.

**OPERATIONAL COMPLIANCE**

**RISK MANAGEMENT**

**Recommendation 16**

We recommend that Shops develop and adopt a written risk management policy, including procedures to actively identify, analyze, quantify, and manage risk.

**Campus Response**

We concur. The Shops management has drafted a Risk Management Policy which has been presented to the Board of Directors on 12/11/09 for initial review and comment. Upon approval the policy will be implemented accordingly. Estimated date of completion is May 31, 2010.

## EMPLOYEES

### Recommendation 17

We recommend that Shops reinstate post-employment health benefits for its full-time employees to ensure the comparability of salaries, wages, and benefits for its full-time employees in relation to those provided campus employees performing substantially similar services.

### Campus Response

The University has explored the full context of Recommendation 17 with Shops' management and its governing board.

The compensation comparability standard raised in the finding applies only to the full-time employees holding positions substantially similar to those positions within the CSU system. That standard for only those positions extends to employee salaries, working conditions, and benefits in total, i.e., the total of these factors must be competitive with CSU employment in the same class.

Shops approached with considerable diligence and deliberation the action to end post-employment medical coverage for hires beginning January 1, 2009. The magnitude of the future financial obligation for such coverage, coupled with the statutory *self-supporting* standard for auxiliary commercial operations, required prudent and timely action (FASB 106 and Education Code Section 89905).

Absent, however, was a formal internal compensation policy framework and plan within which Shops acted that would more fully demonstrate compliance with Education Code Section 89900(c) and Title 5, Section 42405.

The University will work closely with Shops' management and the Board of Directors to assure the adoption of a clear policy and plan that supports the action taken on this issue. Estimated date of completion is May 31, 2010.

## SEGREGATION OF DUTIES

### Recommendation 18

We recommend that Shops appropriately segregate certain accounts receivable duties in its accounting office or institute mitigating procedures approved by the campus CFO.

### Campus Response

We concur. The Shops agree to further segregate the accounts receivable (A/R) function to be compliant with the recommendation. The Shops A/R activities consist of less than a full time task which is being further divided amongst staff. The A/R policy and procedure has been revised accordingly to address specific segregation of duties. Corrective action on this issue is complete.

## PETTY CASH AND CHANGE FUNDS

### PETTY CASH

#### Recommendation 19

We recommend that Shops:

- a. Update its petty cash policy to include a dollar threshold.
- b. Reiterate to staff petty cash policies and procedures and prohibit supplements to petty cash funds with funds from other sources.

#### Campus Response

We concur:

- a. The Shops petty cash policy is under revision with a stipulated threshold of \$200.
- b. The revised policy will include new language around the refunding process and prohibition of supplements. Staff will also be informed of the policy updates.

Estimated date of completion is May 31, 2010.

### CHANGE FUNDS

#### Recommendation 20

We recommend Shops:

- a. Establish a specific vault fund amount.
- b. Maintain the vault fund separate from cash collected from daily sales and periodically reconcile the general ledger record of cash on hand to actual cash on hand.
- c. Perform periodic, documented independent cash counts of the vault fund.

#### Campus Response

We concur.

- a. The Shops is currently drafting a separate vault policy that will specify stated cash balances for the various economic cycles that occur during the school year.
- b. As part of the new policy vault funds will remain isolated from daily sales activity and reconciled accordingly.

c. Policy will include independent (other than cash room) audit of the vault funds.

Estimated date of completion is May 31, 2010.

## **PROPERTY AND EQUIPMENT**

### **Recommendation 21**

We recommend that Shops promptly perform an independent physical inventory of its property and equipment, including reconciliation to the general ledger, and establish procedures to conduct periodic, independent physical counts on a regular basis.

### **Campus Response**

We concur. The Shops updated its Fixed Asset/Property control policy to include a formally established physical audit and reconciliation process. Estimated date of completion is January 31, 2010.

## **INFORMATION TECHNOLOGY**

### **PASSWORD SECURITY**

#### **Recommendation 22**

We recommend that Shops set effective password security parameters for all Shops systems, including Active Directory in accordance with campus and security industry guidelines.

#### **Campus Response**

We concur. The Shops will revisit its password security parameters for each of its systems and move towards a standardized process in accordance with proposed guidelines for those systems falling short. Estimated date of completion is May 31, 2010.

### **SYSTEM BACKUPS**

#### **Recommendation 23**

We recommend that Shops promptly store system backups in a fireproof safe and contract with an off-campus backup storage facility for the regular storage of system backups.

#### **Campus Response**

We concur. The Shops is currently evaluating several system backup options and will implement the best value solution upon assessment completion. Estimated date of completion is May 31, 2010.

## **SYSTEM SECURITY AND ENVIRONMENTAL CONTROLS**

### **Recommendation 24**

We recommend that Shops:

- a. Relocate the critical servers to the Shops data center.
- b. Install a fire suppression device appropriate for electrical equipment in the data center.

### **Campus Response**

We concur.

- a. The Anti-Virus server in question was relocated to the Data Center during the time of audit. The NBC server will be moved as part of a system upgrade and VM migration scheduled for January 31, 2010.
- b. A fire suppression device was installed in the data center. Corrective action on this issue is complete.

## **DISPOSITION OF PROTECTED DATA**

### **Recommendation 25**

We recommend that Shops implement a process to ensure that hard-drive wiping is performed and sufficiently documented.

### **Campus Response**

We concur. The Shops will implement a formal process for hard-drive wiping/destruction in accordance with the above recommendation. Currently, new vendors are being targeted for performing this function due to bankruptcy of the initial vendor. Estimated date of completion is January 31, 2010.

## **DATA CONFIDENTIALITY FORMS**

### **Recommendation 26**

We recommend that Shops:

- a. Establish a policy requiring data confidentiality forms from all employees prior to granting them access to critical systems and protected data.
- b. Obtain completed forms from personnel who currently have access to such systems and data.

**Campus Response**

We concur. The Shops will implement a process requiring the use of data confidentiality forms and will ensure that these forms are completed for personnel with access to such systems and data. Estimated date of completion is January 31, 2010.

**ASSOCIATED STUDENTS,**  
**CALIFORNIA STATE UNIVERSITY, LONG BEACH**

**OPERATING AND ADMINISTRATIVE AGREEMENTS**

**Recommendation 27**

We recommend that AS:

- a. Ensure that all future agreements include an appropriate indemnification provision.
- b. Ensure that all future agreements are executed prior to inception.
- c. Amend the cited agreement for the secure disposal of AS hard drives to include appropriate provisions for information security and data confidentiality responsibilities and indemnification, and consider using the CSU General Provisions for Information Technology Acquisitions, which includes references for information security responsibilities and the confidentiality of data for all vendor service agreements relating to access to protected records or data, or update its own standard agreement to include such references.

**Campus Response**

We concur. ASI has provided its legal counsel with an updated template containing the appropriate indemnification provisions. Addenda to the existing agreements have been executed to correct the indemnification clause. A tickler file has been established to provide advance notice of agreement expiration dates so that extensions or renewals are executed prior to inception. A Confidential Information Addendum has been executed with the current provider of e-waste disposal services. We will further consider adapting the CSU General Provisions of Information Technology Acquisitions for our purchasing purposes. Corrective action on this item is complete.

**SEGREGATION OF DUTIES**

**Recommendation 28**

We recommend that AS appropriately segregate certain payroll processing functions or institute mitigating procedures approved by the campus CFO.

**Campus Response**

We concur. The payroll and human resource functions have been segregated. The Accounting Manager now serves as the back-up for payroll. The ASI Director of Administrative Services now serves as the back-up for human resources. Corrective action on this item is complete.

## CASH RECEIPTS AND HANDLING

### Recommendation 29

We recommend that AS:

- a. Periodically perform an independent reconciliation of pre-numbered receipts to the receipt book (with carbon copies) or to the cash receipts journal at the Child Development Center.
- b. Promptly change the safe combination at the Recycling Center and reiterate to staff that future changes in personnel with safe access should be promptly reported.

### Campus Response

We concur. The Child Development Center Director has been assigned the responsibility of reconciling the pre-numbered receipts to the cash receipts journal at the Child Development Center. ASI's policy of changing safe combinations after changes in personnel has been reiterated with the Recycling Center Supervisor. Corrective action on this item is complete.

## PURCHASING AND ACCOUNTS PAYABLE

### Recommendation 30

We recommend that AS:

- a. Update existing policies and procedures, as warranted, to reflect current practices.
- b. Reiterate to staff existing cash disbursement policies and procedures regarding appropriate authorization, sufficient and appropriate supporting documentation, and daily maximum meal allowances.

### Campus Response

We concur. ASI will update its signature authorization policies to reflect actual practice whereby we accept in limited cases substitute signatures when primary signatories are not available. We will also provide training to reiterate to staff our existing cash disbursement policies and procedures. Estimated date of completion is January 31, 2010.

## PROPERTY AND EQUIPMENT

### Recommendation 31

We recommend that AS:

- a. Ensure that all equipment is tagged.
- b. Ensure the completion of a missing item report or memo explaining the circumstances surrounding any lost property.

### Campus Response

We concur. In accordance with our Policy on Business Property, ASI will conduct a complete physical inventory of its fixed assets. Any missing tags will be replaced and Missing Item Reports will be completed for any items reported as lost, destroyed or stolen. Procedures for reporting missing items will be reiterated with staff through follow-up training. Estimated date of completion is May 31, 2010.

## INFORMATION TECHNOLOGY

### PASSWORD AND DATA SECURITY

#### Recommendation 32

We recommend that AS:

- a. Set effective password and login security parameters for the ABRA, Private Advantage, and MAS systems in accordance with campus and leading information security industry guidelines and perform an assessment of password security parameters for all other AS systems.
- b. Apply encryption controls to the ABRA, Private Advantage, and MAS systems and all other AS computers, databases, and file servers that house protected and/or sensitive data.

### Campus Response

We concur with qualifications. Currently, the vendors of the ABRA, Private Advantage and MAS systems do not support the password and login parameters recommended by the auditors, and ASI does not have adequate resources at this time to replace these systems. Likewise, the recommended encryption controls are not supported by the vendors of these systems. The campus and the ASI both accept the risks inherent in not encrypting sensitive personnel information and not applying certain password and login security parameters.

ASI has the following preventative and detective controls in place. It was agreed that these controls protect sensitive data with the best available technology.

- All desktops have been set to automatically lock-out after ten minutes of inactivity.
- All desktops have been set to lock-out after five unsuccessful login attempts.
- Password complexity for the Windows operating system meets the requirements stated in the CSULB Password Standard.
- Password expiration for the Windows operating system is being reset to expire every ninety days for all users with access to the MAS, Private Advantage and ABRA systems.

In addition, the following is being implemented:

- The server on which the MAS, Private Advantage and ABRA databases reside is being moved behind the campus hardware firewall.
- The Private Advantage software is being replaced by a new program with better encryption and password complexity capabilities.

Estimated date of completion for these actions is March 31, 2010.

## **SYSTEM BACKUPS**

### **Recommendation 33**

We recommend that AS encrypt system backups with protected data and ensure that the off-site transfer and storage of backups is secure.

### **Campus Response**

We concur. ASI has started encrypting system back-ups with protected data. Corrective action on this item is complete.

## **VENDOR MASTER FILE**

### **Recommendation 34**

We recommend that AS ensure that users with accounts payable processing duties are restricted from add/edit access to the vendor master file.

### **Campus Response**

We concur. We have eliminated access to the vendor master file for all users assigned to the accounts payable role. Corrective action on this item is complete.

THE CALIFORNIA STATE UNIVERSITY  
OFFICE OF THE CHANCELLOR



BAKERSFIELD

January 22, 2010

CHANNEL ISLANDS

CHICO

**MEMORANDUM**

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FROM: Charles B. Reed  
Chancellor

A handwritten signature in black ink, appearing to read "Charles B. Reed", is written over the printed name of the Chancellor.

FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 09-16 on *Auxiliary Organizations*,  
California State University, Long Beach

LONG BEACH

LOS ANGELES

In response to your memorandum of January 22, 2010, I accept the response as submitted with the draft final report on *Auxiliary Organizations*, California State University, Long Beach.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS