

**FISMA**

**CALIFORNIA STATE UNIVERSITY,  
BAKERSFIELD**

**Audit Report 07-12  
August 14, 2008**

---

**Members, Committee on Audit**

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

---

**Staff**

University Auditor: Larry Mandel  
Senior Director: Michelle Schlack  
IT Audit Manager: Greg Dove  
Senior Auditor: Dominick Owens

---

**BOARD OF TRUSTEES**

**THE CALIFORNIA STATE UNIVERSITY**

---

## CONTENTS

Executive Summary .....	1
Introduction.....	4
Statement of Internal Controls .....	4
Purpose .....	5
Scope and Methodology.....	6

---

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Cash Receipts.....	8
Main Cashiering .....	8
Satellite Cashiering .....	10
Non-Sufficient Funds .....	11
Student Fees .....	11
Application Fee Reconciliation.....	12
Accounts Receivable.....	13
Write-Off of Uncollectible Debt .....	13
Employee Accounts Receivable.....	14
Payroll and Personnel .....	15
Employee Eligibility Verification .....	15
Local Escheat Account.....	16
Fixed Assets.....	17
Information Technology .....	19
Information Security Oversight.....	19
Security of Vendor Supported Systems .....	21
PeopleSoft Access and Passwords .....	22
Trust Funds .....	24

## **APPENDICES**

APPENDIX A:	Personnel Contacted
APPENDIX B:	Campus Response
APPENDIX C:	Chancellor's Acceptance

---

## **ABBREVIATIONS**

AD	Active Directory
AVC	Antelope Valley Campus
CMS	Common Management Systems
CSU	California State University
CSUB	California State University, Bakersfield
EO	Executive Order
FISMA	Financial Integrity and State Manager's Accountability Act
GC	Government Code
HCM	Human Capital Management
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NSF	Non-Sufficient Funds
SAM	State Administrative Manual
SCO	State Controller's Office
SCF	Separation Clearance Form
SHS	Student Health Services
SUAM	State University Administrative Manual

---

## EXECUTIVE SUMMARY

The California Legislature passed the Financial Integrity and State Manager's Accountability Act (FISMA) of 1983, Government Code (GC) Sections 13400 through 13407. This act requires state agencies to establish and maintain a system of internal accounting and administrative control. To ensure that the requirements of this act are fully complied with, state entities with internal audit units are to complete biennial internal control audits (covering accounting and fiscal compliance practices) in accordance with the *International Standards for the Professional Practice of Internal Auditing* (Institute of Internal Auditors) as required by GC, Section 1236. The Office of the University Auditor of the California State University (CSU) is currently responsible for conducting such audits within the CSU.

California State University, Bakersfield (CSUB) management is responsible for establishing and maintaining adequate internal control. This responsibility, in accordance with GC, Sections 13402 et seq., includes documenting internal control, communicating requirements to employees, and assuring that 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 accounting and administrative control are to provide management with reasonable, but not absolute, assurance that:

- ▶ Assets are safeguarded against loss from unauthorized use or disposition.
- ▶ Transactions are executed in accordance with management's authorization and recorded properly to permit the preparation of reliable financial statements.
- ▶ Established controls are not only effective but also promote operational efficiency.
- ▶ Financial operations are conducted in accordance with policies and procedures established in the State Administrative Manual, Education Code, Title 5, and Trustee policy.

We visited the CSUB campus from February 4, 2008, through April 3, 2008, and made a study and evaluation of the accounting and administrative control in effect as of April 3, 2008. This report represents our biennial review.

Our study and evaluation revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the campus did not maintain adequate internal control over the following areas: cash receipts, accounts receivable, payroll and personnel, fixed assets, information technology, and trust funds. One of the 14 findings was a repeat from the prior FISMA audit. These conditions, along with other weaknesses, are described in the executive summary and body of this report.

In our opinion, except for the effect of the weaknesses described above, CSUB's accounting and administrative control in effect as of April 3, 2008, 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.

### **CASH RECEIPTS [8]**

Cash control weaknesses were found at the main cashier's office. Checks were not always deposited within ten working days of receipt or endorsed on the day they were received, and cashiers were not responsible for counting cash tills at the beginning of the day or the start of a new cashiering session to verify the amount of the start-up change fund. Further, payments (cash and checks) received via mail at the general accounting office were opened, sorted, and transferred to main cashiering office without the use of transfer receipts, and checks received in the mail not payable to the CSUB were not pre-listed by the person opening the mail. Documentation of individuals with access to the safe was outdated. Cash control weaknesses were found at one of the two satellite cashiering areas visited. The satellite cashiering locations reviewed included the Antelope Valley campus and student health services (SHS). At SHS, accountability for cash receipts was not always localized which is a repeat finding from the prior FISMA review. Returned checks holds were not placed on five of ten accounts that showed an outstanding unrecovered non-sufficient funds check balance. In addition, new fees and changes to existing fees were not always approved, and the campus could not provide evidence that application fee reconciliations were prepared since the prior FISMA review.

### **ACCOUNTS RECEIVABLE [13]**

Write-offs of uncollectible debt were not approved, as the campus did not seek discharge from accountability from the State Controller's Office (SCO) for those accounts written-off over \$1,000 and documentation to support the write-off of receivables with balances each under \$1,000 was not in file. Employee accounts receivable controls were inadequate. A review of 20 outstanding travel advances for 14 employees as of February 2008 disclosed that policies and procedures that impact the system of internal accounting and administrative control for employee accounts receivables had not been fully documented. Lastly, the advance account was not up-to-date and the collection process was not timely or adequate overall for two separated employees with a combined outstanding balance of \$2,924.

### **PAYROLL AND PERSONNEL [15]**

Federal Form I-9, employment eligibility verification, was not always completed timely. A review of 15 new hire transactions disclosed that in three instances, the Form I-9 was not completed within the required three days. Campus escheat account controls were inadequate. A review of 18 undelivered salary warrants that were deposited to a local escheat account between June and October 2007 disclosed

that in 14 instances, the warrants remained unclaimed as of the audit date and showed no documented evidence of employee follow-up or that due-diligence letters were sent to the rightful owners. In addition, there were no policies and procedures on file to address this practice or to properly report the unclaimed property to the SCO after the dormancy period.

## **FIXED ASSETS [17]**

Administration of fixed assets did not ensure that all property was inventoried, identified, and reconciled timely. A complete physical count of all property had not been made and reconciled to the general ledger since the 2002-2004 inventories. Also, verification, tagging, and checkout of 20 laptop computers utilized by campus personnel disclosed that in one instance, an assigned laptop could not be located, in nine instances, the property department did not have equipment custody forms on file, and identification tags were not always attached to campus property.

## **INFORMATION TECHNOLOGY [19]**

The identification and reporting of information security projects was inadequate. There was no comprehensive plan for identifying and prioritizing campus information security needs and for existing information security related projects, there were no projected due dates to help ensure that such projects were completed in a timely manner. In addition, the campus had not developed written security guidelines including the necessary security requirements for systems supported by outsourced vendors or third parties and as a result, security over the runner card system was not adequate and security requirements over the donor system had not been defined. Lastly, account access was not removed from some terminated employees in the PeopleSoft Finance system, and password history was not used in the PeopleSoft Human Capital Management system.

## **TRUST FUNDS [24]**

Cash control, contractual services, and procedural weaknesses were found with the public performance jazz account. Accumulated cash receipts (approximately \$19,922) deposited from the weekend jazz festival on May 16, 2007, were not adequately secured; the music department chair appointed family members to assist in handling security, cash receipts, and bookkeeping for the event; a proper segregation of duties and compensating controls were not maintained for the jazz festival concession sales; and the music department chair was designated the custodian of the change fund, controller of daily count sheets for the cashiers' tills, and was responsible for securing the cash receipts and making the deposit. There were other control issues related to the jazz festival and other department events that are included in the report.

---

## INTRODUCTION

### **STATEMENT OF INTERNAL CONTROLS**

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. The ultimate responsibility for good internal control rests with management.

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, personnel of a quality commensurate with responsibilities, and an effective system of internal review.

#### 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.

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.

Experience indicates that the existence of certain danger signals will usually be indicative of a poorly maintained or vulnerable control system. These symptoms may apply to the organization as a whole or to individual units or activities, and generally include any of the following danger signals:

- ▶ Policy and procedural or operational manuals are either not currently maintained or are non-existent.
- ▶ Lines of organizational authority and responsibility are not clearly articulated or are non-existent.
- ▶ Financial and operational reporting is not timely and is not used as an effective management tool.

- ▶ Line supervisors ignore or do not adequately monitor control compliance.
- ▶ No procedures are established to assure that controls in all areas of operation are evaluated on a reasonable and timely basis.
- ▶ Internal control weaknesses detected are not acted upon in a timely fashion.
- ▶ Controls and/or control evaluations bear little relationship to organizational exposure to risk of loss or resources.

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.

### **PURPOSE**

The principal audit objective was to assess the adequacy of controls and systems to ensure that:

- ▶ Cash receipts are processed in accordance with laws, regulations, and management policies.
- ▶ Receivables are promptly recognized and balances are periodically evaluated.
- ▶ Purchases are made in accordance with laws, regulations, and management policies.
- ▶ Operating fund disbursements are authorized and processed in accordance with laws, regulations, and management policies.
- ▶ Cash disbursements are properly authorized and made in accordance with established procedures, and adequate segregation of duties exists.
- ▶ Payroll/personnel criteria for hiring employees, establishing compensation rates, and authorizing disbursements are controlled and access to personnel and payroll records and processing areas are restricted.
- ▶ Purchase and disposition of fixed assets are controlled and assets are promptly recorded in the subsidiary records.

- ▶ Fiscal information systems are adequately controlled and safeguarded, and adequate segregation of duties exists.
- ▶ Investments are adequately controlled and securities are safeguarded.
- ▶ Trust funds are established in accordance with State University Administrative Manual guidelines.

## **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 year 2006/07 was the primary period reviewed. In certain instances, we were concerned with representations of the most current data; in such cases, the test period was January 2006 to September 2007. Our primary focus was on internal controls. Specifically, we reviewed and tested:

- ▶ Procedures for receipting and storing cash, segregation of duties involving cash receipting, and recording of cash receipts.
- ▶ Establishment of receivables and adequate segregation of duties regarding billing and payment of receivables.
- ▶ Approval of purchases, receiving procedures, and reconciliation of expenditures to State Controller's balances.
- ▶ Limitations on the size and types of operating fund disbursements.
- ▶ Use of petty cash funds, periodic cash counts, and reconciliation of bank accounts.
- ▶ Authorization of personnel/payroll transactions and accumulation of leave credits in compliance with state policies.
- ▶ Posting of the property ledger, monthly reconciliation of the property to the general ledger, and physical inventories.
- ▶ Access restrictions to accounting systems and related computer facilities/equipment, and administration of information technology operations.
- ▶ Procedures for initiating, evaluating, and accounting for investments.
- ▶ Establishment of trust funds, separate accounting, adequate agreements, and annual budgets.

---

INTRODUCTION

We have not performed any auditing procedures beyond April 3, 2008. 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**

### **CASH RECEIPTS**

#### **MAIN CASHIERING**

Cash control weaknesses were found at the main cashier's office.

##### **Main Cashiering**

- ▶ Checks were not always deposited within ten working days of receipt or endorsed on the day they were received. We found 15 (\$36,353) unprocessed checks dated from October 18, 2007, to February 1, 2008, in the cashier's office safe. Additionally, 14 (\$36,053) of the 15 unprocessed receipts were not restrictively endorsed as of our review. The checks were manually endorsed and processed during the audit.
- ▶ Cashiers were not responsible for counting cash tills at the beginning of the day or the start of a new cashiering session to verify the amount of the start-up change fund.
- ▶ The preparation of the consolidated campus deposit was not verified by a second employee. Although the daily deposit worksheet required dual review and signature verification, we found that the practice did not ensure that deposits were verified by a second employee prior to deposit.
- ▶ Payments (cash and checks) received via mail at the general accounting office were opened, sorted, and transferred to main cashiering office for processing without the use of transfer receipts.
- ▶ Checks received in the mail not payable to the California State University, Bakersfield (CSUB) were not pre-listed by the person opening the mail.
- ▶ Documentation of individuals with access to the safe was outdated. We found that safe access records included two individuals who were no longer employed and omitted one new employee with safe access. The list was updated during the audit.

State Administrative Manual (SAM) §8020.1 states that all incoming mail receipts consisting of cash and negotiable instruments, not payable to the state agency, will be pre-listed by the person opening the mail to localize accountability of these assets.

SAM §8021 states that a separate series of transfer receipts will be used to localize accountability for cash or negotiable instruments to a specific employee from the time of its receipt to its deposit. This series of receipts need not be press-numbered. The receiving employee will sign a receipt whenever cash or checks not payable to the state agency are transferred between employees. State agencies will retain copies of these receipts.

SAM §8023 states that all checks, money orders, and warrants received for deposit will be restrictively endorsed for deposit as soon as possible after receipt, but no later than the end of the working day.

SAM §8024 requires the campus to retain a record listing the names of persons knowing the present safe combination and the date the combination was last changed, and to change the safe combination when employees leave a department.

SAM §8032.1 states, in part, that agencies are required to deposit receipts in a timely and economical manner. Agencies that have safes, vaults, money chests, or other comparable storage that is adequate to safeguard cash will accumulate collections until they amount to \$1,000 in cash or \$10,000 in cash, checks, money orders, and warrants (excluding state warrants and state checks), whichever occurs first. Accumulated receipts of any amount will not remain undeposited for more than ten working days.

SAM §20050 states that the elements of a satisfactory system of internal accounting and administrative controls shall include a system of authorization and recordkeeping procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenditures.

The vice president of business and administrative services stated that the campus tills were counted daily at the end of the day but he did not feel additional controls were warranted to again count each till at the beginning of each day. He also stated that the campus did not prepare transfer receipts because they had not been part of the campus procedures in the past. Lastly, he stated that the combination on the safe had been appropriately changed, but the access listing had not been changed due to oversight.

Inadequate control over cash receipts increases campus exposure to loss from inappropriate acts.

### **Recommendation 1**

We recommend that the campus:

- a. Ensure that all checks are restrictively endorsed immediately upon receipt or at minimum, by the end of each day.
- b. Deposit checks in a timely manner and utilize a suspense account to maintain accountability for long-outstanding checks received but not applied as payments.
- c. Establish and implement procedures for counting cash tills at the beginning of the day or the start of a new cashiering session.
- d. Enforce campus deposit procedures for the dual verification of the daily deposits.
- e. Implement procedures for transfer receipts from the general accounting office to the main cashiering office for checks received in the mail.

- f. Establish procedures to prepare a pre-listing of cash and checks received not payable to the university.
- g. Require the safe access log with the written records of individuals with knowledge of the safe to be updated at prescribed frequencies.

### **Campus Response**

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will retrain staff to ensure that the procedures are followed. Target completion date is January 31, 2009.

### **SATELLITE CASHIERING**

Cash control weaknesses were found at one of the two satellite cashiering areas visited.

The satellite cashiering locations reviewed included the Antelope Valley campus (AVC) and student health services (SHS).

#### **Student Health Services**

Accountability for cash receipts was not always localized at SHS. We noted that the four employees responsible for cashiering did not always use their unique swipe card and ID prior to processing transactions, which limited the accountability of cash receipts to a specific employee. This is a repeat finding from the prior Financial Integrity and State Manager's Accountability Act (FISMA) audit.

SAM §20050 states that the elements of a satisfactory system of internal accounting and administrative controls shall include a system of authorization and recordkeeping procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenditures.

The California State University (CSU) Information Security Policy, dated August 2002, states that campus policies and procedures should provide for individual unique user ID/passwords (no shared IDs).

The vice president of business and administrative services stated that procedures had not been adequately followed or enforced at SHS.

Inadequate control over cash receipts increases campus exposure to loss from inappropriate acts.

### **Recommendation 2**

We recommend that the campus prohibit SHS cashiers from sharing cashiering sessions in order to localize accountability over receipts.

### **Campus Response**

We concur. The SHS director has reworked the procedures such that this practice is not permitted. Personnel have been retrained to comply with the new procedures. Target completion date is January 31, 2009.

### **NON-SUFFICIENT FUNDS**

Returned check holds were not placed on five of ten accounts reviewed that showed an outstanding unrecovered non-sufficient funds (NSF) check balance.

SAM §20050 states that the elements of a satisfactory system of internal accounting and administrative controls include a system of authorization and recordkeeping procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenditures.

The vice president of business and administrative services stated that the campus not consistently applying NSF check holds was an oversight.

Inadequate control over dishonored checks increases the campus exposure to the receipt of multiple NSF checks from a single maker.

### **Recommendation 3**

We recommend that the campus consistently apply existing NSF check holds to deter the acceptance of multiple checks from a single source.

### **Campus Response**

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will retrain staff to ensure that the procedures are followed with respect to NSF holds. Target completion date is January 31, 2009.

### **STUDENT FEES**

New fees and changes to existing fees were not always approved.

Our review of five new and three increased fees as of summer 2007 disclosed that in three instances, there was no evidence of the chancellor or the president's approval for one new and two increased fees, respectively.

Executive Order (EO) 740, *Student Fee Policy*, dated April 13, 2000, states, in part, that the chancellor is delegated authority to establish new campus fees and the president is delegated authority to increase, decrease, or abolish campus fee.

The vice president of business and administrative services stated that due to turnover in key positions, the appropriate fee approval was not properly documented before implementation.

Inadequate control over new fees and changes to existing fees increases the possibility that unapproved fees are potentially imposed upon the student body.

#### **Recommendation 4**

We recommend that the campus strengthen procedures to ensure that the requisite approval is obtained and documented prior to establishing new or increased fees.

#### **Campus Response**

We concur. The campus will develop a procedure to ensure that approvals for new and modified fees are obtained and documented before implementation. Target completion date is January 31, 2009.

### **APPLICATION FEE RECONCILIATION**

The campus could not provide evidence that application fee reconciliations had been prepared since the prior FISMA audit.

State University Administrative Manual (SUAM) §3825.01 states that a reconciliation of applications for admission to fees received shall be prepared for each academic year term and maintained on file by each campus. The reconciliations should be completed one month after the end of the academic term being reconciled.

The vice president of business and administrative services stated that the failure to reconcile application fees was an oversight.

Failure to reconcile fees in a timely and complete manner increases the risk that errors and irregularities will not be detected and compromises accountability.

#### **Recommendation 5**

We recommend that the campus strengthen controls to ensure that application fee reconciliations are prepared in a timely and complete manner for each academic term.

#### **Campus Response**

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will retrain staff to ensure that the procedures are followed regarding application fee reconciliations. Target completion date is January 31, 2009.

## ACCOUNTS RECEIVABLE

### WRITE-OFF OF UNCOLLECTIBLE DEBT

Write-offs of uncollectible debt were not approved.

Our review of the listing of accounts written-off from May 2006 to August 2007 disclosed that the campus did not seek discharge from accountability from the State Controller's Office (SCO) for all four accounts with balances over \$1,000. Documentation to support the write-offs of all 11 accounts with balances each under \$1,000 was also not in file.

EO 616, *Discharge of Accountability*, dated April 19, 1994, states that campuses will be obligated to comply with the collection efforts as outlined in SAM §8776.6, which includes collection procedures that assure prompt follow-up on receivables. Authority is also delegated to the campus for local adjustments of up to \$1,000 that are determined to be uncollectible or where the amount does not justify the collection costs.

SAM §8776.6 provides procedures and guidelines regarding adequate collection efforts and follow-up on receivables, including specific requirements for filing applications for discharge from accountability with the SCO. If all reasonable collection procedures do not result in payment, departments may request discharge from accountability of uncollectible amounts due from private entities. Departments will file an application for Discharge of Accountability Form, STD. 27, with the SCO, Division of Collections.

The vice president of business and administrative services stated that although there had been discussions in this regard, personnel failed to provide documentation for the review and approval for write-offs.

Failure to obtain the documented approval prior to charging-off accounts receivables increases the risk of premature and unapproved write-offs.

### Recommendation 6

We recommend that the campus seek approval from the Office of the Chancellor or the SCO with requests to write-off uncollectible accounts greater than \$1,000 that are related to CSU fund categories or operations within the CSU trust funds or state appropriated funds, respectively.

### Campus Response

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will retrain staff to ensure that the procedures are followed regarding the write-off of uncollectible accounts. Target completion date is January 31, 2009.

## EMPLOYEE ACCOUNTS RECEIVABLE

Employee accounts receivable controls were inadequate.

Our review of 20 outstanding travel advances for 14 employees as of February 2008, disclosed that:

- ▶ Policies and procedures that impact the system of internal accounting and administrative control for employee accounts receivable (including travel advances) had not been fully documented. For example, policies and procedures had not been fully documented for monitoring of delinquent employee accounts receivable, the time frame in which accounts payable should process travel expense claims, and the employee advance account reconciliations to the general ledger.
- ▶ The employee travel advance account was not up-to-date. Fourteen advances for 14 employees, dated between April 1, 2006, and February 18, 2008, had not been substantiated by a travel expense claim, which overstated the account by \$24,024. We also noted that travel expense claims were previously submitted for six of the 14 advances; however, accounts payable had not processed the claims by chargeback to the respective departments as of the audit date.
- ▶ The collection process was not timely or adequate overall for two separated employees with a combined outstanding travel advances of \$2,924. The sequence of three collection letters had not been sent in 30-day intervals nor was personnel action request forms submitted to the SCO in order to flag the employees in the event of returning to state service at another agency. Additionally, the lack of collection activity prevented the submission of the accounts for recovery by tax offset.

SAM §7901 states that the accuracy of an agency's accounting records may be proved partially by making certain reconciliations and verifications.

SAM §7920 states that each agency is responsible to complete any reconciliation necessary to safeguard state assets and ensure reliable financial data.

SAM §8116.2 requires the submittal of a properly prepared travel expense claim to substantiate travel expenses as soon as possible after the trip or at least once a month.

SAM §8776 states that an accounts receivable is defined as a claim against a person, firm, corporation, or other entity for money owed to the state.

SAM §8776.2 states that a valid accounts receivable is a receivable which is due and payable and for which there is no apparent disagreement over the validity of the claim or the amount at the time it was established.

SAM §8776.7 provides collection procedures to be employed in the collection of amounts due from employees.

SUAM §3822 states that, each campus will establish procedures that provide for prompt follow-up of accounts receivable, including preparation and issuance of follow-up letters and/or calls.

The vice president of business and administrative services stated that this finding was due in large part to timing and that the campus allowed athletic coaches to use university credit cards to fund their travel instead of providing cash advances. He also stated that monthly credit card statements were required to clear these receivables that caused a delay in processing. Lastly, he stated that separated employees' balances were not adequately controlled due to employee turnover and that the incumbent had been unable to pursue collections due to a lack of contact information.

Inadequate control over delinquent employee receivables reduces the likelihood of collection, increases the amount of resources expended on collection efforts, and negatively impacts cash flow.

### **Recommendation 7**

We recommend that the campus:

- a. Develop and implement procedures for monitoring of delinquent employee accounts receivable, the time frame in which accounts payable should process travel expense claims, and the employee advance reconciliation account to the general ledger.
- b. Strengthen procedures to ensure that employee travel advances are timely cleared and offset against processed travel expense claims.
- c. Strengthen procedures to ensure that collection efforts are documented and timely performed for delinquent employee accounts receivables.

### **Campus Response**

We concur. The campus will update its policies and procedures to improve monitoring of delinquent accounts receivable. The campus will modify procedures to address delinquent travel expense claims and other employee receivables. Target completion date is January 31, 2009.

## **PAYROLL AND PERSONNEL**

### **EMPLOYEE ELIGIBILITY VERIFICATION**

Federal Form I-9, Employment Eligibility Verification, was not always completed timely.

Our review of 15 new hire transactions disclosed that in three instances, the Form I-9 was not completed within the required three days. The completion dates ranged from 12 to 47 days.

The Immigration Reform and Control Act of 1986 states that all employees, citizens, and non-citizens are required to complete Form I-9, Employment Eligibility Verification, at the time of hire, which is the actual beginning of employment. The act requires employers to examine evidence of identity and employment eligibility within three business days of the date employment begins.

The director of human resources stated that, in each instance, the exceptions resulted from a delay in the creation of the employee offer letter, which most likely stemmed from late information submitted to the provost's office from the hiring department.

Untimely completion of employment eligibility verification increases the risk of non-compliance with federal employment regulations.

### **Recommendation 8**

We recommend that the campus strengthen procedures to ensure timely completion of Form I-9.

### **Campus Response**

We concur. A notice will be sent before each quarter begins to all schools and departments reminding them that employees must sign their new hire forms, including the I-9, within three days of their start date as required by law. Target completion date is January 31, 2009.

## **LOCAL ESCHEAT ACCOUNT**

Escheat account controls were inadequate.

Our review of 18 undelivered salary warrants that were deposited to a local escheat account between June and October 2007 disclosed that in 14 instances, the warrants remained unclaimed as of the audit date and showed no documented evidence of employee follow-up or that due-diligence letters were sent to the rightful owners. In addition, policies and procedures had not been appropriately documented to address this practice or to properly report the unclaimed property to the SCO after the dormancy period.

SCO *General Reporting Instructions for Holders of Unclaimed Property*, dated January 2008, states that holders are required to review their records each year to determine if they hold any property that has remained unclaimed for the dormancy period. Additionally, holders are required to send notices to owners prior to reporting accounts to the SCO. The notice must clearly state that the property will escheat to the state if a timely response to the notification is not received.

SAM §8580.5 states that salary warrants not delivered within five days of pickup shall be returned to the office which distributes salary warrants. A written record of all undelivered warrants will be maintained and a copy given to the payroll office. Warrants not delivered within 90 calendar days of receipt must be deposited and remitted to an escheat revenue account in the original fund that

provided the resources to the State Payroll Revolving Fund. Agencies will maintain a subsidiary ledger of all amounts credited to and disbursed from the escheat revenue accounts.

The vice president of business and administrative services stated his belief that limited resources and campus turnover prevented the department from adequately documenting employee follow-up on undelivered salary warrants.

Failure to monitor the campus escheat account increases the risk of accumulated unclaimed property, stale dated checks, and misappropriated funds.

### **Recommendation 9**

We recommend that the campus establish and implement procedures for monitoring the campus escheat account and performing appropriate employee follow-up with undelivered salary warrants.

### **Campus Response**

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will retrain staff to ensure that the procedures are followed. Target completion date is January 31, 2009.

## **FIXED ASSETS**

Administration of fixed assets did not ensure that all property was inventoried, identified, and reconciled timely.

We found that:

- ▶ A complete physical count of all property had not been made and reconciled to the general ledger since the 2002-2004 inventory periods.
- ▶ Verification, tagging, and checkout of 20 laptop computers utilized by campus personnel disclosed that in one instance, a laptop that was assigned to the information technology (IT) services support department could not be located and in nine instances, the property department did not have inventory equipment and materials checkout forms on file. A lost/stolen report was completed to account for the missing laptop.
- ▶ Identification tags were not always attached to campus property. Two of the ten fixed assets reviewed were located at the AVC and lacked a CSUB identification tag. These assets ranged from \$6,572 to \$8,602 in value and were checked out to a professor without the use of an inventory equipment and materials checkout form.

The CSUB Asset Management Standard Operating Policy states that non-capital equipment will be monitored with a perpetual system with no one cycle taking longer than three years and that all capital and non-capital equipment is bar-coded with a unique identification number and recorded in property inventory records and remains so identified as long as it is in the custody, possession, or control of the university.

SAM §7924 requires that departments reconcile property at least quarterly or monthly, depending upon the volume of property transactions. Agencies will reconcile the acquisitions and dispositions of capitalized property with the amounts recorded into the property ledger.

SAM §8600 states that property accounting procedures are designed to maintain uniform accountability for state property. These standard procedures are used to provide accurate records for the acquisition, maintenance, control, and disposition of property. The combination of accurate accounting records and strong internal controls must be in place to protect against and detect the unauthorized use of state property.

SAM §8651 states that all state property will be tagged after acquisition. This includes property, which does not meet all of the state's capitalization requirements. The purpose of tagging assets is to designate the assets as belonging to the state. Tags will be placed so that they are in plain sight and easy to read.

SAM §8652 requires a physical count of all property and reconciliation of the count with accounting records at least once every three years.

The director of facilities operations stated that the property survey board policy change on inventory items in 2007 and the training of newly appointed property custodians on the policy changes delayed the completion of a complete physical inventory. The general accounting manager stated that the reconciliations were outstanding due to the verification of the cost of the additions and that one company had failed to invoice the university for several months delaying the finalization of the reconciliations. Further, the director of facilities operations added that the inconsistent use of inventory equipment and materials checkout forms could potentially be attributed to limited follow-up training of all designated property custodians and that the lack of CSUB identification tags at the AVC was attributed to a miscommunication between the different parties.

Insufficient control over fixed assets, untimely completion of reconciliations, and failure to utilize inventory equipment and materials checkout forms increases the risk of inappropriate activities, misstated property records, theft, unauthorized use of state property, and reduces accountability over state property.

### **Recommendation 10**

We recommend that the campus:

- a. Perform a physical count of all property and reconcile the count with accounting records at least once every three years.

- b. Attach an identification tag to all property.
- c. Strengthen the enforcement of laptop controls for off-campus use of university equipment.
- d. Enforce policies and procedures for fixed assets at off-site locations.

### **Campus Response**

We concur. The campus completed a capital asset inventory September 2007 and a non-capital inventory May 2008. The Asset Management Standard Operating Policy (modified February 2008) indicates how capital and non-capital assets are to be identified and tagged. It also includes how equipment such as laptops and other equipment that may be maintained off-campus are to be controlled.

## **INFORMATION TECHNOLOGY**

### **INFORMATION SECURITY OVERSIGHT**

The identification and reporting of information security projects was inadequate.

Specifically, we noted that:

- ▶ There was no comprehensive plan for identifying and prioritizing campus information security needs.
- ▶ For existing information security related projects, there were no projected due dates to help ensure that such projects were completed in a timely manner.

SAM §4841 requires state agencies to provide for the proper use and protection of its information assets by establishing appropriate policies and procedures for preserving the integrity and security of automated files and databases.

The information security officer stated that information security projects were reported on an informal basis to executive management.

Security practices that do not ensure campus-wide policy and compliance increase the risk of unauthorized exceptions and could compromise compliance with statutory information security requirements, while lack of a comprehensive system of information security management increases campus exposure to security breaches and the risk of inappropriate access to data.

### **Recommendation 11**

We recommend that the campus:

- a. Develop a comprehensive plan to identify and prioritize campus information security needs.
- b. Develop time frames for completing existing information security projects.

### **Campus Response**

The university concurs with this recommendation.

The information security working group has created the following list of projects that have been completed in 2008 and a second list for which completion is planned in the next six months. The information security officers will inform the president's cabinet of the projects and other security issues either by memo or by presentation four times per year.

1. Complete movement of all appropriate users to Active Directory (AD). Move PCs to AD should be done by January 2009. Move Macs to AD should be done by July 2009. Generate campus users for AD; was completed April 2008. Generate auxiliary or persons of interest for AD; target completion date is January 2009.
2. Install new firewalls and tighten firewall rules. Firewall improvement was completed by mid-August 2008.
3. Require authentication for wireless users. Wireless authentication should be deployed by December of 2008.
4. Hire a PeopleSoft security person. Completed, individual has been hired.
5. Establish a protocol for creation of any new database that contains confidential or protected information. Protocol was put in place August 2008.
6. Review CSUB information security policies and procedures and integrate with the CSU policies and procedures once they are approved. CSUB is waiting on the release of the CSU policy on information security.
7. Internally audit de-provisioning process twice a year to assure compliance with campus practice. This will be ongoing.
8. Review critical IT resources for vulnerabilities with an aim towards minimizing risk. This will be ongoing.
9. Continue providing campus-based security training while waiting on the CSU to offer a comprehensive training program.

The campus concurs that it needs to develop a plan for identifying and resolving campus security concerns. Over the next six months, the campus will develop an IT security risk assessment plan that will be informed by published information from IT security organizations such as Certified Information System Security Professionals, SANS, the CSU information security officers working group, etc. While budget constraints prevent the campus from conducting an ongoing, institution-wide security assessment of all IT business practices, IT staff members have conducted office IT security assessments on request. Target completion date is March 31, 2009.

## **SECURITY OF VENDOR SUPPORTED SYSTEMS**

The campus had not developed written security guidelines, including the necessary security requirements for systems supported and maintained by outsourced vendors or third parties. As a result, we noted that security over the runner card system was not adequate and security requirements over the donor system had not been defined.

SAM §4841 requires state agencies to provide for the proper use and protection of its information assets by establishing appropriate policies and procedures for preserving the integrity and security of automated files and databases.

The assistant vice president of IT services stated the campus did not have the expertise to administer security for the runner card system and that the donor system was still being implemented.

Failure to ensure that sensitive information is adequately protected could require the campus to notify all affected personnel in the event of a breach of security.

### **Recommendation 12**

We recommend that the campus develop written security guidelines for the protection of sensitive information pertaining to data processing activities conducted by vendors and third parties on behalf of the campus that includes security and recovery requirements of the information and system.

### **Campus Response**

The campus concurs with this recommendation. The campus has added the following requirements for all vendors bidding on projects within the scope of this recommendation:

CSUB requires all vendors handling confidential data to outline the steps and protocols they have in place to protect CSUB data. Please respond to each of the following questions. If the question is not applicable for the service being offered please indicate with N/A, and state why.

- Describe the encryption mechanism used for electronic transmission of data (e.g., SSL/SSH/etc.).
- What kind of secure login and authentication is used to protect access to our data?

- Describe the intrusion detection and/or prevention used for all devices and network nodes.
- Describe your server and network vulnerability testing protocols.
- What kind of firewall infrastructure, virus protection, and patch management systems are in place to protect our data?
- What measures do you take to harden servers and disable unnecessary services?
- How will our data be backed up, by whom, where, and how will the backups be stored (on-site/off-site, temperature and humidity controls, fire protection, etc.), will they be stored in an encrypted format?
- Describe the background check protocol of all employees who handle or have access to our data.

These guidelines are campus policy. The policy, non-disclosure agreement, and security addendum are posted online. The processes for identifying new projects or procurements that may need to comply with this policy are outlined in the policy document.

## **PEOPLESOFT ACCESS AND PASSWORDS**

Account access was not removed from some terminated employees in the PeopleSoft Finance system, and password history was not used in the PeopleSoft Human Capital Management (HCM) system.

SAM §4841 requires state agencies to provide for the proper use and protection of its information assets by establishing appropriate policies and procedures for preserving the integrity and security of automated files and databases.

The director of administrative computing services stated that they were uncertain why some old accounts had not been suspended, and that the password history setting was an oversight.

Active accounts for former employees could lead to unauthorized or inappropriate access, and password history prevents users from reusing the same password.

### **Recommendation 13**

We recommend that the campus remove any accounts that are not assigned to a current employee, investigate the cause of access not being removed, and use the password history function to ensure that new passwords are selected by users.

## **Campus Response**

The campus concurs with this recommendation.

### Access:

The campus has an established policy and procedure to terminate employee's access to the university's enterprise systems including PeopleSoft. Employees are required to complete a separation clearance form (SCF) that is signed off by the employee's department, IT units, library services, and cashiering office. Removal of PeopleSoft access is based on the signed SCF.

The account access for two terminated employees that were not removed at the time of the audit has since been removed. These were due to oversight in the termination process. One was for a technical consultant whose name was misspelled on an account creation, but the account had never been used and was not removed. The other was due to a termination that occurred during Christmas break and the termination procedure was overlooked. Administrative computing is making every effort to log and process the SCF to remove account access diligently.

### Passwords:

The password history has not been used in the PeopleSoft HCM system because the Common Management Systems (CMS) authentication was planned (and now in production) to authenticate via Lightweight Directory Access Protocol (LDAP) against our AD system which has a password history of four. At the time of the FISMA audit in January of this year, the campus was in the midst of HCM Campus Solutions implementation with rolling go-live milestones. There was dynamic decision making in the implementation of CMS authentication.

For PeopleSoft Finance, the password history function is configured for passwords to expire every 90 days and the previous three are kept in history.

As it stands today, the password history function for PeopleSoft HCM is not used because we are authenticating current user access through LDAP, which is enforcing a password history of four. However, there is a very small group of legacy users (less than 100 of mostly human resources and time and labor users) who still authenticate through PeopleSoft security. We are working towards a process to address this small group by either converting them to the LDAP authentication or enabling the PeopleSoft password history function.

Target completion date is December 31, 2008.

## TRUST FUNDS

Cash control, contractual services, and procedural weaknesses were found with the public performance jazz account.

We noted that:

- ▶ Accumulated cash receipts (approximately \$19,922) deposited from the weekend jazz festival on May 16, 2007, were not adequately secured. We noted that at the end of each day, cash receipt collections were placed into the music department chair's personal vehicle, taken to his home, sorted, counted, and stored in large garbage bags. On the first business day following the event, the garbage bags were transported from the department chair's home via personal vehicle to the main cashier's office for deposit.
- ▶ The music department chair appointed family members to assist in handling security, cash receipts, and bookkeeping for the event. The family members were not employed with the campus and volunteered to work the weekend event.
- ▶ Proper segregation of duties and compensating controls were not maintained for the jazz festival concession sales. The music department chair was designated the custodian of the change fund, controller of daily count sheets for the cashiers' tills, and was responsible for securing the cash receipts and making the deposit.
- ▶ Jazz festival ticket sales were not reconciled to revenue recorded in the general ledger.
- ▶ The inventory of concession tickets used during the jazz festival for food and beverage sales was not adequately controlled. Specifically, concession ticket sales were not reconciled to receipts and revenue recorded in the general ledger and was not adequately secured before, during, and subsequent to the three-day event.
- ▶ Daily interim cash pickups by the primary security officer were collected and stored in an unsecured trailer located in a high traffic area during the jazz festival.
- ▶ Weekend concert receipts were transferred from the department directors to the music department without the use of transfer receipts.
- ▶ Checks received at weekend concerts were not restrictively endorsed on the day received. The checks were not endorsed until after they were brought to the music department and prepared for deposit.
- ▶ Change funds issued to department directors for weekend concerts were not always adequately secured. We found that the cash tills issued did not have a locking mechanism to adequately secure receipts. Additionally, the funds were stored at a music department director's home or in his/her personal vehicle prior and subsequent to the events.

- ▶ The music department did not maintain a written record of employees with access to the locking file cabinet where cash receipts were maintained.
- ▶ The public performance jazz trust fund agreement did not clearly define the type of allowable expenditures.
- ▶ Jazz festival donations were included with other monies in the public performance jazz trust account that were used to fund other departmental events and activities.
- ▶ Policies and procedures did not exist for advertising trade-outs received.
- ▶ The agreement between the third-party ticket vendor and CSUB was not signed by the campus.

SAM §8023 states that all checks, money orders, and warrants received for deposit will be restrictively endorsed for deposit as soon as possible after receipt, but no later than the end of the working day.

SAM §8034.1 states that agencies will endorse checks, warrants, money orders, and other negotiable instruments on the day they are received. Timely endorsements serve to discourage the use of lost or stolen negotiable instruments by someone other than the state agency.

SAM §8070 states that state officers and employees who receive and disburse money will be held accountable for the money in their custody. They will be held personally responsible for any cash discrepancies. Each department is responsible for establishing standards of performance for their cashiers and prescribing corrective actions to be utilized when performance standards are not satisfied.

SAM §19420 requires that each trust account established be supported by documentation which includes the persons authorized to withdraw or expend funds.

SAM §20050 states that one symptom of a deficient internal control system is policy and procedural or operational manuals that are either not currently maintained or are non-existent.

The vice president of business and administrative services stated that the music department was provided instructions on cash management and that the instructions had not been adequately enforced.

Inadequate control over cash receipts and trust fund administration increases campus exposure to loss from inappropriate acts.

#### **Recommendation 14**

We recommend that the campus:

- a. Evaluate the current practice of handling cash receipts for the annual jazz festival and consider the use of other personnel such as campus accounting to administer the fiscal aspects of this event.
- b. Ensure that all the music department's receipts are adequately safeguarded in cash drawers or other secure mechanism until deposited.
- c. Ensure that all potential conflicts of interest are disclosed and adequately controlled.
- d. Establish procedures to review cashiering activities at the music department and take appropriate action to either segregate duties or establish effective mitigating controls.
- e. Establish procedures to reconcile receipts to revenue recorded to ensure adequate accountability over revenue.
- f. Establish procedures to reconcile concession sales subsequent to the event to ensure adequate accountability over revenue.
- g. Maintain a written record of individuals with access to the locking file cabinet used to store cash receipts at the music department.
- h. Revise the trust fund agreement to clearly define the allowable expenses.
- i. Develop and distribute appropriate policies and procedures for advertising trade-outs.
- j. Obtain a signed agreement between the third-party ticket vendor and CSUB.

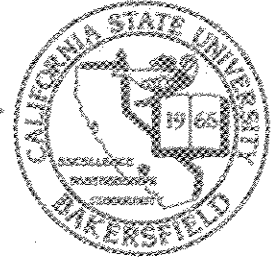
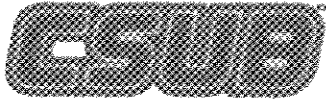
#### **Campus Response**

We concur. The campus will develop procedures to ensure campus accounting personnel administer the fiscal aspects of special events. These procedures will include how revenue and expense activity relative to special events will be controlled including records regarding access to cash receipts and storage. Additionally, the protocol will include procurement and contract procedures for third-party ticket vendors. As well, the music department activities will fall under this new protocol including revising trust agreements that will define allowable expenses. Target completion date is January 31, 2009.

---

## **APPENDIX A: PERSONNEL CONTACTED**

<b><u>Name</u></b>	<b><u>Title</u></b>
Horace Mitchell	President
Karen Abercrombie	Account Technician II
Cassie Alvarez	Administrative Support Assistant, Health Center
Marge Becas	Accountant, Student Financial Services
Cindy Breor	Fiscal Services Administrative Support Technician, Antelope Valley Campus (AVC)
Stephanie Burgess	Lead Cashier
Catherine Byrne	Manager, Student Financial Services
Michael Chavez	Director, Procurement
Doug Davis	Chair, Music Department
Perry Eggleston	Sergeant, University Police Department
Mike Fleming	Network Analyst
Lizeth Gamez	Accounting Supervisor
Felix Garcera	Director, Facilities Operations
Kellie Garcia	Director, Human Resources
Rod Hersberger	Information Security Officer
John Hultsman	Associate Vice President/Director, AVC
Kathy Ives	Accountant II
Fedel Kabagbag	Accountant
Irene Leung	Director, Administrative Computing Services
Janet Martin	Director, Payroll Services
Michelle Mills	University Budget Officer
Suzanne Muller	General Accounting Manager
Claudia Neal	Director, University Police Department
Michael Neal	Vice President, Business and Administrative Services
Lisa Rey	Accounts Receivable Technician
Isabel Rivera	Accounts Receivable Accountant
Clark Sanford	Assistant Vice President, Information Technology Services
Doug Smith	Property Clerk II, Facilities Management



Office of the Vice President of Business and Administrative Services  
California State University, Bakersfield

38 ADM  
9001 Stockdale Highway  
Bakersfield, California 93311-1022

(861) 854-2287  
FAX (861) 854-8323  
Email: mneal@csub.edu

RECEIVED  
UNIVERSITY AUDITOR

OCT 9 2008

THE CALIFORNIA STATE  
UNIVERSITY

October 3, 2008

Mr. Larry Mandel  
University Auditor  
California State University  
401 Golden Shore, 4<sup>th</sup> Floor  
Long Beach, CA 90802-4210

Re: Revised Campus Response to Recommendations of Audit Report Number 07-12 at California State University, Bakersfield

Dear Mr. Mandel:

Per your request, the attached documents are the revised Campus Responses to the audit recommendations. An electronic copy of these documents is also being provided to Anne Douglas.

Please have your staff review our responses and corrective action plan and return any comments or suggestions to myself and Douglas Wade. Our plan is to have corrective actions implemented and evidence provided to your office by the end of January 2009.

Sincerely,

Michael A. Neal  
Vice President  
Business and Administrative Services

cc's: without attachments

Horace Mitchell, President  
Douglas Wade, Assistant Vice President, Fiscal Services

*"ATTITUDE MAKES THE DIFFERENCE"*

**FISMA**

**CALIFORNIA STATE UNIVERSITY,  
BAKERSFIELD**

**Audit Report 07-12**

**CASH RECEIPTS**

**MAIN CASHIERING**

**Recommendation 1**

We recommend that the campus:

- a. Ensure that all checks are restrictively endorsed immediately upon receipt or at minimum, by the end of each day.
- b. Deposit checks in a timely manner and utilize a suspense account to maintain accountability for long-outstanding checks received but not applied as payments.
- c. Establish and implement procedures for counting cash tills at the beginning of the day or the start of a new cashiering session.
- d. Enforce campus deposit procedures for the dual verification of the daily deposits.
- e. Implement procedures for transfer receipts from the general accounting office to the main cashiering office for checks received in the mail.
- f. Establish procedures to prepare a pre-listing of cash and checks received not payable to the university.
- g. Require the safe access log with the written records of individuals with knowledge of the safe to be updated at prescribed frequencies.

**Campus Response**

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will re-train staff to ensure that the procedures are followed. Target completion date is 1/31/2009.

**SATELLITE CASHIERING**

**Recommendation 2**

We recommend that the campus prohibit SHS cashiers from sharing cashiering sessions in order to localize accountability over receipts.

**Campus Response**

We concur. The SHS director has re-worked the procedures such that this practice is not permitted. Personnel have been re-trained to comply with the new procedures. Target completion date is 1/31/2009.

**NON-SUFFICIENT FUNDS**

**Recommendation 3**

We recommend that the campus consistently apply existing NSF check holds to deter the acceptance of multiple checks from a single source.

**Campus Response**

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will re-train staff to ensure that the procedures are followed with respect to NSF holds. Target completion date is 1/31/2009.

**STUDENT FEES**

**Recommendation 4**

We recommend that the campus strengthen procedures to ensure that the requisite approval is obtained and documented prior to establishing new or increased fees.

**Campus Response**

We concur. The campus will develop a procedure to ensure that approvals for new and modified fees are obtained and documented before implementation. Target completion date is 1/31/2009.

**APPLICATION FEE RECONCILIATION**

**Recommendation 5**

We recommend that the campus strengthen controls to ensure that application fee reconciliations are prepared in a timely and complete manner for each academic term.

**Campus Response**

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will re-train staff to ensure that the procedures are followed regarding application fee reconciliations. Target completion date is 1/31/2009.

## ACCOUNTS RECEIVABLE

### WRITE-OFF OF UNCOLLECTIBLE DEBT

#### Recommendation 6

We recommend that the campus seek approval from the Office of the Chancellor or the SCO with requests to write-off uncollectible accounts greater than \$1,000 that are related to CSU fund categories or operations within the CSU trust funds or state appropriated funds, respectively.

#### Campus Response

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will re-train staff to ensure that the procedures are followed regarding the write-off of uncollectible accounts. Target completion date is 1/31/2009.

## EMPLOYEE ACCOUNTS RECEIVABLE

#### Recommendation 7

We recommend that the campus:

- a. Develop and implement procedures for monitoring of delinquent employee accounts receivable, the time frame in which accounts payable should process travel expense claims, and the employee advance reconciliation account to the general ledger.
- b. Strengthen procedures to ensure that employee travel advances are timely cleared and offset against processed travel expense claims.
- c. Strengthen procedures to ensure that collection efforts are documented and timely performed for delinquent employee accounts receivables.

#### Campus Response

We concur. The campus will update its policies and procedures to improve monitoring of delinquent accounts receivable. The campus will modify procedures to address delinquent travel expense claims and other employee receivables. Target completion date is 1/31/2009.

## PAYROLL AND PERSONNEL

### EMPLOYEE ELIGIBILITY VERIFICATION

#### Recommendation 8

We recommend that the campus strengthen procedures to ensure timely completion of Form I-9.

**Campus Response**

We concur. A notice will be sent before each quarter begins to all Schools and Departments reminding them that employees must sign their new hire forms, including the I-9, within three days of their start date as required by law. Target completion date is 1/31/2009.

**LOCAL ESCHEAT ACCOUNT**

**Recommendation 9**

We recommend that the campus establish and implement procedures for monitoring the campus escheat account and performing appropriate employee follow-up with undelivered salary warrants.

**Campus Response**

We concur. The campus has updated its procedures for cashiering and student financial services. The campus will re-train staff to ensure that the procedures are followed. Target completion date is 1/31/2009.

**FIXED ASSETS**

**Recommendation 10**

We recommend that the campus:

- a. Perform a physical count of all property and reconcile the count with accounting records at least once every three years.
- b. Attach an identification tag to all property.
- c. Strengthen the enforcement of laptop controls for off-campus use of university equipment.
- d. Enforce policies and procedures for fixed assets at off-site locations.

**Campus Response**

We concur. The campus completed a capital asset inventory September 2007 and a non-capital inventory May 2008. As well, the asset management standard operating policy (modified February 2008) indicates how capital and non-capital assets are to be identified and tagged. It also includes how equipment such as laptops and other equipment that may be maintained off-campus are to be controlled.

## INFORMATION TECHNOLOGY

### INFORMATION SECURITY OVERSIGHT

#### Recommendation 11

We recommend that the campus:

- a. Develop a comprehensive plan to identify and prioritize campus information security needs.
- b. Develop time frames for completing existing information security projects.

#### Campus Response

The University concurs with this recommendation.

The Information Security Working Group has created the following list of projects that have been completed in 2008 and a second list for which completion is planned in the next 6 months. The ISO will inform the President's Cabinet of the projects and other security issues either by memo or presentation four times per year.

1. Complete movement of all appropriate users to Active Directory.  
Move PCs to Active Directory should be done by January 2009.  
Move Macs to Active Directory should be done by July 2009.  
Generate campus users for Active Directory; was completed April 2008.  
  
Generate auxiliary or Persons of Interest for Active Directory; target completion date is January 2009.
2. Install new firewalls and tighten firewall rules.  
Firewall improvement was completed by mid-August 2008.
3. Require authentication for wireless users.  
Wireless authentication should be deployed by December of 2008
4. Hire a PeopleSoft security person. Completed, individual has been hired.
5. Establish a protocol for creation of any new database that contains confidential or protected information. Protocol was put in place August 2008.
6. Review CSUB information security policies and procedures and integrate with the CSU policies and procedures once they are approved. CSUB is waiting on the release of the CSU policy on Information Security.
7. Internally audit de-provisioning process twice a year to assure compliance with campus practice. This will be ongoing.
8. Review critical IT Resources for vulnerabilities with an aim towards minimizing risk. This will be ongoing.

9. Continue providing campus-based security training while waiting on the CSU to offer a comprehensive training program.

The campus concurs that it needs to develop a plan for identifying and resolving campus security concerns.

Over the next six months the campus will develop an IT security risk assessment plan that will be informed by published information from IT security organizations such as CISSP, SANS, the CSU ISO working group, etc.

While budget constraints prevent the campus from conducting an ongoing, institution-wide security assessment of all IT business practices, IT staff members have conducted office IT security assessments on request.

Target completion date is 3/31/09.

## **SECURITY OF VENDOR SUPPORTED SYSTEMS**

### **Recommendation 12**

We recommend that the campus develop written security guidelines for the protection of sensitive information pertaining to data processing activities conducted by vendors and third parties on behalf of the campus that includes security and recovery requirements of the information and system.

### **Campus Response**

The campus concurs with this recommendation.

The campus has added the following requirements for all vendors bidding on projects within the scope of this recommendation:

CSUB requires all vendors handling confidential data to outline the steps and protocols they have in place to protect CSUB data. Please respond to each of the following questions. If the question is not applicable for the service being offered please indicate with N/A, and state why.

- Describe the encryption mechanism used for electronic transmission of data (e.g., ssl/ssh/etc.).
- What kind of secure login and authentication is used to protect access to our data?
- Describe the intrusion detection and/or prevention used for all devices and network nodes.
- Describe your server and network vulnerability testing protocols
- What kind of firewall infrastructure, virus protection, and patch management systems are in place to protect our data?

- What measures do you take to harden servers and disable unnecessary services?
- How will our data be backed up, by whom, where and how will the backups be stored (onsite/offsite, temperature and humidity controls, fire protection, etc.), will they be stored in an encrypted format?
- Describe the background check protocol of all employees who handle or have access to our data.

These guidelines are campus policy. The policy, non-disclosure agreement, and security addendum is posted at: <http://www.csub.edu/BAS/fiscal/procurement/index.shtml>. The process for identifying new projects or procurements that may need to comply with this policy are outlined in the policy document.

## **PEOPLESOFT ACCESS AND PASSWORDS**

### **Recommendation 13**

We recommend that the campus remove any accounts that are not assigned to a current employee, investigate the cause of access not being removed, and use the password history function to ensure that new passwords are selected by users.

### **Campus Response**

The campus concurs with this recommendation.

#### Access:

The campus has an established policy and procedure to terminate employee's access to the University's enterprise systems including PeopleSoft. Employees are required to complete a Separation Clearance Form (SCF) that is signed off by the employees department, IT units, Library services and Cashiering Office. Removal of PeopleSoft Access is based on the signed SCF.

The account access for two terminated employees that were not removed at the time of the audit has since been removed. These were due to oversight in the termination process. One was for a technical consultant whose name was misspelled on an account creation, but the account had never been used and was not removed. The other was due to the termination occurred during Christmas break and the termination procedure was overlooked. Administrative Computing is making every effort to log and process the SCF to remove account access diligently.

#### Passwords:

The password history has not been used in the PeopleSoft HCM system because the CMS authentication was planned (and now in production) to authenticate via LDAP against our Active Directory system which has a password history of 4. At the time of the FISMA audit in January of this year, the campus was in the midst of HCM Campus Solutions

implementation with rolling go-live milestones. There was dynamic decision making in the implementation of CMS authentication.

For PeopleSoft Finance, the password history function is configured for passwords to expire every 90 days and the previous 3 are kept in history.

As it stands today, the password history function for PeopleSoft HCM is not used because we are authenticating current user access through LDAP which is enforcing a password history of 4. However, there are a very small group of legacy users (less than 100 of mostly HR and T&L users) who still authenticate through PeopleSoft Security. We are working towards a process to address this small group by either converting them to the LDAP authentication or enabling the PeopleSoft password history function.

Target completion date is 12/31/08.

## TRUST FUNDS

### Recommendation 14

We recommend that the campus:

- a. Evaluate the current practice of handling cash receipts for the annual jazz festival and consider the use of other personnel such as campus accounting to administer the fiscal aspects of this event.
- b. Ensure that all the music department's receipts are adequately safeguarded in cash drawers or other secure mechanism until deposited.
- c. Ensure that all potential conflicts of interest are disclosed and adequately controlled.
- d. Establish procedures to review cashiering activities at the music department and take appropriate action to either segregate duties or establish effective mitigating controls.
- e. Establish procedures to reconcile receipts to revenue recorded to ensure adequate accountability over revenue.
- f. Establish procedures to reconcile concession sales subsequent to the event to ensure adequate accountability over revenue.
- g. Maintain a written record of individuals with access to the locking file cabinet used to store cash receipts at the music department.
- h. Revise the trust fund agreement to clearly define the allowable expenses.
- i. Develop and distribute appropriate policies and procedures for advertising trade-outs.
- j. Obtain a signed agreement between the third-party ticket vendor and CSUB.

**Campus Response**

We concur. The campus will develop procedures to ensure campus accounting personnel administer the fiscal aspects of special events. These procedures will include how revenue and expense activity relative to special events will be controlled including records regarding access to cash receipts and storage. Additionally the protocol will include procurement and contract procedures for third party ticket vendors.

As well, the music department activities will fall under this new protocol including revising trust agreements that will define allowable expenses. Target completion date is 1/31/09.


  
**THE CALIFORNIA STATE UNIVERSITY**  
 OFFICE OF THE CHANCELLOR

BAKERSFIELD

October 20, 2008

CHANNEL ISLANDS

CHICO

**MEMORANDUM**

DOMINGUEZ HILLS

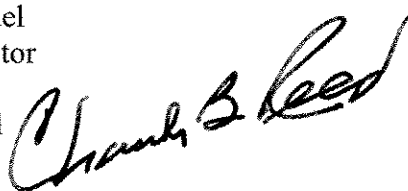
EAST BAY

FRESNO

TO: Mr. Larry Mandel  
University Auditor

FULLERTON

FROM: Charles B. Reed  
Chancellor



HUMBOLDT

LONG BEACH

SUBJECT: Draft Final Report 07-12 on *FISMA*,  
California State University, Bakersfield

LOS ANGELES

MARITIME ACADEMY

In response to your memorandum of October 20, 2008, I accept the response as submitted with the draft final report on *FISMA*, California State University, Bakersfield.

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/jt

SACRAMENTO

Enclosure

SAN BERNARDINO

cc: Dr. Horace Mitchell, President  
Mr. Michael A. Neal, Vice President, Business and Administrative Services

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS