

FISMA

**CALIFORNIA STATE UNIVERSITY,
LONG BEACH**

**Audit Report 07-09
May 1, 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
Internal Auditors: Dominick Owens and Julia Mathis

**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.....	7
Accounts Receivable.....	10
Payroll Receivable.....	10
Third-Party Receivable.....	11
Purchasing.....	12
Operating Fund	13
Payroll and Personnel	14
Employee Eligibility Verification	14
Employee Separation.....	15
Fixed Assets	16
Information Technology	17
Password Controls.....	17
Data Center Power Generator.....	18
Encryption of Sensitive Data.....	18
Network Security.....	19
Disaster Recovery Plan.....	20

APPENDICES

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

ABBREVIATIONS

AWOL	Absent Without Leave
CSU	California State University
CSULB	California State University, Long Beach
FISMA	Financial Integrity and State Manager's Accountability Act
GC	Government Code
PAN	Primary Account Number
PCI DSS	Payment Card Industry Data Security Standard
PTES	Parking, Transportation and Event Services
RDS	Reporting Data Store
SAM	State Administrative Manual
SUAM	State University Administrative Manual
UCES	University College and Extension Services

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.

The California State University, Long Beach (CSULB) 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 CSULB campus from November 19, 2007, through January 14, 2008, and made a study and evaluation of the accounting and administrative control in effect as of January 14, 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, purchasing, operating fund, payroll and personnel, fixed assets, information technology. 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, CSULB's accounting and administrative control in effect as of January 14, 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 [7]

Cash control weaknesses were found at each of the three satellite cashiering areas visited. The satellite cashiering locations reviewed included housing and residential services, University College and Extension Services (UCES), and parking, transportation and event services (PTES). At housing and residential services, an unauthorized petty cash fund was maintained from revenue generated from laundry services. At UCES, credit card and cash receipts collected were not always deposited within ten working days of receipt and personal information (i.e., credit card number and social security number) captured on the registration forms for enrollees paying by credit card was not redacted subsequent to authorization. At PTES, patron bags issued to parking officers for event collections were not documented to establish an adequate transfer of custody. Lastly, although cashiering duties were performed at the parking annex, the campus did not recognize the parking annex as an authorized satellite cashiering location, payments received via mail and customer walk-in at the parking annex were transferred to the parking administration building between employees without the use of transfer receipts, and the parking annex did not maintain a written record of the names of the persons with access to the locking file cabinet.

ACCOUNTS RECEIVABLE [10]

Delinquent payroll accounts receivable were not adequately pursued to ensure timely collection. Twelve payroll accounts receivables noted on the October 2007 aging report disclosed nine instances in which the three collection letters in 30-day intervals were not sent. This is a repeat finding from the prior FISMA audit. Pursuit of delinquent third-party accounts receivables was not always adequate. A review of ten third-party accounts receivables as of October 2007 disclosed that a sequence of three collection letters in 30-day intervals was not sent timely for nine closed third-party/auxiliary receivables. In addition, there was no documented evidence of collection correspondences on file to support collection efforts.

PURCHASING [12]

Campus procurement card policies and procedures were not always adequately enforced. A review of 23 procurement card statements for 12 cardholders dated between October and November 2006 disclosed that one procurement cardholder had five lost receipts totaling \$1,067 and the same cardholder violated policy by using the card for shuttle service for a guest speaker totaling \$87 plus two gratuity payments

totaling \$30. Also, documentation was not on file to indicate that the cardholder's multiple violations of the procurement card policy had been handled according to policy. The spreadsheet used to track multiple occurrences had not been maintained since May 2006.

OPERATING FUND [13]

Salary advances were not always adequately documented. In seven of ten salary advances reviewed, the salary advance forms did not indicate circumstances warranting the salary advances. This is a repeat finding from the prior FISMA audit.

PAYROLL AND PERSONNEL [14]

Federal Form I-9, Employment Eligibility Verification, was not always timely completed. A review of 15 new hire transactions disclosed that in one instance, the Form I-9 was signed by the employee five months after the effective employment date and approved eight months after the employment date by the authorized representative and in another instance, the employee and authorized representative did not sign the Form I-9 until 18 days after the employee's effective date noted on the Form I-9. Employee separation procedures did not always ensure complete clearance forms were always completed. A review of 11 separations from January 1, 2006, to September 30, 2007, disclosed that three of the 11 employees reviewed did not have a separation clearance certificate on file, and four absent without leave employees did not have separation clearance certificates on file and the campus did not provide evidence that any follow-up was done to retrieve state property from the employees.

FIXED ASSETS [16]

Campus equipment custody forms were not always completed and approved for off-campus use of university laptops. A review of ten laptop computers used by campus personnel disclosed that six were used off-campus. The property department did not have equipment custody forms on file for all six laptops that were used off-campus, three of the six faculty and staff that were permitted to remove/borrow equipment from the campus had not completed an equipment custody form, and in one instance, the equipment custody form on file did not indicate a checkout and return date for the equipment.

INFORMATION TECHNOLOGY [17]

Password controls for the human resources system were not set to effectively restrict access, the computer room did not have an emergency power generator capable of sustaining computer operations in the event of a power outage, and the campus did not encrypt some sensitive personal information stored on the reporting data store. Also, network security technologies were not configured to limit unwanted network traffic from certain critical servers and the campus did not have a current disaster recovery plan.

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.

We have not performed any auditing procedures beyond January 14, 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

Cash control weaknesses were found at each of the three satellite cashiering areas visited.

The satellite cashiering locations reviewed included housing and residential services, University College and Extension Services (UCES), and parking, transportation and event services (PTES).

Housing and Residential Services

An unauthorized petty cash fund was maintained from revenue generated from laundry services. We found that a third-party laundry service provider issued the housing department a monthly manager's allowance of \$30 and rather than depositing the allowance as revenue, it was used as a second petty cash fund.

State Administrative Manual (SAM) §8111.2 states, in part, that the total amount advanced rather than cash on hand will be shown in the monthly reconciliation of revolving fund resources. The custodian will be personally responsible for the amount advanced from the revolving fund. Transfers of custody will be accomplished only after: (a) a personal audit of the fund has been made by the employees directly concerned; and (b) a receipt has been given by the newly assigned custodian to the custodian being relieved. A copy of such receipt signed by both parties will be delivered to the accounting officer. An employee other than the custodian of the change or petty cash fund will count it.

The director of housing and residential life stated that the manager's allowance existed when he took over operations and he assumed it was an acceptable practice.

University College and Extension Services

- ▶ Credit card and cash receipts (checks) collected were not always deposited within ten working days of receipt. We visited UCES on November 29, 2007, and found eight unprocessed manually documented registration forms for credit card receipts totaling \$3,120, which were received on October 10, 2007. Additionally, we found two checks dated August 9, 2007, and August 20, 2007, totaling \$780, which were neither deposited nor restrictively endorsed as of the audit. The credit card and cash receipts were pending sign-off of the course proposals by the academic department. All held transactions were processed during the audit.
- ▶ One check dated October 14, 2007, for \$2,700 was held for a student that was currently enrolled. The student requested that the campus hold the check until she successfully completed the course and received tuition reimbursement from her employer. Additionally, the check had not been restrictively endorsed as of the audit. During the audit, UCES contacted the student and deposited the check.

- ▶ Personal information (i.e., credit card number and social security number) captured on the registration forms for enrollees paying by credit card was not redacted subsequent to authorization.

SAM §8032.1 requires agencies to deposit receipts in a timely and economical manner. Accumulated receipts of any amount will not remain undeposited for more than ten working days.

SAM §8034.1 and §8023 require checks and other negotiable instruments to be endorsed on the day they are received.

Payment Card Industry Data Security Standard (PCI DSS) Version 1.1, §3.2 and §3.3, dated September 2006, instructs merchants to not store sensitive authentication data subsequent to authorization and to mask primary account number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed).

The chief financial officer of UCES stated that the standard practice is to immediately endorse checks, process enrollments/payments immediately upon receipt, and make deposits the following business day. He further stated that there has been very rare situations where items were not processed due to pending actions. He added that because of security measures in place, UCES believed that personal information was duly protected.

Parking, Transportation and Event Services

- ▶ Patron bags issued to parking officers for event collections were not documented to establish an adequate transfer of custody.
- ▶ Although cashiering duties were performed at the parking annex, we noted that the campus did not recognize the parking annex as an authorized satellite cashiering location.
- ▶ Payments received via mail and customer walk-in at the parking annex were transferred to the parking administration building between employees without the use of transfer receipts. This is a repeat finding from the prior Financial Integrity and State Manager's Accountability Act (FISMA) audit.
- ▶ Receipts were not available to walk-in customers paying by cash or check at the parking annex.
- ▶ The parking annex did not maintain a written record of the names of the persons with access to the locking file cabinet.

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.

SAM §8021 requires 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.

SAM §8020 requires that state agencies prepare receipts for all collections from payers who request receipts.

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.

The associate director of PTES stated that the transfer of custody documentation was previously discontinued upon the inception of strict vault controls. The interim chief of police stated that the expansion of the citation processing function to the parking annex location and delays in both the formal training schedule and the communication of key function requirements limited the installation of appropriate business controls to support the collection process.

Inadequate control over cash receipts and confidential personal data increases campus exposure to loss from inappropriate acts and information security breaches.

Recommendation 1

We recommend that the campus:

- a. Identify all petty cash funds used throughout the campus and ensure that they are properly established and that completed count sheets are retained as evidence that independent counts are performed at prescribed frequency intervals.
- b. Process credit card receipts in a timely manner.
- c. Deposit checks in a timely manner and utilize a suspense account to maintain accountability for checks received but not applied as payments.
- d. Ensure that all checks are restrictively endorsed immediately upon receipt, or at minimum, by the end of each day.
- e. Establish mitigating controls to ensure that UCES appropriately safeguard PAN(s) and any other sensitive personal data at all times.
- f. Implement accountability procedures for the use of distributing patron bags for events.
- g. Approve parking annex as a satellite location or redirect cashiering duties to the appropriate department. If approved as a satellite location, implement procedures for transfer receipts, ensure that press-numbered receipts are available, and maintain a written record of individuals with access to the locking file cabinet used to store cash receipts at the parking annex.

Campus Response

We concur.

- a. We will identify any petty cash funds not currently established with campus approval and bring them into compliance with current campus policy or eliminate the fund if not approved. Estimated date of completion is October 2008.
- b. All credit cards will be processed in a timely manner and current campus cash handling procedures will be updated to include the handling of credit card transactions. Estimated date of completion is October 2008.
- c. All checks will be deposited in a timely manner as outlined in our current campus cash handling procedures. Estimated date of completion is May 2008.
- d. All checks will be restrictively endorsed upon receipt as outlined in our current campus cash handling procedures. Estimated date of completion is May 2008.
- e. Cash handling procedures will be updated to include the handling of credit card transactions including security requirements of PCI DSS. Estimated date of completion is July 2008.
- f. Cash handling procedures will be updated to include procedures for the distribution and control of patron bags for events. Estimated date of completion is July 2008.
- g. We will eliminate cash handling at the parking annex. Estimated date of completion is May 2008.

ACCOUNTS RECEIVABLE

PAYROLL RECEIVABLE

Delinquent payroll accounts receivable were not adequately pursued to ensure timely collection.

Our review of 12 payroll accounts receivables noted on the October 2007 aging report disclosed nine instances in which the three collection letters in 30-day intervals were not sent. This is a repeat finding from the prior FISMA audit.

State University Administrative Manual (SUAM) §3822 requires each campus to establish procedures that provide for prompt follow-up of accounts receivable, including preparation and issuance of follow-up letters and/or calls, and utilization of the offset claim procedures for accounts greater than \$10.

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

The associate vice president of human resources management stated that the campus procedures were not followed for these incidents and supporting documentation was not generated due to staff turnover.

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

Recommendation 2

We recommend that the campus strengthen procedures to ensure that payroll accounts receivable are promptly pursued for collection.

Campus Response

We concur. We have developed a PeopleSoft solution that creates custom payroll accounts receivable letters that generate automatically on a monthly basis for the second and third collection notices. This new automated process will ensure the second and third notices go out on a timely basis and reduce workload for the payroll technicians. We have reinforced the accounts receivable process with all payroll technicians within the payroll office. Estimated date of completion is June 2008.

THIRD-PARTY RECEIVABLE

Pursuit of delinquent third-party accounts receivables was not always adequate.

Our review of ten third-party accounts receivables as of October 2007 disclosed that a sequence of three collection letters in 30-day intervals was not sent timely for nine closed third-party/auxiliary receivables. Additionally, there was no documented evidence of collection correspondences (i.e. e-mails, phone call log) on file to support supplemental collection efforts.

SAM §8776.6 and §8776.7 provide collection procedures to be employed in the collection of amounts due from employees, including a sequence of three collection letters issued at 30-day intervals.

SAM §8776.6 requires that each department develop collection procedures that will assure prompt follow-up on receivables and states that a sequence of three collection letters is to be sent. Further, if all reasonable collection procedures are unsuccessful, an analysis should be prepared to determine what additional collection efforts should be made.

SUAM §3822 requires each campus to establish procedures that provide for prompt follow-up of accounts receivable, including preparation and issuance of follow-up letters and/or calls, and utilization of the offset claim procedures for accounts greater than \$10.

The manager of general accounting stated that collection letters were not sent timely due to personnel turnover in the department.

Inadequate control over delinquent third-party accounts receivable reduces the likelihood of collection, increases the amount of resources expended on collection efforts, and negatively impacts cash flow.

Recommendation 3

We recommend that the campus strengthen procedures to ensure that third-party receivables are promptly pursued for collection.

Campus Response

We concur. The campus has filled staff vacancies and provided training to each new hire regarding the campus established procedures for collections. Estimated date of completion is June 2008.

PURCHASING

Campus procurement card policies and procedures were not always adequately enforced.

Our review of 23 procurement card statements for 12 cardholders dated between October and November 2006 disclosed that:

- ▶ One procurement cardholder had five lost receipts totaling \$1,067. The same cardholder violated policy by using the card for shuttle service for a guest speaker totaling \$87 plus two gratuity payments totaling \$30. Documentation was not on file to indicate that the cardholder's multiple violations of the procurement card policy had been handled according to policy.
- ▶ The procurement and support services department was responsible for tracking cardholders' violations of the procurement policies via an Excel spreadsheet that had not been maintained since May 2006.

The California State University, Long Beach (CSULB) *Procurement Card Manual* states that the cardholder is responsible for obtaining original, itemized receipts or confirmations (for Internet purchases) to be attached to the monthly procurement card purchase report, prohibited purchases are defined as purchases that are not authorized by university policy, and the use of the procurement card is strictly prohibited for travel (with the exception of registration fees) includes meals, gasoline, airlines, lodging, and car rental. The manual also states that all procurement cardholders will be

tracked monthly for violations of procurement card policy. Tracking will be accomplished by means of a spreadsheet maintained by the procurement card coordinator. For a first violation, the procurement card coordinator will send a warning and request for an explanation. For a second violation, the action will be elevated to the director of procurement and support services. For a third violation, the action will be elevated to the associate vice president of financial management. Any violation deemed serious enough will be elevated to the director or associate vice president for action including possible card cancellation.

The director of procurement and support services stated that tracking cardholders misuse had not been maintained due to an oversight in documentation.

Insufficient control over procurement cards increases the risk of loss from inappropriate acts.

Recommendation 4

We recommend that the campus ensure that documentation is on file to indicate cardholder violations are handled and tracked in accordance with campus procurement card policy.

Campus Response

We concur. The campus will ensure the spreadsheet tracking system is up-to-date and approved monthly by the director of procurement. Violations of the campus policy will be documented in writing as outlined in our current policy. Estimated date of completion is July 2008.

OPERATING FUND

Salary advances were not always adequately documented.

Our review of ten salary advances issued between January 2006 and September 2007 disclosed that in seven instances, the salary advance forms did not indicate the circumstances warranting the salary advances. This is a repeat finding from the prior FISMA audit.

SAM §8595 states that agencies will prepare written criteria for salary advances including the procedures that must be followed before advances are given. The specific reason for the advance must be written on the request.

The associate vice president of human resources management stated that the campus was operating under the assumption that the term “salary advance” was sufficient explanation on the request for university check form.

Insufficient documentation of circumstances warranting the salary advance increases the risk that revolving fund monies may be expended for inappropriate purposes.

Recommendation 5

We recommend that the campus accurately document the reason for the advance in the section provided on the university check form.

Campus Response

We concur. Procedures have been reviewed with the payroll technicians who complete these forms. In addition, two management personnel employees will approve all requests. This new step will ensure that specific reasons for the request are documented and reviewed. Estimated date of completion is July 2008.

PAYROLL AND PERSONNEL

EMPLOYEE ELIGIBILITY VERIFICATION

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

Our review of 15 new hire transactions disclosed that:

- ▶ In one instance, the Form I-9 was signed by the employee five months after the effective employment date and approved eight months after the employment date by the authorized representative.
- ▶ In one instance, the employee and authorized representative did not sign the Form I-9 until 18 days after the employee's effective date noted on the Form I-9.

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 payroll services and human resource services stated that in the first instance, the employee was an adjunct faculty member responsible for developing a course and was not on campus to officially sign the form and in the second instance, the employee did not report to the payroll office timely.

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

Recommendation 6

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

Campus Response

We concur. We are reinforcing employment eligibility verification policy with all stakeholders. Non-payroll employees will no longer process I-9 paperwork. Employees who work off-campus and who cannot come to payroll to sign-in must have a notary or other California State University (CSU) campus to assist in the completion of the I-9 process. Estimated date of completion is July 2008.

EMPLOYEE SEPARATION

Employee separation procedures did not always ensure that clearance forms were completed.

Our review of 11 separations from January 1, 2006, to September 30, 2007, disclosed that:

- ▶ Three of the 11 employees reviewed did not have a separation clearance certificate on file.
- ▶ Four absent without leave (AWOL) employees did not have separation clearance certificates on file and the campus did not provide evidence that any follow-up was done to retrieve state property from the employees. Additionally, campus procedures did not address clearance waiver criteria or special exceptions for AWOL employees.

SAM §4842.2 states, in part, that personnel practices related to security management must include termination procedures that ensure that agency information assets are not accessible to former employees.

SAM §8580.4 describes the need for adequate separation procedures, including preparation of a clearance form that includes clearance of operating fund advances (travel and salary), return of keys, equipment, credit cards, etc.

The CSULB *Employee Clearance Procedures* states, in part, that employee clearance is done to ensure all university property and resources are recovered prior to an employees' last day physically worked. Departments may be responsible for costs associated with failure to secure university property and resources upon the termination of an employee. The department is responsible for assuring all university property, including sensitive equipment that has been issued to the employee, is returned.

The associate vice president of human resources management stated that the payroll office did not capture the omission of the form because the checks and balances process the payroll office has in place was not conducted in these instances.

Insufficient administration of employee separations increases the risk of loss of state funds and inappropriate use of state resources.

Recommendation 7

We recommend that the campus review and strengthen employee separation procedures to ensure complete clearance documentation.

Campus Response

We concur. We are reinforcing clearance process procedures with all stakeholders. Each month a letter will be sent to departments/colleges listing all separated employees lacking clearance forms. This letter requests departments provide missing clearance forms, if available, or certify/acknowledge that the forms were not completed and the circumstances. This new “check and balance” process ensures all departments/colleges are aware of missing clearance forms and the need to take responsibility for lost or missing assets. Estimated date of completion is July 2008.

FIXED ASSETS

CSULB equipment custody forms were not always completed and approved for off-campus use of university laptops.

Our review of ten laptop computers used by campus personnel disclosed that six were used off-campus. We found that:

- ▶ The property department did not have equipment custody forms on file for all six laptops that were used off-campus.
- ▶ Three of the six faculty and staff that were permitted to remove/borrow equipment from the campus had not completed an equipment custody form.
- ▶ In one instance, the equipment custody form on file did not indicate a check out and return date for the equipment.

The CSULB *Property Management/Security and Protection of Property Guideline* states precautions that should be taken to protect against the loss of equipment include but are not limited to: designation of an employee responsible for equipment, maintaining a system of equipment “sign-out” and “sign-in,” and completion of appropriately approved custody forms whenever equipment is taken off-campus.

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.

The receiving/property manager stated his belief that the custody form program was decentralized and that the forms were being issued by the appropriate departments.

Failure to utilize equipment custody forms increases the risk of unauthorized use and loss of state property.

Recommendation 8

We recommend that the campus implement the use of equipment custody forms for off-campus use of university equipment.

Campus Response

We concur. We are in the process of updating the property policy to reflect the current business practices for property management. The campus procedures will reflect the need to complete an equipment custody form or a departmental log for off-campus use of university equipment. Estimated date of completion is October 2008.

INFORMATION TECHNOLOGY

PASSWORD CONTROLS

Password controls for the human resources system were not set to effectively restrict access.

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 university controller stated that the system was recently upgraded and that not all password controls had been reset.

The absence of comprehensive password controls increases the risk that passwords may be compromised and could lead to unauthorized or inappropriate access.

Recommendation 9

We recommend that the campus activate the password controls in the human resources system to effectively restrict access in accordance with campus password security guidelines.

Campus Response

We concur. The campus has been working on the Human Capital Management password control project and plans to activate password controls in accordance with campus password security guidelines. Estimated date of completion is June 2008.

DATA CENTER POWER GENERATOR

The computer room did not have a generator capable of sustaining computer operations in the event of a power outage.

SAM §4842.2 requires each state agency to establish and maintain physical security measures that provide for management control of physical access to information assets. Physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility.

The director of administrative computing services stated that there was a generator, but that it only provided emergency lighting and did not provide power to the data center computers.

The campus could lose the ability to provide data processing services in the event of a power outage, which could disrupt campus operations.

Recommendation 10

We recommend that the campus provide a means of alternate power to support data processing services in the event of a loss of power.

Campus Response

We concur. The campus will work with an engineering firm to determine the feasibility and cost of isolating the data center power supply and adding an alternate power source dedicated to the data center in the event of a loss of power. Estimated date of feasibility study completion is November 2008.

ENCRYPTION OF SENSITIVE DATA

The campus did not encrypt some sensitive personal information stored on the reporting data store (RDS).

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 encryption would cause a performance degradation and other mitigating controls were in place to protect the data.

Failure to encrypt sensitive personal information could require the campus to notify all affected individuals in the event of a breach of security and potentially damage CSU's reputation.

Recommendation 11

We recommend that campus encrypt sensitive personal information stored in the RDS as soon as possible.

Campus Response

We concur. The campus has researched the feasibility of encrypting the entire RDS database as well as certain data fields in the database and found both to be overly taxing on system performance and hardware resources. This has been corroborated by the database vendor. The university has applied several layers of security controls to the RDS server and will continue to evaluate encryption as a security protocol in addition to existing controls. The university's current controls are in compliance with laws and regulations and are consistent with CSU systemwide student system applications controls. The university accepts the risk inherent in not encrypting sensitive personal information. Encryption of sensitive information will continue to be evaluated as a security protocol within these application areas. Estimated date of completion is November 2008.

NETWORK SECURITY

Network security technologies were not configured to limit unwanted network traffic from certain critical servers.

SAM §4842.2 states that appropriate risk management procedures should be implemented to provide control of access to information assets. Effective network security practices enforcement of authentication standards and proper restriction on all network access points.

The director of network services stated that many network security features had been implemented and that the server's operating systems were sufficiently secured but it would be possible to further protect the servers by preventing unwanted network traffic from reaching them.

Failure to restrict unwanted network traffic from certain critical servers increases campus exposure to unauthorized activities by unknown individuals, which could lead to unauthorized access.

Recommendation 12

We recommend that the campus configure network security technologies to limit unwanted network traffic from reaching certain critical servers.

Campus Response

We concur. The campus limits unwanted network traffic such as worms, viruses, network scans, and other intrusions at the network firewall layer and intrusion prevention system layer. A secondary physical firewall in front of the data center was planned as part of the CSU Infrastructure Terminal Resources Project 2 initiative; however, that project was temporarily suspended by the chancellor's office due to the state budget reductions. Due to the project suspension, the campus is now planning to procure and deploy a physical firewall as a campus project. Estimated date of completion is September 2008.

DISASTER RECOVERY PLAN

The campus did not have a current disaster recovery plan.

SAM §4843.1 requires each state agency to establish and maintain both an operational recovery plan to protect its information assets in the event of a disaster or serious disruption to its operations and a plan to resume operation following a disaster affecting those applications.

The CSU *Information Security Policy*, dated August 2002, states that campuses must have plans and procedures for the protection of data against natural, accidental, and intentional disasters, which include disaster recovery planning.

The director of administrative computing services stated that the campus was in the middle of developing a campus-wide business continuity plan and that certain aspects of the information technology recovery plan had been completed; however, a final recovery plan for data processing services had not yet been completed.

The absence of a current information technology disaster recovery plan increases the risk that the campus may be unable to restore computer operations within a reasonable time frame.

Recommendation 13

We recommend that the campus prepare a current disaster recovery plan to reflect the existing environment and recovery strategies.

Campus Response

We concur. The campus will prepare a current data center disaster recovery plan. Estimated date of completion is November 2008.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
F. King Alexander	President
Celia Afan	Supervisor, Self Support Operations
Scott Apel	Assistant Vice President, Human Resources Management
Thomas Bass	Senior Director, Parking, Transportation and Event Services (PTES)
Raquel Bazan	Tax Analyst/Specialist
Elizabeth Beall	Purchasing Manager
Phil Buford	Supervisor, Payroll Services
Ignacio Carrillo	Associate Director, PTES
Nancy Eckhous	Bursar
Bob Escalante	Manager, Receiving/Property
Les Freeman	Manager, General Accounting
John Fugatt	Manager, Student Accounts Services and Cashiering
Laurinda Fuller	Senior Internal Auditor, Internal Auditing Services
William Griffith	Vice President, Administration and Finance (At time of review)
Charles Hughes	Director, Procurement and Support Services
Denitra Jones	Coordinator, Citation Processing, Parking and Transportation Services
Michael Jones	Chief Financial Officer, University College and Extension Services
Ted Kadowaki	Assistant Vice President, Budget Planning and Administration
Joseph Latter	Associate Vice President, Financial Management
Steve Law	Director, Network Services
Robyn Mack	Associate Vice President, University Services and Chief of Staff (At time of review)
Michael Markoski	Director, Administrative Computing Services, Information Technology Services
Sandy Miyake	Director, Payroll Services and Human Resource Services
Alan Moore	Field Services Operations Manager, Parking and Transportation Services
Gina Morey	Human Resources Training Program Specialist, Human Resources Management
Randy Nielson	Supervisor, Cashiering Services
Stan Olin	Director, Housing and Residential Life
Janet Parker	Associate Vice President, Human Resources Management
Christine Phu	Associate Director, Housing and Residential Life
Lauri Reilly	Manager, Accounts Payable
Marcy Rieg	Supervisor, General Accounting
Beth Ryan	Director, Human Resources Service Group
Stanley Skipworth	Interim Chief of Police, University Police Department
Aysu Spruill	Director, Internal Auditing Services
Mary Stephens	Vice President, Administration and Finance
Sergio Suarez	Director, Financial Management Information Systems
Sharon Taylor	Associate Vice President, Financial Management
Christine Welch	University Controllor



OFFICE OF THE PRESIDENT
CALIFORNIA STATE UNIVERSITY, LONG BEACH
1250 BELFLOWER BOULEVARD
LONG BEACH, CALIFORNIA 90840-0115
562/985-4121

RECEIVED
UNIVERSITY AUDITOR

JUN 26 2008

THE CALIFORNIA STATE
UNIVERSITY

June 25, 2008

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

Re: FISMA Audit Report # 07-09

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 cursive script that reads "F. King Alexander".

F. King Alexander
President

Enclosure

IA-0184

- c: Scott Apel, Associate Vice President, Human Resources Management
Janet Foster, Associate Vice President, Information Technology Services
Ted Kadowaki, Associate Vice President, Budget and University Services
Aysu Spruill, Director, Internal Auditing Services
Mary Stephens, Vice President, Administration and Finance
Sharon Taylor, Associate Vice President, Financial Management

FISMA

**CALIFORNIA STATE UNIVERSITY,
LONG BEACH**

Audit Report 07-09

CASH RECEIPTS

SATELLITE CASHIERING

Recommendation 1

We recommend that the campus:

- a. Identify all petty cash funds used throughout the campus and ensure that they are properly established and that completed count sheets are retained as evidence that independent counts are performed at prescribed frequency intervals.
- b. Process credit card receipts in a timely manner.
- c. Deposit checks in a timely manner and utilize a suspense account to maintain accountability for checks received but not applied as payments.
- d. Ensure that all checks are restrictively endorsed immediately upon receipt, or at minimum, by the end of each day.
- e. Establish mitigating controls to ensure that UCES appropriately safeguard PAN(s) and any other sensitive personal data at all times.
- f. Implement accountability procedures for the use of distributing patron bags for events.
- g. Approve parking annex as a satellite location or redirect cashiering duties to the appropriate department. If approved as a satellite location, implement procedures for transfer receipts, ensure that press-numbered receipts are available, and maintain a written record of individuals with access to the locking file cabinet used to store cash receipts at the parking annex.

Campus Response

- a. We concur. We will identify any petty cash funds not currently established with campus approval and bring them into compliance with current campus policy or eliminate the fund if not approved. Estimated date of completion is October 2008.
- b. We concur. All credit cards will be processed in a timely manner and current campus cash handling procedures will be updated to include the handling of credit card transactions. Estimated date of completion is October 2008.

- c. We concur. All checks will be deposited in a timely manner as outlined in our current campus cash handling procedures. Estimated date of completion is May 2008.
- d. We concur. All checks will be restrictively endorsed upon receipt as outlined in our current campus cash handling procedures. Estimated date of completion is May 2008.
- e. We concur. Cash handling procedures will be updated to include the handling of credit card transactions including security requirements of PCI DSS. Estimated date of completion is July 2008.
- f. We concur. Cash handling procedures will be updated to include procedures for the distribution and control of patron bags for events. Estimated date of completion is July 2008.
- g. We concur. We will eliminate cash handling at the parking annex. Estimated date of completion is May 2008.

ACCOUNTS RECEIVABLE

PAYROLL RECEIVABLE

Recommendation 2

We recommend that the campus strengthen procedures to ensure that payroll accounts receivable are promptly pursued for collection.

Campus Response

We concur. We have developed a PeopleSoft solution that creates custom payroll accounts receivable letters that generate automatically on a monthly basis for the second and third collection notices. This new automated process will ensure the second and third notices go out on a timely basis and reduce workload for the payroll technicians. We have reinforced the accounts receivable process with all payroll technicians within the payroll office. Estimated date of completion is June 30, 2008.

THIRD-PARTY RECEIVABLE

Recommendation 3

We recommend that the campus strengthen procedures to ensure that third-party receivables are promptly pursued for collection.

Campus Response

We concur. The campus has filled staff vacancies and provided training to each new hire regarding the campus established procedures for collections. Estimated date of completion is June 30, 2008.

PURCHASING

Recommendation 4

We recommend that the campus ensure that documentation is on file to indicate cardholder violations are handled and tracked in accordance with campus procurement card policy.

Campus Response

We concur. The campus will ensure the spreadsheet tracking system is up to date and approved monthly by the Director of Procurement. Violations of the campus policy will be documented in writing as outlined in our current policy. Estimated date of completion is July 2008.

OPERATING FUND

Recommendation 5

We recommend that the campus accurately document the reason for the advance in the section provided on the university check form.

Campus Response

We concur. Procedures have been reviewed with the payroll technicians who complete these forms. In addition, two management personnel employees will approve all requests. This new step will ensure that specific reasons for the request are documented and reviewed. Estimated date of completion is July 2008.

PAYROLL AND PERSONNEL

EMPLOYEE ELIGIBILITY VERIFICATION

Recommendation 6

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

Campus Response

We concur. We are reinforcing employment eligibility verification policy with all stakeholders. Non-payroll employees will no longer process I-9 paperwork. Employees who work off campus and who cannot come to payroll to sign in, must have a notary or other CSU campus to assist in the completion of the I-9 process. Estimated date of completion is July 2008.

EMPLOYEE SEPARATION

Recommendation 7

We recommend that the campus review and strengthen employee separation procedures to ensure complete clearance documentation.

Campus Response

We concur. We are reinforcing clearance process procedures with all stakeholders. Each month a letter will be sent to departments/colleges listing all separated employees lacking clearance forms. This letter requests departments provide missing clearance forms, if available, or certify/acknowledge that the forms were not completed and the circumstances. This new "check and balance" process ensures all departments/colleges are aware of missing clearance forms and the need to take responsibility for lost or missing assets. Estimated date of completion is July 2008.

FIXED ASSETS

Recommendation 8

We recommend that the campus implement the use of equipment custody forms for off-campus use of university equipment.

Campus Response

We concur. We are in the process of updating the Property Policy to reflect the current business practices for property management. The campus procedures will reflect the need to complete an equipment custody form or a departmental log for off-campus use of university equipment. Estimated date of completion is October 2008.

INFORMATION TECHNOLOGY

PASSWORD CONTROLS

Recommendation 9

We recommend that the campus activate the password controls in the human resources system to effectively restrict access in accordance with campus password security guidelines.

Campus Response

We concur. The campus has been working on the HCM password control project and plans to activate password controls in accordance with campus password security guidelines. Estimated date of completion is June 30, 2008.

DATA CENTER POWER GENERATOR

Recommendation 10

We recommend that the campus provide a means of alternate power to support data processing services in the event of a loss of power.

Campus Response

We concur. The campus will work with an engineering firm to determine the feasibility and cost of isolating the data center power supply and adding an alternate power source dedicated to the data center in the event of a loss of power. Estimated date of feasibility study completion is November 2008.

ENCRYPTION OF SENSITIVE DATA

Recommendation 11

We recommend that campus encrypt sensitive personal information stored in the RDS as soon as possible.

Campus Response

We concur. The campus has researched the feasibility of encrypting the entire Reporting Data Store (RDS) database as well as certain data fields in the database and found both to be overly taxing on system performance and hardware resources. This has been corroborated by the database vendor. The university has applied several layers of security controls to the RDS server and will continue to evaluate encryption as a security protocol in addition to existing controls. The university's current controls are in compliance with laws and regulations and are consistent with CSU systemwide student system applications controls. The university accepts the risk inherent in not encrypting sensitive personal information. Encryption of sensitive information will continue to be evaluated as a security protocol within these application areas. Estimated date of completion is November 2008.

NETWORK SECURITY

Recommendation 12

We recommend that the campus configure network security technologies to limit unwanted network traffic from reaching certain critical servers.

Campus Response

We concur. The campus limits unwanted network traffic such as worms, viruses, network scans, and other intrusions at the network firewall layer and intrusion prevention system layer. A secondary physical firewall in front of the data center was planned as part of the CSU ITRP2 initiative; however that project was temporarily suspended by the Chancellor's Office due to the state budget reductions. Due to the project suspension, the campus is now planning to procure and deploy a physical firewall as a campus project. Estimated date of completion is September 30, 2008.

DISASTER RECOVERY PLAN

Recommendation 13

We recommend that the campus prepare a current disaster recovery plan to reflect the existing environment and recovery strategies.

Campus Response

We concur. The campus will prepare a current data center disaster recovery plan. Estimated date of completion is November 2008.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR



BAKERSFIELD

July 2, 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 07-09 on *FISMA*,
California State University, Long Beach

LOS ANGELES

MARITIME ACADEMY

In response to your memorandum of July 2, 2008, I accept the response as submitted with the draft final report on *FISMA*, California State University, Long Beach.

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/jt

SACRAMENTO

Enclosure

SAN BERNARDINO

cc: Dr. F. King Alexander, President
Ms. Mary Stephens, Vice President, Administration and Finance

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS