

FISMA

**CALIFORNIA STATE UNIVERSITY,
STANISLAUS**

**Report Number 05-04
October 7, 2005**

Members, Committee on Audit

Raymond W. Holdsworth, Chair
Herbert L. Carter, Vice Chair
Roberta Achtenberg Debra S. Farar
Bob Foster George G. Gowgani
William Hauck

Staff

University Auditor: Larry Mandel
Senior Director: Janice Mirza
IS Audit Manager: Greg Dove
Internal Auditor: Ann Casey

BOARD OF TRUSTEES

THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction.....	4
Purpose	4
Scope and Methodology.....	4

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Cash Receipts.....	6
Main and Satellite Cashiering	6
Fee Authorization	9
Bank Surveys.....	10
Accounts Receivable.....	11
Third-Party Receivables	11
Write-Off and Collection.....	12
Payroll and Personnel	13
Authorization of Personnel/Payroll Transactions.....	13
Employee Separation.....	14
Fixed Assets	16
Fiscal Information Technology.....	17
Production Data Access.....	17
PeopleSoft Access Privileges	18
Sensitive Data Authorization.....	19
Disaster Recovery Plan.....	20
Information Security Procedures.....	20
Trust Funds	21
PeopleSoft Implementation.....	22
Reconciliations	22
Long-Outstanding Checks	23

APPENDICES

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

ABBREVIATIONS

CFO	Chief Financial Officer
CIO	Chief Information Officer
CMS	Common Management Systems
CSU	California State University
CSUS	California State University, Stanislaus
EO	Executive Order
FISMA	Financial Integrity and State Manager's Accountability Act
HR	Human Resources
HRL	Housing and Residential Life
ISO	Information Security Officer
MC	Main Cashier's Office
PIMS	Personnel/Payroll Management Information System
PMB	Parking Management Bureau
PPSD	Personnel/Payroll Services Division
PS	Public Safety
SAM	State Administrative Manual
SC	Stockton Campus Cashiering Office
SCO	State Controller's Office
US	United States

EXECUTIVE SUMMARY

The California Legislature passed the Financial Integrity and State Manager's Accountability Act (FISMA) of 1983. 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 Government Code, 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, Stanislaus (CSUS) management is responsible for establishing and maintaining adequate internal control. This responsibility, in accordance with Government Code, 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.
- ▶ 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 CSUS campus from March 28, 2005, through May 27, 2005, and made a study and evaluation of the accounting and administrative control in effect as of May 27, 2005. 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, fiscal information technology, and PeopleSoft implementation. 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, CSUS's accounting and administrative control in effect as of May 27, 2005, 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 [6]

Cash control weaknesses were found at the main cashier's office (MC) and all of the three satellite cashiering areas visited. Checks were not always restrictively endorsed on the day received at the parking management bureau (PMB). Duties and responsibilities related to cashiering and the reconciliation/deposit of cash receipts were not properly segregated at housing and residential life (HRL), public safety, the PMB, and the Stockton campus cashiering office. Access to funds and/or the safe at the MC and satellite locations visited was not adequately controlled, documentation of safe access required updating, and personal information at HRL was not properly protected. Additionally, receipts were not always issued to the payer at HRL. Further, newly established and changed fees were not always properly processed and approved. This is a repeat finding from our prior FISMA audit. In addition, the campus did not have a procedure to periodically request local banks to search for unauthorized bank accounts that use the campus' name, address, and federal identification number.

ACCOUNTS RECEIVABLE [11]

A receivable account had been created for a non-existent third party. In addition, the campus wrote-off some accounts receivables without requesting relief from accountability from the State Controller's Office (SCO). This is a repeat finding from our prior FISMA audit. Further, collection efforts did not include the use of a series of three collection letters with a progressively stronger tone, which is also a repeat finding from our prior FISMA audit, and an aged accounts receivable report was not generated on a regular basis for management and follow-up of delinquent third-party accounts.

PAYROLL AND PERSONNEL [13]

The delegation of authority on file with the SCO to authorize personnel and payroll transactions was not kept current, and signature cards were not properly maintained for all individuals listed on the most recently submitted delegation. In addition, employee separation procedures did not ensure timely payment of wages due and complete clearance documentation. A review of 13 employee separations disclosed that the final salary payment was not issued within 72 hours of the effective separation date in eight instances, the personnel/payroll transaction form was not properly approved in seven instances, and the campus clearance certification form was not on file in four instances and incomplete in nine instances.

FIXED ASSETS [16]

Duties and responsibilities related to the maintenance of property inventory and property records were not properly segregated.

FISCAL INFORMATION TECHNOLOGY [17]

Control over the integrity of data files was not adequate because there was no authorization or monitoring process over the use of Oracle IDs that allowed modification to production PeopleSoft data. Additionally, access roles and privileges to the PeopleSoft financial system were not effectively assigned to prevent unauthorized access and data modification. Further, the process for granting system access to sensitive data did not include obtaining proper authorization from the campus president or vice president of business and finance. In addition, the campus disaster recovery plan had not been updated since 2003 even though several changes had occurred in the environment and recovery strategy. Finally, there was no campuswide information security process, no individual assigned to ensure that appropriate security practices were being applied to all systems attached to the campus network, and there were no policies or procedures for identifying or controlling copying of sensitive information stored by the university.

TRUST FUNDS [21]

Trust fund expenditures were not always properly approved. A review of 22 trust fund expenditures disclosed that nine had not been properly approved.

PEOPLESOFT IMPLEMENTATION [22]

Certain reconciliations were not timely prepared and/or complete. A review of various reconciliations in April 2005 disclosed that the January 2005 and March 2005 revolving fund reconciliations were prepared 44 and 49 days after month's end, respectively, and the most recent bank/SCO expense, fixed assets, and investment reconciliations were for December 2004. In addition, the February 2005 revolving fund reconciliation was neither signed nor dated by the preparer or the reviewer, and the March 2005 reconciliation was not signed and dated by the reviewer. Further, long-outstanding checks were not processed/canceled in a timely manner. A review of the most recent list of outstanding checks for December 2004 showed 76 checks older than one year and one check older than two years.

INTRODUCTION

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.
- ▶ Revolving 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 2003/04 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 July 2004 to January 2005. Our primary focus was on internal controls. Specifically, we reviewed and tested:

INTRODUCTION

- ▶ 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 revolving 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 May 27, 2005. 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 AND SATELLITE CASHIERING

Cash control weaknesses were found at the main cashier's office (MC) and three satellite cashiering areas visited.

The satellite cashiering locations reviewed included housing and residential life (HRL), public safety (PS), the parking management bureau (PMB), and the Stockton campus cashiering office (SC). In addition, we reviewed safe access and combination change documentation for all satellite locations.

Restrictive Endorsement of Checks

At the PMB, checks were not always restrictively endorsed on the day received. Checks not processed by the end of the day were stored overnight in the safe and endorsed when processed the following day.

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

The PMB administrative coordinator stated that checks were not always endorsed on the same day due to limited staff availability.

Segregation of Duties

Duties and responsibilities related to cashiering and the reconciliation/deposit of cash receipts were not properly segregated at HRL, PS, the PMB, and the SC.

- ▶ At HRL, the administrative support assistant performed all cash receipt functions with no supervision or verification of work performed.
- ▶ At PS and the PMB, the individual that received and processed payments also posted receipts information, prepared the deposit, and performed reconciliations.
- ▶ At the SC, the administrative support assistant performed all cash receipt functions, the academic support services coordinator collected monies from copy machines and prepared the deposit, and the library center manager received and collected library monies and posted all cash receipts to the library cashiering system.

SAM §8080, §8080.1, and §8080.2 state, in part, that no one person will perform more than one of the following types of duties: maintaining books of original entry, receiving and depositing remittances, inputting receipts information, and reconciling input to output.

SAM §8032.3 states that except where the supervisor and the person depositing cash are not at the same location, the person supervising the person depositing cash will verify that receipts have been deposited intact and in accordance with SAM §8032.1.

The HRL administrative support assistant, PS support services supervisor, and SC academic support services coordinator stated that current staffing levels limited the ability to adequately segregate each of the functions.

Safety of Funds and Protection of Confidential Data

Access to funds and/or the safe at the MC and satellite locations visited was not adequately controlled, documentation of safe access required updating, and personal information at HRL was not properly protected.

We found that:

- ▶ At the MC, checks were not placed in the cash drawers or other secure storage facility upon receipt from customers. Instead, the checks were placed in a plastic index card holder mounted to the cashiering counter.
- ▶ At HRL and the SC, keys to the cash drawers or other secure storage facility were not adequately controlled. At HRL, we observed that a check was being stored in a desk drawer with the key in the lock and were told that the key was kept in the drawer lock at all times during operating hours even when the cashier stepped away for breaks. At the SC, the whereabouts of the keys to the cash drawers were unknown; consequently, the drawers remained unlocked. In addition, cash drawers at PS were not transferred to the safe for safekeeping after hours.
- ▶ At HRL, daily receipts/deposits of currency typically ranged from \$64 to \$10,000. However, deposits were transferred to the MC by only one individual in a plain white envelope.
- ▶ At the SC, the combination to the safe was written on an index card and kept under a ten-key calculator on a desk located in the academic support services coordinator's office, which was kept unlocked with the door open throughout the day. In addition, campus documentation of individuals with access to safes required updating because HRL and procurement department safes were not included on the listing.
- ▶ At the MC and SC, safes were kept unlocked throughout the day even though the doors to the rooms where the safes were located remained unlocked and open. In addition, the HRL safe was located in a high traffic area, which was accessible to an unknown number of individuals and viewable from outside the building, and the safe was not anchored to the building.
- ▶ At HRL, students' social security numbers were being written on checks after acceptance for payment.

SAM §8032.1 requires that receipts be adequately safeguarded until deposited. When such funds are not in use, they will be locked in a desk, file cabinet, or other mechanism providing comparable safekeeping.

SAM §8032.4 states that whenever coin and currency to be deposited exceeds \$3,000 and armored car service is either not available, or excessively expensive, two employees should be assigned to deliver the deposit jointly or two or more deposits may be made to reduce the cash transported at one time.

SAM §8024 requires the campus to change the safe combinations when employees leave a department and to retain a record listing the names of individuals with knowledge of a department's safe combination and the date the combination was last changed.

SAM §8025 states that, as a deterrent to burglary, state agencies will securely anchor a safe to the building and, where practical, to the building's foundation.

SAM §20050 states that the elements of a satisfactory system of accounting and administrative control shall include, in part, a plan that limits access to state assets to authorized personnel who require these assets in the performance of assigned duties. Further, internal accounting controls comprise the methods and procedures directly associated with safeguarding assets.

California State University (CSU) directive HR 2005-16, *Requirements for Protecting Confidential Personal Data*, dated April 8, 2005, states that each campus and the chancellor's office must take necessary measures to protect confidential personal information, which includes, but is not limited to social security numbers.

The MC lead cashier, HRL administrative support assistant, PS support services supervisor, and SC academic support services coordinator stated their beliefs that the issues noted above were not substantial risks. The assistant vice president of financial services stated that she was unaware of the above-mentioned practices. She also stated that the campus had established procedures to adequately safeguard all collections; however, the satellite locations chose to deviate from those procedures.

Receipts

At HRL, receipts were only issued to the payer upon request.

SAM §8020 states that state agencies will prepare receipts for all collections, unless specifically exempted in writing by the Department of Finance, Fiscal Systems and Consulting Unit, of coin or currency received in person from payers who are not given press-numbered documents of fixed value (such as guest meal tickets) at the time of payment.

The HRL administrative support assistant stated her belief that receipts were not needed since all student transactions could be viewed via the Internet.

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

Recommendation 1

We recommend that the campus:

- a. Ensure that all checks received at the PMB are restrictively endorsed by the end of the day.
- b. Review cashiering activities at HRL, PS, the PMB, and the SC, and take appropriate action to either segregate duties or establish effective mitigating controls.
- c. Ensure that all receipts at the MC, HRL, and the SC are adequately safeguarded in cash drawers or other secure mechanism until deposited.
- d. Establish and implement procedures at HRL for two employees to transport funds whenever coin and currency to be deposited exceeds \$3,000.
- e. Change the SC safe combination, remind those individuals with knowledge of safe combinations of the need to keep them confidential, and update campus documentation of individuals with access to safes.
- f. Require that safes at the MC and SC be kept locked when not in use and appropriately anchor the HRL safe to the building and consider relocating the safe to a more secure location.
- g. Establish and implement a policy to prohibit writing social security numbers on checks.
- h. Establish and implement procedures at HRL to ensure that payers are given receipts at the time of payment.

Campus Response

We concur. Cashiering activities at HRL, PS, the PMB, MC, and SC are being reviewed to ensure appropriate internal controls are in place. The director of student financial services has begun meeting with each area to ensure the items listed above are corrected and proper procedures are established. Each satellite cashiering site will be visited at least twice annually to ensure compliance. All deficiencies will be corrected by January 2006.

FEE AUTHORIZATION

Newly established and changed fees were not always properly processed and approved. This is a repeat finding from our prior Financial Integrity and State Manager's Accountability Act (FISMA) audit.

We found that:

- ▶ One new fee (Entomology 4332) and one changed fee (Microbiology 3032) lacked evidence of consideration by the campus fee advisory committee and authorization by the president.
- ▶ One changed fee (Parking – Daily) lacked evidence of authorization by the president.

Executive Order (EO) 740, *The California State University Student Fee Policy*, dated April 13, 2000, states, in part, that delegated authority is given to the chancellor to establish new campus fees and to the president to increase, decrease, or abolish campus fees. For category III fees, consideration by the campus fee advisory committee is required before the president either requests the chancellor to establish a new fee or adjusts a current fee.

The assistant vice president of financial services stated that it was an oversight that the fees had not been discussed by the campus fee advisory committee and were not approved by the president.

Improper fees could be assessed if the required authorization and consideration by the campus fee advisory committee is not obtained.

Recommendation 2

We recommend that the campus take appropriate action to obtain approval for the above-mentioned fee actions and strengthen controls to ensure that fee actions are properly processed and approved in the future.

Campus Response

We concur. The fees not appropriately approved by the student fee advisory committee have been brought before the committee and will be voted on shortly. Parking fee increases will be presented to the president for approval. These actions will be completed by January 2006.

BANK SURVEYS

The campus did not have a procedure to periodically request local banks to search for unauthorized bank accounts that use the campus' name, address, and federal identification number.

Government Code §13401(b)(3) states that all levels of management of state agencies must be involved in assessing and strengthening the systems of internal accounting and administrative control to minimize fraud, errors, abuse, and waste of government funds.

The assistant vice president of financial services stated that prior efforts to search for unauthorized bank accounts had been made but had not been recently attempted.

The lack of a process to periodically search for unauthorized bank accounts increases the risk of the campus being associated with improper bank accounts.

Recommendation 3

We recommend that the campus establish and implement procedures to periodically request local banks to search for unauthorized bank accounts that use the university's name, address, and federal identification number.

Campus Response

We concur. Letters have been sent to local banks asking them to search for bank accounts using the university's name, address, and federal ID number. A sample of these letters will be forwarded by January 2006.

ACCOUNTS RECEIVABLE

THIRD-PARTY RECEIVABLES

A receivable account had been created for a non-existent third party.

A receivable account and related invoices were created for a non-existent third party, the California State University, Stanislaus (CSUS) Study Abroad Program. Invoices were created for the tuition of foreign exchange students attending CSUS, even though the foreign exchange students paid tuition at their home school and never directly paid tuition to CSUS. The invoices were created with the expectation that students in the United States (US) would go abroad in exchange and the US students' tuition would be applied against the foreign exchange students' invoices/CSUS Study Abroad Program receivables.

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.

The assistant vice president of financial services stated that she was unaware of this procedure and added that it would be discontinued.

Recording non-existent accounts receivables results in an overstatement of assets.

Recommendation 4

We recommend that the campus immediately discontinue the aforementioned practice, close-out the CSUS Study Abroad Program receivable account, and strengthen procedures to ensure that only valid accounts receivables are recorded.

Campus Response

We concur. The campus has suspended the practice of recording non-existent third-party receivables for foreign exchange students. A printout showing a zero balance in the receivable account will be forwarded by January 2006.

WRITE-OFF AND COLLECTION

The campus wrote-off some accounts receivables without requesting relief from accountability from the State Controller's Office (SCO), and collection efforts required improvement.

We found that:

- ▶ The campus wrote-off some accounts over \$1,000 without submitting an application for discharge from accountability from the SCO. This is a repeat finding from the prior FISMA audit.
- ▶ Although monthly account statements were sent, accounts receivable collection efforts did not include the use of a series of three collection letters with a progressively stronger tone. This is a repeat finding from the prior FISMA audit.
- ▶ An aged accounts receivable report was not generated on a regular basis for management and follow-up of delinquent third-party accounts. In addition, our review of the aged accounts receivable report generated for our audit as of April 2005 disclosed that 15 of the 63 accounts had outstanding balances 120 days or older. In total, \$105,805 of the \$471,929 (22.4%) accounts receivable balance at April 2005 was outstanding 120 days or more.

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.

SAM §8776.6 provides procedures and guidelines regarding adequate collection efforts and follow-up on receivables, including a sequence of three collection letters at 30-day intervals with a progressively stronger tone and specific requirements for filing applications for Discharge From Accountability (form STD. 27) with the SCO.

SAM §20050 indicates, in part, 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. Further, financial and operational reporting that is not timely or used as an effective management tool is a signal of a poorly maintained or vulnerable control system.

The director of student financial services stated that the campus had not submitted any applications for discharge from accountability because past applications were denied no matter how much documentation was provided; consequently, discharge from accountability had become a low priority

because of the additional work required and the low probability of success. The assistant vice president of financial services stated her belief that billing statements generated and sent out monthly were sufficient for collection efforts. She also stated that an aged accounts receivable report was not a necessary tool to monitor accounts receivables and therefore the campus did not utilize one.

Inadequate control over accounts receivables increases the risk that receivables will not be properly controlled and reflected in campus financial statements, reduces the likelihood of collection, and negatively impacts cash flow.

Recommendation 5

We recommend that the campus:

- a. Reestablish procedures to submit applications for discharge of accountability to the SCO for accounts exceeding \$1,000.
- b. Establish and implement procedures to use a series of three collection letters with a progressively stronger tone.
- c. Produce and use an aged accounts receivable report on a regular basis in its management and follow-up of delinquent accounts.

Campus Response

We concur. All old accounts receivables over \$1,000 will be submitted to the SCO for discharge of accountability. Progressively stronger collection letters are now being sent to campus debtors and an accounts receivable aging report will be run at least quarterly. A copy of procedures, sample letters, and an aging report will be provided by January 2006.

PAYROLL AND PERSONNEL

AUTHORIZATION OF PERSONNEL/PAYROLL TRANSACTIONS

The delegation of authority on file with the SCO to authorize personnel and payroll transactions was not kept current, and signature cards were not properly maintained for all individuals listed on the most recently submitted delegation.

We found that:

- ▶ Three of the Signature Authorization Personnel/Payroll Documents (PPSD 8A-Rev) did not bear a signature of an appointing power.
- ▶ Two individuals approving payroll/personnel transactions did not have signature cards (PPSD 8A-Rev).

- ▶ One individual approving payroll/personnel transactions was not listed on the SCO listing.

The CSU *Personnel/Payroll Management Information System (PIMS) User Manual* indicates that transactions keyed at the campus may be documented on any campus-generated form or report as long as there is an authorized signature on the document (under *General Information in Transaction Overview*).

The SCO, Personnel/Payroll Services Division *Payroll Procedures Manual* requires an authorized signature certifying that the information on the payroll document is correct. It is the responsibility of each campus to ensure that the signature card file of employees authorized to sign various payroll documents maintained by the SCO, Personnel/Payroll Services Division is accurate (under *Introduction §1500 and Agency/Campus Responsibility §1501*).

The assistant vice president of financial services stated that the missing documentation and authorizations were an oversight.

Failure to maintain current delegations of authority and signature cards increases the risk of inappropriate or unauthorized transactions.

Recommendation 6

We recommend that the campus strengthen controls to ensure that the delegation of authority on file with the SCO remains current and signature cards are kept on file.

Campus Response

We concur. The delegation of authority on file with the SCO has been updated and copies of the submitted signature cards are on file. Copies of the current delegation and signature cards will be forwarded by January 2006.

EMPLOYEE SEPARATION

Employee separation procedures did not ensure timely payment of wages due and complete clearance documentation.

Our review of 13 employee separations between August 2003 and December 2004 disclosed that:

- ▶ In eight instances, the final salary payment was not issued within 72 hours of the effective separation date.
- ▶ In seven instances, the personnel/payroll transaction form was not signed by an official approving authority.
- ▶ In four instances, the campus clearance certification form was not on file.

- ▶ In two instances, verification of the clearance of revolving fund advances was not evidenced on the campus clearance certification form.
- ▶ In seven instances, the campus clearance certification form did not provide a line for the verification for clearance of revolving fund advances. Two different clearance forms were being utilized. The human resources campus clearance certification form addressed clearance of revolving fund advances, while the faculty affairs' form did not.

CSU directive HR 2003-15, Attachment B, states that Labor Code §201 and §202 require the CSU to pay separating employees in a specified time frame. Payment of owed wages to discharged and resigned employees is treated differently in the Labor Code. An employee who is discharged must immediately be paid wages earned. An employee who resigns from employment must be paid wages earned no later than 72 hours from the date of separation. However, if the employee provides the employer at least 72 hours notice of his/her impending separation, he/she is entitled to wages owed at the time of separation.

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

The assistant vice president of financial services stated that she was unaware that separation procedures and policies were not being adhered to and that the inconsistency of the clearance forms was an oversight.

Insufficient control over employee separations increases the risk of late wage payments, 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 the timely payment of wages and complete clearance documentation.

Campus Response

We concur. We are working to remedy the situation and will strengthen employee separation procedures. Separation wages will be paid in a timely manner and clearance forms will be completed appropriately. Copies of forms and procedures will be forwarded by February 2006.

FIXED ASSETS

Duties and responsibilities related to the maintenance of property inventory and records were not properly segregated.

We noted that the property clerk performed the following duties:

- ▶ Reviewed purchase orders and invoices to verify that charges were appropriately assigned to the correct general ledger account.
- ▶ Performed the physical inventory of the fixed assets and sometimes tagged property.
- ▶ Managed and maintained the fixed assets inventory database and inventory records/property ledgers.
- ▶ Processed, approved/certified, arranged, and directed all disposals of fixed assets. Processed forms for disposal of lost or stolen property and presented forms to the property survey board. The property clerk was also a member of the property survey board.
- ▶ Prepared the fixed assets monthly reconciliation, which was sent to general accounting as notification of any additions or removals of property to/from inventory. General accounting adjusted the general ledger fixed assets accounts accordingly, but did not review corresponding purchase orders or invoices.
- ▶ Reported property losses and thefts to the campus police department.
- ▶ Maintained property check-out forms for property loaned to employees.
- ▶ Managed and maintained the retired property stock room.

SAM §20050 states that the elements of a satisfactory system of internal accounting and administrative controls shall include a plan of organization that provides segregation of duties appropriate for proper safeguarding of state assets.

SAM 8652 states that the person in charge of the stockroom will not be in charge of maintaining records or the taking of physical inventories.

The assistant vice president of financial services stated that due to limited manpower, the property clerk had to assume the above-listed duties.

Inadequate segregation of duties over assets increases the risk of errors, irregularities, and misappropriation.

Recommendation 8

We recommend that the campus review fixed assets duties and take appropriate action to either segregate incompatible duties or establish effective mitigating controls.

Campus Response

We concur. All current job duties and responsibilities assigned to the property clerk are being reviewed. A new job description and new procedures are being developed. The new procedures and/or mitigating controls will be sent by January 2006.

FISCAL INFORMATION TECHNOLOGY

PRODUCTION DATA ACCESS

There were no authorization or monitoring controls over the use of Oracle IDs that allowed modification to production PeopleSoft data.

SAM §4842.2 states that appropriate risk management procedures should be implemented to safeguard the integrity of data files, which includes effective account management. Effective account management is considered to include an appropriate authorization and monitoring of accounts that have access to production data files.

The database administrator stated that guidelines had not yet been established for monitoring the use of production Oracle accounts.

Inadequate control over the use and monitoring of accounts with access to production data increases the risk of unauthorized and undetected modification of production data.

Recommendation 9

We recommend that the campus implement a process for authorizing and monitoring the use of Oracle IDs with access to production data to ensure that all such access is authorized and appropriate.

Campus Response

We concur. Starting immediately, the chief information officer (CIO) and chief financial officer (CFO) will review any application for an Oracle ID and authorize based on merit. Each application will have a sunset date. After that date, an application can be renewed using the same process as the initial application. Reports from available Common Management Systems (CMS) central data will be given to both the CIO and CFO on a regular basis to monitor the use of the Oracle IDs.

PEOPLESOFT ACCESS PRIVILEGES

Access roles and privileges to the PeopleSoft financial system were not effectively assigned to prevent unauthorized access and data modification.

We found that:

- ▶ Consultants had been granted privileges.
- ▶ Unused classes had not been removed.
- ▶ Unused IDs had not been removed.
- ▶ Some individuals had been given privileges to the purchasing, general ledger, and accounts payable modules, which were not compatible with their assigned duties.
- ▶ Test accounts were present in the production environment.

SAM §8080.1 states that each state agency to establish and maintain an adequate system of internal control, and that a key element in a system of internal control is separation of duties. Further, “no one person shall perform more than one of 11 types of duties, including maintaining records file and operating mechanized equipment, initiating disbursement documents, approving disbursement documents, and inputting disbursement information.”

SAM §20050 states that the elements of a satisfactory system of internal accounting and administrative controls include a plan of organization that provides segregation of duties appropriate for proper safeguarding of state assets.

The business systems analyst of financial services stated that the system had been recently implemented, and the privileges that were set up for pre-production had not yet been reevaluated.

Failure to properly limit access to only those who need to perform job duties increases the risk of fraudulent or unauthorized activities.

Recommendation 10

We recommend that the campus review access privileges and take appropriate action to segregate duties and restrict update responsibilities. Specifically, the campus should:

- a. Remove consultant access to production.
- b. Remove unused roles, permissions, and IDs.
- c. Remove individual privileges to multiple application modules incompatible with their assigned duties.

- d. Remove test accounts from the production environment.

Campus Response

We concur. The financial services systems analyst is reviewing all access privileges and working with the assistant vice president of financial services to determine appropriate segregation of duties and restriction of update and deletion privileges. Evidence of correction of this finding will be sent by January 2006.

SENSITIVE DATA AUTHORIZATION

The process for granting system access to sensitive data did not include obtaining proper authorization from the campus president or vice president of business and finance.

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 chancellor's information security memorandum to CSU presidents dated March 28, 2003, states that no CSU employee will be granted access to confidential information contained in the CSU computer systems without review and written approval by the campus president or vice president of administration.

The director of administrative technology support stated his belief that the campus process was in compliance with the memorandum from the chancellor's office.

Failure to properly obtain executive management authorization increases the risk of inappropriate access to sensitive data.

Recommendation 11

We recommend that the campus amend its access request process to include proper authorization from the campus president or vice president of business and finance.

Campus Response

We concur. The form that is used for access request will be modified to include a place for the approval of the vice president of business and finance. The revised form will be submitted by January 2006.

DISASTER RECOVERY PLAN

The campus disaster recovery plan had not been updated since 2003 even though several changes had occurred in the environment and recovery strategy.

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 technology support stated that the campus had recently completed making significant changes to its information technology environment and an update of the disaster plan was intentionally delayed until the changes to the environment were complete.

Without a current information technology disaster recovery plan that addresses all significant components required for recovery, the campus may not be able to restore computer operations within a reasonable time frame.

Recommendation 12

We recommend that the campus update its disaster recovery plan to reflect the existing environment.

Campus Response

We concur. We are in the process of setting up a cold site for disaster recovery and will update the plan as soon as the implementation is complete. The updated plan will be submitted by February 2006.

INFORMATION SECURITY PROCEDURES

There was no campuswide information security process, no individual assigned to ensure that appropriate security practices were being applied to all systems attached to the campus network, and there were no policies or procedures for identifying or controlling copying of sensitive information stored by the university.

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 CSU *Information Security Policy*, dated August 2002, states that campuses must have security policies and procedures that, at a minimum, implement information security, confidentiality practices consistent with these policies, and end-user responsibilities for the physical security of the equipment

and the appropriate use of hardware, software, and network facilities. The policy applies to all data systems and equipment on campus that contain data deemed private or confidential, including departmental, divisional, and other ancillary systems and equipment.

The CIO stated that a formal information security officer (ISO) position had not been created and that campuswide security policies and procedures were addressed on an as-needed basis.

Security practices that fail to ensure campuswide policy and compliance increase the risk of unauthorized exceptions, and could compromise compliance with statutory information security requirements.

Recommendation 13

We recommend that the campus create a campuswide information security process, including policies and procedures for copying sensitive information, and assign an individual to ensure appropriate security practices on a campuswide basis. One method to ensure campuswide participation in information security practices would be the establishment of an interdepartmental executive council with responsibility and authority to address information security issues, in conjunction with a campuswide working committee to oversee security implementation and monitoring.

Campus Response

We concur. The campus has developed security incident reporting guidelines and a network security practices document. These will be submitted to various affected campus committees and implemented by March 2006. The systemwide ISO group has drafted policies and procedures for records and information retention, information security roles and responsibilities, and protected information classification level guidelines. The CIO currently serves as the ISO and attends the systemwide meetings. We will use these policies as models and finalize campus procedures. We also hope to have an individual in place by the end of fiscal year 2005/06 responsible for monitoring that appropriate security practices on campus are in place. The policies and procedures for information security practices will be in place by June 2006.

TRUST FUNDS

Trust fund expenditures were not always properly approved.

Our review of 22 trust fund expenditures disclosed that nine had not been approved by an individual who was authorized per the corresponding trust agreement.

SAM §19440.1 provides that each trust account established shall be supported by documentation of the persons authorized to withdraw or expend funds, their specimen signatures, the purpose of the trust, and restrictions on the use of monies.

The assistant vice president of financial services stated that the lack of authorization of trust expenditures was related to trust procurement card and travel expenditures that were not reviewed for appropriate authorizing signatures. She added that the other unauthorized signatures were an oversight by the accountant assigned to perform this review.

Failure to obtain proper authorization for trust expenditures increases the risk of inappropriate expenditures and loss.

Recommendation 14

We recommend that the campus strengthen procedures to ensure that trust fund expenditures are properly authorized.

Campus Response

We concur. The campus is strengthening procedures governing trust accounts to ensure expenditures are reviewed for an appropriate authorizing signature. New procedures will be implemented by January 2006.

PEOPLESOFT IMPLEMENTATION

RECONCILIATIONS

Certain reconciliations were not timely prepared and/or complete.

During our review of various reconciliations in April 2005, we noted that:

- ▶ The revolving fund reconciliations for January 2005 and March 2005 were prepared 44 and 49 days after month's end, respectively. The February 2005 reconciliation was neither signed nor dated by the preparer or the reviewer such that we were unable to determine when it was completed, and the March 2005 reconciliation was not signed and dated by the reviewer.
- ▶ The most recent bank/SCO expense reconciliation was for December 2004.
- ▶ The most recent fixed assets reconciliation was for December 2004.
- ▶ The most recent investment reconciliation was for December 2004.

SAM §7800 requires that subsidiary records be reconciled to the general ledger monthly.

SAM §7908 requires all reconciliations show the preparer's name, reviewer's name, date prepared, and dated reviewed.

SAM §7920 requires a reconciliation of two or more accounts or other record kept by an agency such as reconciliation of office revolving fund assets to the amount withdrawn.

SAM §7901 requires monthly preparation of all reconciliations within 30 days of the preceding month.

SAM §7923 requires departments reconcile their end-of-the-month bank and centralized State Treasury system account balances monthly showing fund's share on the bank reconciliation and an explanation on the reconciliation of every reconciling item between the bank and the department's records. Errors on the bank statement will be corrected as provided in SAM §8060. The person reconciling the bank statement will trace every reconciling item between the bank and the agency's records and include an explanation on the reconciliation.

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 §20500 states that the elements of a satisfactory system of internal accounting and administrative control include a system of authorization and recordkeeping procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenditures.

The assistant vice president of financial services stated that the delay in producing the reconciliations was due to setbacks resulting from the PeopleSoft conversion.

Untimely reconciliations limit the campus' ability to detect errors and irregularities and increase the likelihood of loss of state funds.

Recommendation 15

We recommend that the campus strengthen procedures to ensure that all reconciliations are prepared in a timely and complete manner.

Campus Response

We concur. Reconciliations temporarily were not prepared in a timely manner following the initial implementation of CMS/PeopleSoft Financials. All reconciliations are now being completed on a timely basis. Samples of completed reconciliations will be sent by January 2006.

LONG-OUTSTANDING CHECKS

Long-outstanding checks were not processed/canceled in a timely manner.

We reviewed the most recent list of outstanding checks for December 2004 and noted 76 checks older than one year, and one check older than two years.

SAM §8042 states that checks have a one-year period of negotiability, unless specific provisions of law require cancellation in a different period of time. Further, agencies will send a stop payment request form to the State Treasurer's Office for all uncashed checks timed to arrive at least one week prior to the end of the one-year period of negotiability.

The general accounting manager stated that the PeopleSoft conversion had limited staff resources.

Failure to process long-outstanding checks increases the risk of misappropriation and requires additional effort to review outstanding checks during the reconciliation process.

Recommendation 16

We recommend that the campus promptly process the noted long-outstanding checks and establish procedures to ensure that future long-outstanding checks are processed in a timely manner.

Campus Response

We concur. The campus is currently processing all long-outstanding checks. This procedure temporarily was not completed for several months due to the staffing resources required to complete the CMS/PeopleSoft Financials implementation. Long-outstanding checks will be processed at least on a quarterly basis. Established procedures and evidence of current processing of long-outstanding checks will be sent by January 2006.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Hamid Shirvani	President
Marvalene Hughes	President (At time of review)
Julie Benevedes	General Accounting Manager, Accounting
Frank Borrelli	Property Clerk, Property Control
Melody Bughi	Buyer, Purchasing
Carol Castillo	Director of Procurement Services, Purchasing
Pamela Craft	Academic Support Services Coordinator, CSUS Stockton Cashiering Office
Shawna Crawford	Administrative Support Assistant, Housing and Residential Life
Debbie DaRosa	Lead Buyer, Purchasing
April Dunham-Filson	Accountant, Accounting
D'Ette Gonzalez	Payroll Technician, Payroll Office
Bety Gonzalez De Brito	Accounting Technician, Student Accounts Receivable
Delfin Guillory	Accounts Receivable and Collections Team Lead, Student Accounts Receivable
Vickie Harrang	Administrative Assistant, Human Resources
Trish Hendrix	Accounting Technician, Accounting
Sara Hoek	Senior Human Resources Technician, Human Resources
Charles Holmberg	Director of Administrative Technology Support, Information Technology
Tammy Horner	Accountant, Accounting
Steven Jaureguy	Director Public Safety/Police Chief, Public Safety/University Police Services
Elisa Johnson	Administrative Assistant, Financial Services
Jacque Keeney	Payroll Technician, Payroll Office
Mary Kobayashi Lee	Director, Human Resources
Michelle Legg	Budget Manager, Financial Services
Dosie Lewis	Cashier Team Lead, Cashier's Office
Maithreyi Manoharan	Chief Information Officer, Information Technology
Vadon McIlwain	Associate Director of Admissions, Admission and Records
Steven Meadows	Support Services, Reprographics
Rudy Medina	Information Technology Consultant, Information Technology
Donna Moore	Accountant, Accounting
Donevon Murrell	Support Services Supervisor, Public Safety/University Police Services
Becka Paulsen	Assistant Vice President, Financial Services
Irma Perrone	Human Resources Analyst, Human Resources
Jim Phillips	Director, Student Financial Services
Jon Potter	Community Service Supervisor, Public Safety/University Police Services
Carrie Retemeyer	Database Administrator, Information Technology
Julia Reynoso	Assistant Director, Facilities Administrative Services
Jose Rios	Administrative Support Coordinator, Information Technology
Sherri Rivera	Payroll Technician, Payroll Office
Robert Rosas	Shipping and Receiving Clerk, Shipping Receiving/Facilities Warehouse

APPENDIX A: PERSONNEL CONTACTED

Christine Sanders	Parking Management Bureau Administrative Coordinator, Public Safety/University Police Services
Bernadette Sather	Business Systems Analyst for Financial Services, Information Technology
Christine Snyder	Assistant to the Vice President, Student Affairs
Mary Stephens	Vice President, Business and Finance

STATEMENT OF INTERNAL CONTROLS

A. INTRODUCTION

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

B. INTERNAL CONTROL DEFINITION

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

1. Internal Accounting Controls

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

2. Operational Controls

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

C. INTERNAL CONTROL OBJECTIVES

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

D. INTERNAL CONTROL SYSTEMS LIMITATIONS

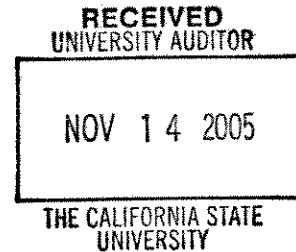
There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal accounting and related operational control. In the performance of most control procedures, errors can result from misunderstanding of instruction, mistakes of judgment, carelessness,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



CALIFORNIA STATE UNIVERSITY, STANISLAUS

801 West Monte Vista Avenue • Turlock, California 95382
(209) 667-3077 • FAX (209) 667-3350

Vice President for Business and Finance



November 14, 2005

Larry Mandel, University Auditor
Office of the Chancellor
401 Golden Shore
Long Beach, CA 90802-4210

Dear Larry:

The campus responses to the recent FISMA audit recommendations are enclosed. We appreciate the effort made to point out our internal control weaknesses and assure you that all areas of weakness will be fully addressed over the next few months.

Any questions concerning the response should be directed to Becka Paulsen, Assistant Vice President for Financial Services, at (209) 667-3379 or via email at bpaulsen@csustan.edu.

Sincerely,

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

Mary Stephens
Vice President for Business and Finance

Attachment

cc: President Shirvani
Assistant Vice President Paulsen

California State University, Stanislaus
Responses to FISMA Audit Findings
Report No. 05-04
October 2005

CASH RECEIPTS

MAIN AND SATELLITE CASHIERING

Recommendation 1

We recommend that the campus:

- a. Ensure that all checks received at the PMB are restrictively endorsed by the end of the day.
- b. Review cashiering activities at HRL, PS, the PMB, and the SC, and take appropriate action to either segregate duties or establish effective mitigating controls.
- c. Ensure that all receipts at the MC, HRL, and the SC are adequately safeguarded in cash drawers or other secure mechanism until deposited.
- d. Establish and implement procedures at HRL for two employees to transport funds whenever coin and currency to be deposited exceeds \$3,000.
- e. Change the SC safe combination, remind those individuals with knowledge of safe combinations of the need to keep them confidential, and update campus documentation of individuals with access to safes.
- f. Require that safes at the MC and SC be kept locked when not in use and appropriately anchor the HRL safe to the building and consider relocating the safe to a more secure location.
- g. Establish and implement a policy to prohibit writing social security numbers on checks.
- h. Establish and implement procedures at HRL to ensure that payers are given receipts at the time of payment.

Campus Response

We concur. Cashiering activities at housing and residential life, public safety, the Parking Management Bureau, main cashiering and Stockton cashiering are being reviewed to ensure appropriate internal controls are in place. The Director of Student Financial Services has begun meeting with each area to ensure the items listed above are corrected and proper procedures are established. Each satellite cashiering site will be visited at least twice annually to ensure compliance. All deficiencies will be corrected by January 2006.

FEE AUTHORIZATION

Recommendation 2

We recommend that the campus take appropriate action to obtain approval for the above-mentioned fee actions and strengthen controls to ensure that fee actions are properly processed and approved in the future.

Campus Response

We concur. The fees not appropriately approved by the Student Fee Advisory Committee have been brought before the Committee and will be voted on shortly. Parking fee increases will be presented to the President for approval. These actions will be completed by January 2006.

BANK SURVEYS

Recommendation 3

We recommend that the campus establish and implement procedures to periodically request local banks to search for unauthorized bank accounts that use the university's name, address, and federal identification number.

Campus Response

We concur. Letters have been sent to local banks asking them to search for bank accounts using the university's name, address, and federal ID number. A sample of these letters will be forwarded by January 2006.

ACCOUNTS RECEIVABLE

THIRD-PARTY RECEIVABLES

Recommendation 4

We recommend that the campus immediately discontinue the aforementioned practice, close-out the CSUS Study Abroad Program receivable account, and strengthen procedures to ensure that only valid accounts receivables are recorded.

Campus Response

We concur. The campus has suspended the practice of recording non-existent third party receivables for foreign exchange students. A printout showing a zero balance in the receivable account will be forwarded by January 2006.

WRITE-OFF AND COLLECTION

Recommendation 5

We recommend that the campus:

- a. Reestablish procedures to submit applications for discharge of accountability to the SCO for accounts exceeding \$1,000.
- b. Establish and implement procedures to use a series of three collection letters with a progressively stronger tone.
- c. Produce and use an aged accounts receivable report on a regular basis in its management and follow-up of delinquent accounts.

Campus Response

We concur. All old accounts receivable over \$1,000 will be submitted to the SCO for discharge of accountability. Progressively stronger collection letters are now being sent to campus debtors and an accounts receivable aging report will be run at least quarterly. A copy of procedures, sample letters, and an aging report will be provided by January 2006.

PAYROLL AND PERSONNEL

AUTHORIZATION OF PERSONNEL/PAYROLL TRANSACTIONS

Recommendation 6

We recommend that the campus strengthen controls to ensure that the delegation of authority on file with the SCO remains current and signature cards are kept on file.

Campus Response

We concur. The delegation of authority on file with the SCO has been updated and copies of the submitted signature cards are on file. Copies of the current delegation and signature cards will be forwarded by January 2006.

EMPLOYEE SEPARATION

Recommendation 7

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

Campus Response

We concur. We are working to remedy the situation and will strengthen employee separation procedures. Separation wages will be paid in a timely manner and clearance forms will be completed appropriately. Copies of forms and procedures will be forwarded by February 2006.

FIXED ASSETS

Recommendation 8

We recommend that the campus review fixed assets duties and take appropriate action to either segregate incompatible duties or establish effective mitigating controls.

Campus Response

We concur. All current job duties and responsibilities assigned to the property clerk are being reviewed. A new job description and new procedures are being developed. The new procedures and/or mitigating controls will be sent by January 2006.

FISCAL INFORMATION TECHNOLOGY

PRODUCTION DATA ACCESS

Recommendation 9

We recommend that the campus implement a process for authorizing and monitoring the use of Oracle IDs with access to production data to ensure that all such access is authorized and appropriate.

Campus Response

We concur. Starting immediately, the CIO and CFO will review any application for an Oracle ID and authorize based on merit. Each application will have a sunset date. After that date, an application can be renewed using the same process as the initial application. Reports from available CMS Central data will be given to both the CIO and CFO on a regular basis to monitor the use of the Oracle IDs.

PEOPLESOFT ACCESS PRIVILEGES

Recommendation 10

We recommend that the campus review access privileges and take appropriate action to segregate duties and restrict update responsibilities. Specifically, the campus should:

- a. Remove consultant access to production.
- b. Remove unused roles, permissions, and IDs.
- c. Remove individual privileges to multiple application modules incompatible with their assigned duties.
- d. Remove test accounts from the production environment.

Campus Response

We concur. The Financial Services systems analyst is reviewing all access privileges and working with the AVP, Financial Services to determine appropriate segregation of duties and restriction of update and deletion privileges. Evidence of correction of this finding will be sent by January 2006.

SENSITIVE DATA AUTHORIZATION

Recommendation 11

We recommend that the campus amend its access request process to include proper authorization from the campus president or vice president for business and finance.

Campus Response

We concur. The form that is used for access request will be modified to include a place for the approval of the VP for Business and Finance. The revised form will be submitted by January 2006.

DISASTER RECOVERY PLAN

Recommendation 12

We recommend that the campus update its disaster recovery plan to reflect the existing environment.

Campus Response

We concur. We are in the process of setting up a cold site for disaster recovery and will update the plan as soon as the implementation is complete. The updated plan will be submitted by February 2006.

INFORMATION SECURITY PROCEDURES

Recommendation 13

We recommend that the campus create a campus wide information security process, including policies and procedures for copying sensitive information, and assign an individual to ensure appropriate security practices on a campus wide basis. One method to ensure campus wide participation in information security practices would be the establishment of an interdepartmental executive council with responsibility and authority to address information security issues, in conjunction with a campus wide working committee to oversee security implementation and monitoring.

Campus Response

We concur. The campus has developed security incident reporting guidelines and a Network Security Practices document. These will be submitted to various affected campus committees and implemented by March 2006. The system-wide ISO group has drafted policies and procedures for records and information retention, information security roles and responsibilities and

protected information classification level guidelines. The CIO currently serves as the ISO and attends the system wide meetings. We will use these policies as models and finalize campus procedures. We also hope to have an individual in place by the end of the fiscal year 2005-06 responsible for monitoring that appropriate security practices on campus are in place. The policies and procedures for information security practices will be in place by June 2006.

TRUST FUNDS

Recommendation 14

We recommend that the campus strengthen procedures to ensure that trust fund expenditures are properly authorized.

Campus Response

We concur. The campus is strengthening procedures governing trust accounts to ensure expenditures are reviewed for an appropriate authorizing signature. New procedures will be implemented by January 2006.

PEOPLESOFT IMPLEMENTATION

RECONCILIATIONS

Recommendation 15

We recommend that the campus strengthen procedures to ensure that all reconciliations are prepared in a timely and complete manner.

Campus Response

We concur. Reconciliations temporarily were not prepared in a timely manner following the initial implementation of CMS/PeopleSoft Financials. All reconciliations are now being completed on a timely basis. Samples of completed reconciliations will be sent by January 2006.

LONG-OUTSTANDING CHECKS

Recommendation 16

We recommend that the campus promptly process the noted long-outstanding checks and establish procedures to ensure that future long-outstanding checks are processed in a timely manner.

Campus Response

We concur. The campus is currently processing all long-outstanding checks. This procedure temporarily was not completed for several months due to the staffing resources required to complete the CMS/PeopleSoft Financials implementation. Long-outstanding checks will be processed at least on a quarterly basis. Established procedures and evidence of current processing of long-outstanding checks will be sent by January 2006.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR



BAKERSFIELD

December 2, 2005

CHANNEL ISLANDS

CHICO

DOMINGUEZ HILLS

MEMORANDUM

EAST BAY

FRESNO

TO: Mr. Larry Mandel
University Auditor

FULLERTON

FROM: Charles B. Reed
Chancellor

HUMBOLDT

LONG BEACH

SUBJECT: Draft Final Report Number 05-04 on *FISMA*,
California State University, Stanislaus

LOS ANGELES

MARITIME ACADEMY

MONTEREY BAY

In response to your memorandum of December 2, 2005, I accept the response as submitted with the draft final report on *FISMA*, California State University, Stanislaus.

NORTHBRIDGE

POMONA

SACRAMENTO

CBR/jt

SAN BERNARDINO

Enclosure

SAN DIEGO

cc: Dr. Hamid Shirvani, President

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS