

FISMA
SAN JOSÉ STATE UNIVERSITY

Audit Report 06-11
May 18, 2007

Members, Committee on Audit

Raymond W. Holdsworth, Chair
Kenneth Fong, Vice Chair
Herbert L. Carter George G. Gowgani
Melinda Guzman William Hauck
Ricardo Icaza Glen O. Toney

Staff

University Auditor: Larry Mandel
Senior Director: Janice Mirza
IS Audit Manager: Greg Dove
Senior Auditor: Gary Miller

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction.....	5
Purpose	5
Scope and Methodology	5

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Cash Receipts.....	7
Satellite Cashiering.....	7
Fee Reconciliations	9
Accounts Receivable.....	10
Cost Allocation Plan.....	10
Delinquent Accounts	11
Purchasing.....	12
Operating Fund	13
Cash Disbursements.....	14
Check Endorsements	14
Vendor Data Records	15
Vendor Master File.....	15
Bank and SCO Account Reconciliations.....	16
Payroll and Personnel	17
Employment Eligibility Verification.....	17
Employee Separation.....	17
Employee Leave Accounting	18
Fixed Assets.....	20
Home Use Permits	20
Property Disposition.....	21
Equipment Inventory	24
Stolen Equipment Assets.....	26
Fiscal Information Technology.....	27
Information Security Organization.....	27
Information Security Procedures.....	28
Desktop Patch Management and Anti-Virus Updates	29
Network Security.....	30
E-mail Management	31
Password Security	32

CONTENTS

Sensitive Data Authorization..... 32

Trust Funds 33

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
CSU	California State University
EO	Executive Order
FISMA	Financial Integrity and State Manager's Accountability Act
FY	Fiscal Year
GAAP	Generally Accepted Accounting Principles
HR	Human Resources
PPSD	Division of Personnel/Payroll Services
SAM	State Administrative Manual
SB	Senate Bill
SCO	State Controller's Office
SJSU	San José State University
SUAM	State University Administrative Manual
TEC	Travel Expense Claim
UPD	University Police Department

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.

San José State University (SJSU) 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 SJSU campus from January 2, 2007, through February 23, 2007, and made a study and evaluation of the accounting and administrative control in effect as of February 23, 2007. This report represents our biennial review.

Our study and evaluation revealed certain conditions that, in our opinion, could result in significant 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, cash disbursements, payroll and personnel, fixed assets, fiscal information technology, and trust funds. 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, SJSU's accounting and administrative control in effect as of February 23, 2007, taken as a whole, was not 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 two of the three satellite cashiering areas visited. At the university police department, parking permit inventories were not reconciled by permit number at the end of each term, permits sold were not reconciled to revenues collected, cash drawers were not counted in between shift changes, and monthly reconciliations were not adequately performed for funds receipted into the T2 PowerPark system. At the student health center, the annual physical count of pharmacy inventory was not reconciled to the perpetual inventory records in order to identify variances and account for any missing inventory. In addition, application and state university fee reconciliations were not always timely prepared or complete.

ACCOUNTS RECEIVABLE [10]

The campus cost allocation plan did not receive an official written review that was signed and dated by the chief financial officer. In addition, the pursuit of delinquent accounts receivable needed improvement. A review of nine delinquent separated employee accounts receivable as of December 31, 2006, disclosed that adequate and timely collection activity had not been performed in eight instances. Further, personnel action request forms were not submitted to the State Controller's Office (SCO) in order to flag the employees' debts in the event of returning to state service at another agency.

PURCHASING [12]

Open purchase orders were not always timely investigated and resolved. A review of the open purchase order report as of November 30, 2006, disclosed ten open purchase orders from 2004 and 2005 with unspent encumbrances totaling \$60,914 and no activity in 2006.

OPERATING FUND [13]

Travel advances were not always recovered in a timely manner. A review of ten travel advances disclosed that four travel expense claims submitted to substantiate travel advances were not completed within 60 days of the employee's end travel date. Instead, these four travel advances were cleared from 74 to 115 days beyond the employees' end travel dates and timely follow-up was not conducted in order to recover the travel advances within 60 days.

CASH DISBURSEMENTS [14]

Checks over \$15,000 were not properly reviewed and signed. Checks over \$15,000 were automatically signed with two authorized facsimile signatures within the PeopleSoft check printing functionally without any manual review by the second authorized signatory. The campus only required manual review/approval and signatures for direct vendor pay requests exceeding \$50,000. Vendor data forms were not always maintained on file. A review of 25 disbursements disclosed that a vendor data form (STD. 204) was not on file for five vendors that had received payment. Further, access to the vendor master file was not adequately segregated from individuals responsible for processing payments. Two individuals had the ability to process payments as well as update the vendor master file within PeopleSoft. Lastly, bank and SCO account reconciliations were not completed since July 2006. This is a repeat finding from the prior FISMA audit.

PAYROLL AND PERSONNEL [17]

Federal Form I-9, Employment Eligibility Verification, was not always timely completed. This is a repeat finding from the prior FISMA audit. A review of ten new hire transactions disclosed that in six instances, the campus completed employment eligibility verification from 9 to 35 days following the effective hire date instead of the required three days. Additionally, one I-9 form could not be located. Separation clearance forms were not always completed for separating employees. A review of ten employee separations disclosed that separation clearance forms were not completed in three instances. Further, vacation leave balances and adjustments were not always adequately controlled. A review of 124 employee year-end accrued vacation leave balances as of December 31, 2005, that required adjustments at January 1, 2006, disclosed that accrued vacation leave balances for 18 employees exceeded the maximum allowable accrual by 1 hour to 84 hours, but were not adjusted as required in January 2006. Additionally, one vacation leave balance that exceeded the maximum allowable accrual by 9.6 hours was incorrectly adjusted by 17.6 hours in January 2006.

FIXED ASSETS [20]

Home use permits were not completed and approved for off-campus use of university equipment. A review of 17 laptop computers utilized by multiple departments on campus disclosed that home use permits were not completed for any of the seven laptops still in active use. The disposition of property assets was not always properly controlled. Property survey reports were not always completed for the disposition of fixed assets, the sale of property assets was not always appropriate or adequately controlled, and documentation was not available to prove that salvaged assets were actually delivered to the facilities, development and operations department for disposition. In addition, the campus physical inventory count was not timely completed, and accountability for sensitive equipment assets valued less than \$5,000 needed improvement. It was noted that 171 assets valued at \$3,230,646 had not been physically counted since October 2003 or before, and the campus could not identify the total inventory of laptop computers on campus. Further, stolen and lost equipment assets were not always adequately controlled. A review of 11 laptop computers reported as stolen in October 2006 disclosed that the investigation of personal confidential information that might be contained on the stolen computers was not performed.

FISCAL INFORMATION TECHNOLOGY [27]

The campus information security organization was deficient. There was no information security plan or consistent oversight of the information security process; and no individual assigned to ensure that appropriate security practices were being applied to all systems attached to the campus network. The information security process did not address all issues needed to provide security over the campus systems and network. For example, there was no comprehensive plan for addressing all security needs or documented time frames for completing known projects and ensuring accountability, a project to identify all sensitive data had not been performed, not all incident response activities were required to be reported, and user departments had not been required to identify all locations of sensitive data. The campus did not have a reliable process for providing desktop software patch management or ensuring installation of anti-virus definitions. Campus network ports did not always require server authentication, departmental network server domains did not always enforce proper authentication, and there was no provision to ensure that unpatched computers could not access core network services. In addition, the campus had not established policies and procedures for managing the multiple e-mail systems in use. Further, passwords were not required to be changed at regular time intervals, password syntax constraints were not consistently implemented, and the process for granting system access to sensitive data did not include obtaining proper authorization from the campus president or vice president of administration and finance.

TRUST FUNDS [33]

Trust fund agreements were not always maintained current, and trust fund balances were not always adequately controlled. Four of the ten trust fund agreements reviewed had expiration dates from March 1, 2005, to October 7, 2006. In addition, one trust fund agreement was not on file, but was completed during the audit. Further, six of these ten trust fund accounts had negative balances at June 30, 2006, ranging from \$1,395 to \$91,991.

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.
- ▶ 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 2005/06 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 2006 to November 2006. 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 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 February 23, 2007. 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

SATELLITE CASHIERING

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

The satellite cashiering locations reviewed included the university police department (UPD), university housing services, and the student health center.

University Police Department

- ▶ Parking permit inventories were not reconciled by permit number at the end of each term. In addition, permits sold were not reconciled to revenues collected.
- ▶ Cash drawers were not counted in between shift changes for the student assistant workers.
- ▶ Monthly reconciliations were not adequately performed for funds receipted into the T2 PowerPark system to the parking citation and permits revenue recorded into the TouchNet subsidiary cashiering system or to the PeopleSoft general ledger.

State Administrative Manual (SAM) §7920 states that each agency is responsible for completing any reconciliation necessary to safeguard assets and ensure reliable financial data.

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.

SAM §7901 states that the accuracy of an agency's accounting records may be proved partially by making certain reconciliations and verifications and requires monthly preparation of all reconciliations within 30 days of the preceding month.

The UPD support services lieutenant stated that parking permit reconciliations were not completed due to uncertainty of the best way to reconcile the various types of permits. He added that not counting cash drawers between shift changes was due to oversight, and the revenue reconciliations were not completed due to limited staffing and an uncertainty of UPD accounting responsibilities.

Student Health Center

The annual physical count of pharmacy inventory was not reconciled to the perpetual inventory records in order to identify variances and account for any missing inventory.

Executive Order (EO) 943, *Policy on University Health Services*, dated April 28, 2005, states that procedures must be developed for inventory control and regular removal of outdated, deteriorated, or recalled medications.

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

The director of the student health center stated that inventory reconciliation was not completed because this requirement had not been known or requested by campus administration.

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

Recommendation 1

We recommend that the campus:

- a. Prepare documented reconciliations of UPD parking permit inventories by permit number at the end of each academic term and reconcile permits sold to revenues collected at UPD.
- b. Ensure that cash drawers are counted in between employee shifts in order to localize accountability for cash receipts.
- c. Prepare documented reconciliations to TouchNet and PeopleSoft for parking citation and permit revenues collected/recorded into the T2 PowerPark system.
- d. Reconcile the annual physical count of pharmacy inventory to perpetual inventory records, including identification and resolution of variances.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will:

- a. Prepare documented reconciliations of UPD parking permit inventories by permit number at the end of each academic term and reconcile permits sold to revenues collected at UPD.
- b. Ensure that cash drawers are counted in between employee shifts.
- c. Prepare documented reconciliations to TouchNet and PeopleSoft for parking citation and permit revenues collected/recorded into the T2 PowerPark system.

- d. Reconcile the annual physical count of pharmacy inventory to perpetual inventory records, including identification and resolution of variances.

FEE RECONCILIATIONS

Application and state university fee reconciliations were not always timely prepared or complete.

Our review of reconciliations for the spring 2005 to fall 2006 terms disclosed that:

- ▶ Application fees were not reconciled during this time frame.
- ▶ While the campus had completed state university fee reconciliations for the fall, spring, and summer academic terms of the 2005/06 fiscal year (FY) in preparation of the GAAP financial statements, the reconciliations were not timely or properly completed (not signed and dated by preparer and reviewer) for the spring 2005 to fall 2006 terms. In addition, the campus completed a reconciliation of the state university fees for the fall 2006 term during the audit. This is a repeat finding from the prior Financial Integrity and State Manager's Accountability Act (FISMA) audit.

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

SUAM §3825.02 states that a reconciliation of state university fees to census date report relative to the number of students accounted on the census date shall be prepared for each academic term. The reconciliation shall be maintained on file by each campus.

The associate vice president of administration and finance stated that application fee reconciliations were not completed because of the complexity of the fee distribution by the California State University (CSU) Mentor application system. He further stated that state university fee reconciliations were not done timely because the campus considered this process to be unnecessary since PeopleSoft system controls should ensure the accurate calculation of fees.

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

Recommendation 2

We recommend that the campus strengthen procedures to ensure that application and state university fee reconciliations are formalized, signed and dated by both preparer and reviewer, and that future reconciliations are timely prepared.

Campus Response

We concur. We will complete compliance action by the end of October 2007. We will strengthen procedures to ensure that application and state university fee reconciliations are formalized, signed and dated by both preparer and reviewer, and that future reconciliations are timely prepared.

ACCOUNTS RECEIVABLE

COST ALLOCATION PLAN

The campus cost allocation plan did not receive an official written review that was signed and dated by the chief financial officer (CFO).

EO 753, *Allocation of Costs to Auxiliary Enterprises*, dated July 28, 2000, states that auxiliary enterprises shall be charged the allowable direct costs plus and allocable portion of indirect costs associated with facilities, goods, and services provided by the university funded from the General Fund. Costs allocations shall be determined in accordance with a written cost allocation plan approved annually by the campus CFO.

The director of internal control stated that the campus had not changed the cost allocation plan since FY 2004/05 because the ratios had not changed in any significant way, and the existing plan was therefore deemed acceptable by the campus and CFO. He added that the lack of CFO approval was due to oversight, but the annual reviews were being done by the CFO ad hoc.

The absence of an approved cost allocation plan increases the risk that the campus General Fund is not fully compensated for support provided to auxiliary enterprises.

Recommendation 3

We recommend that the campus annually update its cost allocation plan or document the decision not to update the plan, including CFO approval in advance of each fiscal year.

Campus Response

We concur. We will complete compliance action by the end of August 2007. We will annually update the cost allocation plan or document the decision not to update the plan, with formal CFO approval in advance of each fiscal year.

DELINQUENT ACCOUNTS

Pursuit of delinquent accounts receivable needed improvement.

Our review of nine delinquent separated employee accounts receivable as of December 31, 2006, disclosed that adequate and timely collection activity had not been performed in eight instances. Further, personnel action request forms were not submitted to the State Controller's Office (SCO) in order to flag the employees' debts in the event of returning to state service at another agency. It should be noted that four of these accounts were eventually submitted for recovery by tax offset or to an external collection agency.

SAM §8593.3 states that state agencies will request the SCO Division of Personnel/Payroll Services (PPSD) to flag its records to notify the agency if a separated employee returns to state service if after three months from date of separation, the agency is unable to collect the amount owed and the employee is not precluded reentry to state service. Requests will be made by submitting a personnel action request form, STD 680-A, prepared in accordance with instructions contained in the payroll procedures manual, maintained by the SCO PPSD. The SCO PPSD will notify the agency of the date the employee returns to state service, the name of the employing agency, and the location of employment. Upon receipt of this information the agency will take necessary action to recover amounts owed it.

SAM §8776.6 and §8776.7 provide collection procedures to be employed in the collection of amounts due from employees.

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, utilization of the offset claim procedures for accounts greater than \$10.

The manager of collections stated that collection activity inadequacies for the terminated employee accounts were due to misunderstandings between human resources and the collections department.

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

Recommendation 4

We recommend that the campus:

- a. Enhance communications between human resources and the collections department in order to identify employee accounts receivable and initiate a more timely collection process.
- b. Establish procedures to request that the SCO PPSD flag its records to notify the campus if a separated employee returns to state service.

Campus Response

We concur. We will complete compliance action by the end of September 2007. We will:

- a. Enhance communications between human resources and the collections department in order to identify employee accounts receivable and initiate a more timely collection process.
- b. Establish procedures to request that the SCO PPSD flag its records to notify the campus if a separated employee returns to state service.

PURCHASING

Open purchase orders were not always timely investigated and resolved.

Our review of the open purchase order report as of November 30, 2006, disclosed ten open purchase orders from 2004 and 2005 with unspent encumbrances totaling \$60,914 and no activity in 2006.

SAM §8340 states that as expenditures are recorded on claims, amounts will be posted to reduce the related encumbrance amount. For partial orders, many automated systems will liquidate the encumbrance for the same amount as the expenditure. However, if it is determined that encumbrance amounts are materially misstated, either over or underestimated, adjustments will be recorded to more accurately reflect the expected expenditure. The encumbrance is fully liquidated when the order is fully satisfied. Estimated decreases will be recorded as a minus amount. This will decrease the unliquidated encumbrance amount and increase the unencumbered balance.

SAM §8422.20 states the agency shall develop procedures to follow-up on open purchase documents/contracts to determine whether all goods and services ordered are actually received.

The director of procurement and support services stated that these outstanding purchase orders were not closed due to a timing difference from the November 30, 2006, report and subsequent handling and closing of the orders in December 2006 in accordance with campus procedures for the annual year-end research of open purchase orders. She added that some older non-General Fund purchase orders had remained open because in prior years only General Fund purchase orders were researched. She further stated that a policy change in December 2006 now included all open purchase orders regardless of funding source.

Failure to investigate and resolve long-outstanding encumbered purchase orders could impair budget analysis and planning and result in less than optimal decision-making.

Recommendation 5

We recommend that the campus strengthen monitoring procedures to ensure that open purchase orders are processed or otherwise timely resolved.

Campus Response

We concur. We will complete compliance action by the end of August 2007. We will strengthen monitoring procedures to ensure that open purchase orders are processed or otherwise timely resolved.

OPERATING FUND

Travel advances were not always recovered in a timely manner.

Our review of ten travel advances issued between February 2006 and October 2006 disclosed that four travel expense claims (TEC) submitted to substantiate travel advances were not completed within 60 days of the employee's end travel date. Instead, these four travel advances were cleared from 74 to 115 days beyond the employees' end travel dates and timely follow-up was not conducted in order to recover the travel advances within 60 days. Although the campus had conducted some follow-up with the employees, it was never before the 60 days after travel had ended.

CSU directive HR 2006-25, *CSU Policy and Procedures Governing Travel and Relocation Expense Reimbursement*, dated December 18, 2006, states, in part, that the TEC must be submitted within a reasonable period of time not to exceed 60 days. If the advance exceeds the substantiated expenses, the employee must submit a check or money order with the TEC to return the excess advance no more than 120 days after the expense is paid or incurred. If an employee does not substantiate and return any excess advances, if applicable, that amount will be deducted from the next payroll. Prior superseded directives included the aforementioned requirements.

SAM §8116.2 and §8116.3 require campuses to perform follow-up activity on outstanding travel advances and to deduct uncollected advances from an employee's payroll warrant. A periodic statement must be sent no less frequently than bi-monthly to notify employees who have travel advances, but have not submitted a TEC to substantiate the travel expenses and/or have not returned any excess travel advance amount.

The director of procurement and support services stated that the campus lost track of these outstanding travel claims due to oversight.

Insufficient control over travel advances increases the risk that operating fund monies may not be available and reduces the likelihood of collection.

Recommendation 6

We recommend that the campus strengthen procedures to improve the timely recovery of travel advances.

Campus Response

We concur. We will complete compliance action by the end of August 2007. We will strengthen procedures to improve the timely recovery of travel advances.

CASH DISBURSEMENTS

CHECK ENDORSEMENTS

Checks over \$15,000 were not properly reviewed and signed.

Checks over \$15,000 were automatically signed with two authorized facsimile signatures within the PeopleSoft check printing functionality without any manual review by the second authorized signatory. The campus only required manual review/approval and signatures for direct vendor pay requests exceeding \$50,000.

SAM §8041 states that any check drawn in excess of \$15,000 will require two authorized signatures unless it is payable to: (1) the State Treasurer, (2) another state agency or account, or (3) if the Department of Finance, Fiscal Systems and Consulting Unit, has authorized, in writing, special instructions permitting an agency to deviate from this requirement. All other checks will require only one authorized signature. Sound business practice mandates that the second authorized signature on checks exceeding \$15,000 be a manual signature to permit review by that signatory.

The director of accounting and financial systems stated that the campus had not considered the impact of the automatic dual signatures for checks in excess of \$15,000 and had considered the practice of dual review of checks less than \$50,000 to be burdensome due to the high volume of checks.

Failure to provide manual review and signature by a second authorized signatory for checks exceeding \$15,000 increases the risk of loss due to improper payments.

Recommendation 7

We recommend that the campus update disbursement system functionality to require the manual review and signature of a second authorized signatory for all checks in excess of \$15,000.

Campus Response

We concur. We will complete compliance action by the end of October 2007. We will update disbursement system functionality to require the manual review and signature of a second authorized signatory for all checks in excess of \$15,000.

VENDOR DATA RECORDS

Vendor data forms were not always maintained on file.

Our review of 25 disbursements dated between April 2006 and August 2006 disclosed that a vendor data form (STD. 204) was not on file for five vendors that had received payment.

SAM §8422.19 states that a completed STD. 204 must be obtained whenever a state agency engages in a transaction that leads to a payment to any individual or any entity that is not a governmental entity. The STD. 204 must be completed by the vendor and attached to each contract. For non-contract transactions, this form must be completed by the vendor and retained in the state agency's business services or accounting office as determined by state agency policy.

The director of procurement and support services stated that the missing forms were obtained many years ago, but had been misfiled/misplaced due to oversight.

Inadequate maintenance of vendor data forms increases the risk of inappropriate payments and may expose the campus to increased tax liability.

The campus took immediate action to contact the five vendors and obtain completed STD. 204 forms prior to the end of audit fieldwork.

VENDOR MASTER FILE

Access to the vendor master file was not adequately segregated from individuals responsible for processing payments.

Two individuals had the ability to process payments as well as update the vendor master file within PeopleSoft.

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."

The director of procurement and support services stated that the segregation of duties issue was unintentional and due to uncertainty regarding the PeopleSoft user permissions granted by each class ID, and possibly a lack of functionality within PeopleSoft to drill down and separate unwanted class IDs from the role names.

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

Recommendation 8

We recommend that the campus restrict vendor update permissions from individuals responsible for processing payments.

Campus Response

We concur. We will complete compliance action by the end of August 2007. We will restrict vendor update permissions from individuals responsible for processing payments.

BANK AND SCO ACCOUNT RECONCILIATIONS

Bank and SCO account reconciliations were not completed since July 2006. This is a repeat finding from the prior FISMA audit.

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.

SAM §8060 states that all bank and centralized State Treasury system accounts will be reconciled promptly at the end of each month.

The director of accounting and financial systems stated that these reconciliations were not completed due to conversions to new banks as a result of the revenue management plan implementation. He added that it was also due to a conversion to the TouchNet cashiering system and to staffing limitations.

Untimely bank and SCO account reconciliations limit the campus' ability to detect errors and irregularities, increase the likelihood of loss of state funds, and compromise accountability.

Recommendation 9

We recommend that the campus strengthen procedures to ensure that bank and SCO account reconciliations are prepared in a timely manner.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will strengthen procedures to ensure that bank and SCO account reconciliations are prepared in a timely manner.

PAYROLL AND PERSONNEL

EMPLOYMENT ELIGIBILITY VERIFICATION

Federal Form I-9, Employment Eligibility Verification, was not always timely completed. This is a repeat finding from the prior FISMA audit.

Our review of ten new hire transactions dated between August 2005 and September 2006 disclosed that in six instances, the campus completed employment eligibility verification from 9 to 35 days following the effective hire date instead of the required three days. Additionally, one I-9 form could not be located.

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 associate director of employee support services stated that new hires did not always complete the required documentation at the beginning of employment. He further stated the payroll services representative did not always receive timely notification of appointments, and departments did not communicate appropriately or submit paperwork in a timely manner.

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

Recommendation 10

We recommend that the campus strengthen procedures to ensure that I-9 forms are completed within three business days of the date of employment.

Campus Response

We concur. We will complete compliance action by the end of August 2007. We will strengthen procedures to ensure that I-9 forms are completed within three business days of the date of employment.

EMPLOYEE SEPARATION

Separation clearance forms were not always completed for separating employees.

Our review of ten employee separations dated between August 2005 and November 2006 disclosed that separation clearance forms were not completed in three instances.

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 associate director of employee support services stated that under certain circumstances employees were not available to complete the clearance process and that the campus had no available means to force separating employees to complete the clearance forms.

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

Recommendation 11

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

Campus Response

We concur. We will complete compliance action by the end of September 2007. We will review and strengthen employee separation procedures to ensure complete clearance documentation.

EMPLOYEE LEAVE ACCOUNTING

Vacation leave balances and adjustments were not always adequately controlled.

Our review of 124 employee year-end accrued vacation leave balances as of December 31, 2005, that required adjustment at January 1, 2006, disclosed that:

- ▶ Accrued vacation leave balances for 18 employees exceeded the maximum allowable accrual by 1 hour to 84 hours, but were not adjusted as required in January 2006.
- ▶ One vacation leave balance that exceeded the maximum allowable accrual by 9.6 hours was incorrectly adjusted by 17.6 hours in January 2006.

Article 34.6 of the California Faculty Association Collective Bargaining Agreement states that credits are cumulative to a maximum of 320 working hours for ten or less years of qualifying service or 440 working hours for more than ten years of such service. Accumulations in excess of this amount as of January 1 of each year shall be forfeited by the faculty unit employee.

Section 42909, Article 4, Subchapter 7, Chapter 1, Division 5 of Title 5 of the California Code of Regulations states as follows:

- (a) An employee may accumulate credit for vacation with pay for which vacation is not taken during the calendar year. On January 1st of any calendar year, an employee covered by

Section 42902 shall not have a credit for vacation with pay of more than 384 hours; an employee covered by Section 42904 shall not have a credit of more than 272 working hours for 10 or less years of qualifying service or 384 working hours for more than 10 years of such service; a Management Personnel Plan employee shall not have a credit of more than 384 working hours for 10 or less years of qualifying service or 440 working hours for more than 10 years of such service; and a campus president, general counsel, vice chancellor, or chancellor shall not have a credit of more than 480 hours.

(b) Notwithstanding subsection (a) to the contrary, the president of a campus at which an employee is employed, or the chancellor in the case of all other employees, may permit an employee to carry over more vacation credits than the prescribed maximum when the employee was prevented from taking enough vacation to reduce the credits because the employee (1) was required to work as a result of fire, flood or other similar emergency, (2) was prevented from taking vacation by work the president or the chancellor, as the case may be, has determined to be of a priority or critical nature over an extended period of time, (3) was absent on full salary for compensable injury, or (4) was prevented by campus rule from taking vacation until December and at that time was unable to take vacation because of illness requiring use of sick leave.

The associate director of employee support services stated that the campus was unaware that only presidential approval was permitted for leave carry over. He added that the year-end leave adjustment errors were due to oversight and manual calculation errors.

Failure to maintain accrued vacation leave balances within prescribed maximums and incorrectly adjust balances results in over/under compensation of employees and exposes the campus to increased liability.

Recommendation 12

We recommend that the campus establish procedures to ensure the appropriate maintenance and adjustment of vacation leave balances in excess of allowable maximum accruals.

Campus Response

We concur. We will complete compliance action by the end of October 2007. We will establish procedures to ensure the appropriate maintenance and adjustment of vacation leave balances in excess of allowable maximum accruals.

FIXED ASSETS

HOME USE PERMITS

Home use permits were not completed and approved for off-campus use of university equipment.

Our review of 17 laptop computers utilized by multiple departments on campus disclosed that home use permits were not completed for any of the seven laptops still in active use.

The San José State University (SJSU) *Take Home Computer Use Policy* states that employees who perform work at home are authorized to take home SJSU computers. These computers are the property of SJSU and will be used solely for work. In order to take home a computer, the employee must complete a form that specifies the machine type, serial number, and intended usage of the computer. A copy of the form will be sent to administrative technology to allow the computer transfer to be tracked in the division of administration and finance's IntelliTrack database, and another copy of the form will be kept on file by the employee's supervisor. Upon termination of employment, the supervisor will be responsible for ensuring the return of the computer and related peripherals to the university. When equipment is returned, administrative technology will be notified. The supervisor will tell administrative technology what the disposition of the equipment will be to ensure that the computerized inventory is accurate and complete.

EO 649, *Safeguarding State Property*, dated February 15, 1996, delegates authority to each campus president to establish and maintain a system of internal controls to safeguard state property.

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.

The director of accounting and financial systems stated that the lack of completed home use permits was due to non-compliance with campus policy by departmental units.

Insufficient control over property increases the risk of misstated property records and theft, loss, or unauthorized use of state property.

Recommendation 13

We recommend that the campus enforce adherence to procedures for utilization of home use permits for off-campus use of university equipment.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will enforce adherence to procedures for utilization of home use permits for off-campus use of university equipment.

PROPERTY DISPOSITION

The disposition of property assets was not always properly controlled.

We found that:

- ▶ Property survey reports were not always completed for the disposition of fixed assets. Property survey reports could not be found for 5 of 20 assets deleted from the IntelliTrack property database from September 2006 to November 2006. Specifically, a property survey report was not completed for four of the assets, and although the other asset was listed on a property survey report, the property survey report had not been approved by the property survey board. In addition, documentation was not available to prove that these salvaged assets were actually delivered to the facilities, development and operations department for disposition.
- ▶ The sale of property assets was not always appropriate or adequately controlled. Our review of ten assets listed on the 2006 revolving equipment inventory disclosed that one asset in the custody of the materials engineering department had been improperly sold via a third-party online auction house (Dove Bid, Inc.) in August 2006. The following exceptions were noted:
 - The sale had not been approved by the property survey board and the asset sold, as well as 38 other assets sold, had not been removed from the inventory records since being inventoried by the property office in July 2006 (prior to sale).
 - The disposition of surplus equipment via third-party auction was not adequately supported by a contract with the auction house, Dove Bid, Inc. The campus had not formally contracted with Dove Bid, Inc. to ensure that the campus was held harmless of liability for the quality of the surplus equipment.
 - The campus also lacked documentation, which stated agreed upon details for payment, merchandise shipment, and the return of unsold equipment. While 69 total assets were placed for sale on the auction site, only 39 assets were sold. During the audit, it could not be determined how many of these assets should have been removed from the inventory records and the disposition of the unsold assets was also unknown.
 - The sale of these 39 assets netted \$20,556, but only \$13,052 was remitted to the campus by Dove Bid, Inc. During the audit, the campus could not provide the reason for the \$7,504 disparity between the total sale price and the amount remitted to the campus. Furthermore,

the funds from the sale of these state assets (purchased with state funds) were incorrectly deposited to the SJSU Foundation.

- ▶ Documentation was not available to prove that salvaged assets were actually delivered to the facilities, development and operations department for disposition. Our review of 17 laptop computers that were utilized by multiple departments on campus disclosed that ten of the laptops were reported as salvaged and deleted from the property inventory in January 2007, however documentation was not available to support that these laptops had been delivered to the facilities, development and operations department for final disposition or that the users had gained pre-approval from the campus property survey board prior to salvaging the equipment. In addition, one laptop reported as salvaged and deleted from the property inventory had not been documented on a property survey report.

The *SJSU Property Manual* states that for capitalized property, the department should fill out the property survey report to notify the property office of dispositions. For both capitalized property and non-capitalized high-risk property, submission of the property survey report and approval by the property survey board is required before property may be removed from campus without replacement. This includes the following conditions: transferring, selling, or donating property to another state agency or certified non-profit agency; discarding, salvaging, or recycling property; releasing or reissuing property for public sale disposal methods. For all property, a detailed procedure is also required when conducting a public sale to include pre-approval from the property survey board, e-mail notice to the purchasing office for redistribution of equipment to other campus departments, and if no department has responded to the owner department within two weeks, offer the property for sale on an online auction site such as eBay. The owner department is responsible for administering the sale, depositing any sales proceeds, and retaining documentation showing that state regulations were followed. Proper separation of duties should be in place as all sales should be approved by a manager and the person who arranges the sale should not receive the proceeds. Sales proceeds must be deposited in the university fund and account out of which the property was originally purchased.

SAM §3520.2 indicates that each agency will have a duly appointed property survey board. It will be the responsibility of the board to determine that the best interest of the state is served in disposing of state property. At least two members of the property survey board will approve all property survey reports and any transfers of location of equipment.

SAM §3520.3 states that when an agency proposes to dispose of state-owned, non-expendable surplus property by sale, by trade-in, or by discarding the property, the agency prepares a property survey report. When an agency proposes to transfer such property to another agency or to a unit within the agency, the agency prepares a transfer of location of equipment form. The agency may use an agency form in lieu of the transfer of location form for intra-agency transfers between organizational units accounted for in the same general ledger account.

EO 715, *CSU Risk Management Policy*, dated October 27, 1999, states that the campus risk management policy should include methods of controlling risks. The liability exposure the campus and the CSU faces for those activities, which are linked to the mission of the CSU, can be minimized

by: transferring risk through third-party waivers, hold harmless agreements, or through vendor contracting; transferring risk through personal liability, health, travel, and life insurance; and preventing/controlling risk through training and supervision.

EO 919, *Policy Governing Non-General Fund Receipts*, dated October 15, 2004, requires, in part, that non-General Fund receipts be held in proper accounts and be administered in accordance with applicable laws and regulations.

SAM §3520.9 states that when an agency disposes of state-owned surplus personal property by means other than the sale of the property (i.e., salvaged, scrapped, discarded, or hauled to landfill) the agency's responsible employee and unit supervisor shall certify in writing that the disposition has been accomplished. The certification may be made on the property survey report or attached and filed with the form. When the agency disposes of the property at a public landfill, the agency's representative obtains the signature of the disposal site operator or attendant, indicating that the property listed was disposed of at the site. If the landfill is unattended, the agency's responsible employee and the unit supervisor shall sign and certify that the disposition described was accomplished.

The director of accounting and financial systems stated that the failure to complete property survey reports was due to oversight while the improper sale was due to a lack of compliance with campus policies by the materials engineering department. He further added that the lack of salvage confirmation was due to a lack of campus policies and procedures that required such action.

Insufficient control over property increases the risk of misstated property records and theft, loss, or unauthorized use of state property.

Recommendation 14

We recommend that the campus:

- a. Strengthen procedures to ensure that property survey reports are completed and properly filed for the disposition of fixed assets.
- b. Ensure that the sale of state assets is conducted in accordance with campus policies.
- c. Ensure that all dispositions are removed from the property ledger in a timely manner.
- d. Document contractual terms with third-party auction houses to specify agreed upon details for payment, merchandise shipment, and the return of unsold equipment.
- e. Ensure that funds received from the sale of state assets are properly receipted and deposited to General Fund accounts.
- f. Develop procedures to require that departmental custodians of salvaged equipment document the transfer of custody to the facilities, development and operations department for final disposition.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will:

- a. Strengthen procedures to ensure that property survey reports are completed and properly filed for the disposition of fixed assets.
- b. Ensure that the sale of state assets is conducted in accordance with campus policies.
- c. Ensure that all dispositions are removed from the property ledger in a timely manner.
- d. Document contractual terms with third-party auction houses to specify agreed upon details for payment, merchandise shipment, and the return of unsold equipment.
- e. Ensure that funds received from the sale of state assets are properly receipted and deposited to General Fund accounts.
- f. Develop procedures to require that departmental custodians of salvaged equipment document the transfer of custody to the facilities, development and operations department for final disposition.

EQUIPMENT INVENTORY

The campus physical inventory count was not timely completed, and accountability for sensitive equipment assets valued less than \$5,000 needed improvement.

We found that:

- ▶ 171 assets valued at \$3,230,646 had not been physically counted since October 2003 or before.
- ▶ Inventory was not adequately maintained for sensitive equipment valued less than \$5,000. For instance, as the accountability of laptop computers maintained by the many departments across campus was decentralized to each department, these laptops were not properly logged or asset tagged, and campus procedures only required that a random sample of these computers be incorporated into the revolving equipment inventory process conducted by the property office. However, documentation was not available of the random sampling of departmental inventory for equipment less than \$5,000. Furthermore, the campus could not identify the total inventory of laptop computers on campus.

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

The *SJSU Property Manual* states departments are required to keep records of high-risk equipment costing \$500 or more but less than \$5,000. High-risk property is defined as property, which poses a special risk of loss due to its marketability and portability. All computer equipment costing \$500 or

more will be considered high-risk. Individual departments will be responsible for determining whether any other property meets the definition of high-risk. Items that are permitted to be taken off campus would fit this definition. The property office will periodically inventory under-\$5,000 equipment on a sample basis. If the property office finds that a department is not keeping adequate records of under-\$5,000 equipment, it will report this to the vice president of the division to which the department belongs. The vice president will be responsible for assuring compliance with university policy.

EO 649, *Safeguarding State Property*, dated February 15, 1996, delegates authority to each campus president to establish and maintain a system of internal controls to safeguard state property ... Some state property may pose a special risk of loss due to its marketability and portability ... It is expected that an effective policy would likely include tagging and inventorying all high risk property with an acquisition cost of at least \$500.

SAM §8650 indicates that the property records for each property acquisition include date acquired, property description, property identification number, cost or other basis of valuation, owner fund, and rate of depreciation, if applicable. Property records shall include both capitalized and non-capitalized property.

SAM §8651 indicates that all state property will be tagged after acquisition.

The director of accounting and financial systems stated that inventory count insufficiency was due to limited staffing in the property management function and the emergence of alternative priorities. He added that the inadequate inventorying of sensitive equipment valued less than \$5,000 was due to non-compliance with campus policy by departmental units and by lack of centralized oversight by the property management function.

Insufficient control over fixed assets increases the risk of inappropriate activities and reduces accountability over state property.

Recommendation 15

We recommend that the campus:

- a. Perform a physical count of all property and reconcile the count with accounting records at least once every three years.
- b. Develop and maintain a property register for acquisitions of non-capitalized property valued less than \$5,000 and ensure that these assets are properly tagged and accounted for.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will:

- a. Implement a schedule to perform a physical count of all property and reconcile the count with accounting records at least once every three years.
- b. Develop and maintain a property register for acquisitions of non-capitalized property valued less than \$5,000 and ensure that these assets are properly tagged and accounted for.

STOLEN EQUIPMENT ASSETS

Stolen and lost equipment assets were not always adequately controlled.

Our review of 11 laptop computers reported as stolen in October 2006 disclosed that an investigation of personal confidential information that might be contained on the stolen computers was not performed.

The SJSU *Portable Computing Security Guidelines* require an employee to immediately report the loss or theft of a laptop containing university information, especially if that information is classified as confidential, personal, and/or proprietary. Employees must also notify their supervisor and university police as soon as possible, immediately complete the lost or stolen portable electronic device report form, and submit a copy to the information security office. If a lost, stolen, or otherwise compromised laptop contains unencrypted confidential information, the responsibility for notifying victims under SB 1386 resides with the department or division where the security breach occurred.

SAM §8643 states that agency management must promptly investigate incidents involving loss, damage, or misuse of information assets.

The director of internal control/information security officer stated that the lack of adequate investigation was due to communication breakdowns between property management, decentralized campus departments, and the information security office.

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

Recommendation 16

We recommend that the campus strengthen controls over the accountability of equipment assets and adhere to campus procedures for the investigation of personal confidential information contained on computers reported as lost or stolen.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will strengthen controls over the accountability of equipment assets and adhere to campus procedures for the investigation of personal confidential information contained on computers reported as lost or stolen.

FISCAL INFORMATION TECHNOLOGY

INFORMATION SECURITY ORGANIZATION

The campus information security organization was deficient.

There was no information security plan or consistent oversight of the information security process; and no individual was assigned to ensure that appropriate security practices were being applied to all systems attached to the campus network by all departments that individually supported their computer systems.

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 information security officer stated that security management and oversight had been divided among various groups, but that there was no individual to ensure that suggested practices were being consistently followed.

Security practices that fail to ensure campus-wide policy and compliance increase the risk of unauthorized exceptions, and could compromise compliance with statutory information security requirements thus, impacting the ability of the campus to opine on the overall effectiveness of existing security provisions related to such data.

Recommendation 17

We recommend that the campus designate one individual with oversight responsibility for campus-wide information security, including policies and procedures, training, monitoring, incident response, and reporting. An alternate method to help 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. We will complete compliance action by the end of November 2007. We will ensure campus-wide participation in information security practices via 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.

INFORMATION SECURITY PROCEDURES

The information security process did not address all issues needed to provide security over the campus systems and network.

Specifically, we noted that:

- ▶ There was no comprehensive plan for addressing all security needs or documented time frames for completing known projects and ensuring accountability.
- ▶ Project status guidelines and reporting requirements to executive management had not been established.
- ▶ A project to identify all sensitive data had not been performed.
- ▶ Not all incident response activities were required to be reported, and user departments had not been required to identify all locations of sensitive data.
- ▶ There was no consistent practice for data cleansing of discarded computers.

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

The information security officer stated that certain information security responsibilities had been assigned to the individual campus departments and that it was their duty to ensure that proper practices were followed.

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

Recommendation 18

We recommend that the campus make information security management more of a priority and allocate more resources, directives, focus, and accountability to ensure that risks are mitigated and internal controls are clearly established and implemented. Further, the campus should enhance its security plan to include all outstanding security projects, and as soon as possible, implement information security processes to ensure that appropriate security practices are in place campus-wide.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will emphasize and allocate more resources, directives, focus, and accountability to ensure that information security risks are mitigated and internal controls are clearly established and implemented. We will document our security plan to include all outstanding security projects, and implement information security processes to ensure that appropriate security practices are in place campus-wide.

DESKTOP PATCH MANAGEMENT AND ANTI-VIRUS UPDATES

The campus did not have a reliable process for providing desktop software patch management or ensuring consistent and prompt installation of anti-virus definitions on all computers.

SAM §4842.2 states that appropriate risk management procedures should be implemented to safeguard the integrity of data files, which includes effective security of computing systems. Effective security of computing systems is considered to include an appropriate method for ensuring that security patches are continually applied to all servers and desktop computers, and that virus threats are mitigated.

The senior manager of network services stated that the technology had been installed to require all computers connecting to the network to be properly patched, but that such technology had not yet been deployed on a campus-wide basis.

Failure to provide a reliable process of desktop software patch management, including updated anti-virus definitions, increases the risk of compromise to campus systems, and accordingly of fraudulent or unauthorized activities and virus threats.

Recommendation 19

We recommend that the campus expand the use of existing technologies to ensure that all computers connecting to the network are appropriately patched and anti-virus definitions maintained current. Administrator privileges to desktop computers should be disallowed to ensure that automatic system updates cannot be turned off, or regular audits should be performed and documented to ensure that the most current updates are installed on computers necessitating administrator privileges.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will expand existing technologies to ensure that all computers connecting to the network are appropriately patched and anti-virus definitions maintained current. We will implement risk-control solutions over the issue of administrator privileges to desktop computers.

NETWORK SECURITY

Campus network ports did not always require server authentication, departmental network server domains did not always enforce proper authentication, and there was no provision to ensure that unpatched computers could not access core network services.

An open network increases the risk of, and exposure to, hack attempts, non-traceable events, and user misconduct. Authentication by a network server ensures that the connected users are authorized by the campus to use network/computing resources and provides accountability for activities performed on campus systems.

SAM §20050 requires that there be a plan that limits access to state agency assets to authorized personnel who require these assets in their assigned duties.

The senior manager of network services stated that the campus was on a network controlled by decentralized login management, that different departments were responsible for individual implementation, and that network tools had recently been obtained to assist in restricting access and enforcing consistent authentication policies.

Network ports that do not require server authentication increases campus exposure to unauthorized activities by unknown individuals, while individually managed network domains could create discrepancies in security policies and system management, which could lead to unauthorized access.

Recommendation 20

We recommend that the campus:

- a. Expand the use of available technologies to force logon to the network and to prevent unpatched computers from gaining access to network resources.
- b. Reduce the number of independently managed network domains and implement technologies to ensure that security policies are enforced on a consistent basis.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will:

- a. Expand the use of available technologies to force logon to the network and to prevent unpatched computers from gaining access to network resources.
- b. Reduce the number of independently managed network domains and implement technologies to ensure that security policies are enforced on a consistent basis.

E-MAIL MANAGEMENT

The campus had not established policies and procedures for managing the multiple e-mail systems in use.

E-mail systems represent a significant threat to network environments, and proper management of such systems is essential to ensure that vulnerabilities are not allowed into the network; incidents are properly escalated; campus usage and retention guidelines are followed; and e-mail addresses are maintained in one location to facilitate campus-wide communications. Our review disclosed that the campus allowed independent e-mail systems, but did not enforce effective management over those systems.

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 senior manager of network services stated that the campus required all employees to use the centralized e-mail system, but allowed them to forward e-mail to secondary e-mail systems that were not managed or controlled by university computing, and that the campus had not yet established policies and procedures for either limiting or managing the various systems.

Inadequate management of e-mail systems increases campus susceptibility to network vulnerabilities and inappropriate document retention and may impede campus-wide communications.

Recommendation 21

We recommend that the campus:

- a. Conduct an assessment to identify e-mail systems used by the campus.
- b. Establish policies and procedures for the proper security and management of all e-mail systems.
- c. Establish monitoring and oversight to ensure that e-mail systems are properly administered.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will:

- a. Conduct an assessment to identify e-mail systems used by the campus.
- b. Establish policies and procedures for the proper security and management of all e-mail systems.
- c. Establish monitoring and oversight to ensure that e-mail systems are properly administered.

PASSWORD SECURITY

Passwords were not required to be changed at regular time intervals, and password syntax constraints were not consistently implemented.

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 senior director of administrative systems stated that some password controls that the campus did not consider to be more effective in preventing unauthorized access had not been activated.

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

Recommendation 22

We recommend that the campus amend its password controls to require that passwords be changed periodically and password syntax controls consistently implemented to ensure appropriate security of campus data.

Campus Response

We concur. We will complete compliance action by the end of November 2007. We will strengthen password controls, including the practices of periodic password change and consistent password syntax requirement.

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 administration 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 senior director of administrative systems stated that the process had previously been performed and that it was an oversight due to the change in the vice president of administration and finance.

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

Recommendation 23

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

Campus Response

We concur. We will complete compliance action by the end of September 2007. We will strengthen the access request process to include proper authorization from the campus president or vice president of administration and finance.

TRUST FUNDS

Trust fund agreements were not always maintained current, and trust fund balances were not always adequately controlled.

We found that:

- ▶ Four of the ten trust fund agreements reviewed had expiration dates from March 1, 2005, to October 7, 2006. In addition, one trust fund agreement was not on file, but was completed during the audit.
- ▶ Six of the ten trust fund accounts had negative balances at June 30, 2006, ranging from \$1,395 to \$91,991. It was noted that the campus had a procedure for charging monthly interest expense to trust accounts with negative balances, however this interest expense was charged in the same manner that earned interest for positive balances was aggregated for all trust funds and allocated only to one account. This minimized the incentive for the individual trust fund account managers to keep a positive balance since they were not kept solely accountable for their negative trust fund balances.

SAM §19440.1 states that each trust account established shall be supported by documentation as to the type of trust, donor, or source of trust monies, purpose of the trust, time constraints, persons authorized to withdraw or expend funds, specimen signatures, reporting requirements, instructions for closing the account, disposition of any unexpended balance, and restrictions on the use of monies for administrative or overhead costs.

The SJSU *Trust Fund policy* requires that trust fund agreements be renewed every three years. The policy further states that the basic approach to controlling negative cash balances in trust funds is to treat them as loans from the university and charge interest expense to the fund, at the same rate as that which we use to credit interest income to trust funds with positive cash balances. Departments are also notified of any negative cash balances to facilitate better management of their funds.

SUAM §3710.01 states that each trust project must maintain a positive cash balance and a positive fund balance.

The director of accounting and financial systems stated that trust fund agreements were not current due to oversight, and the negative balances were due to the inability to enforce department maintenance of positive cash balances.

Inadequate trust fund administration increases the risk of loss due to poor trust fund administration.

Recommendation 24

We recommend that the campus strengthen:

- a. Controls to ensure that trust fund agreements are prepared and updated to support each trust account.
- b. Campus procedures to ensure that only the specific trust funds with negative balances are charged interest.

Campus Response

We concur. We will complete compliance action by the end of September 2007. We will:

- a. Strengthen controls to ensure that trust fund agreements are prepared and updated to support each trust account.
- b. Strengthen campus procedures to ensure that only the specific trust funds with negative balances are charged interest.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Don W. Kassing	President
Rosie Alvarez	Parking Services Coordinator, University Police Department (UPD)
Marlene Anderson	Bursar
Ruben Araiza	Property Officer, Accounting and Financial Systems
Don Baker	Interim Associate Vice President, University Computing
Shawn Bibb	Associate Vice President, Administration and Finance (At time of review)
Rick Casillo	Associate Director, Employee Support Services
Yolanda Castro	Parking Services Enforcement Analyst, UPD
Amy Chan	Accounting Technician, Accounting and Financial Systems
Mike Dunefsky	Senior Director, Administrative Systems
Roger Elrod	Director, Student Health Center
Deana Gerhard Genereux	Manager, Collections
Gloria Gutierrez	Manager, Employee Support Services
Cynthia Haliasz	Director, Budget Management
Paula Hernandez	Assistant Director, Student Health Center
Tuan Ho	Accounting Technician, Accounting and Financial Systems
Bonnie King	Manager, Accounts Payable
Elaine Lee	Accountant, Accounting and Financial Systems
Rose Lee	Vice President, Administration and Finance
Norma Lorigo	Director, Procurement and Support Services
Violeta Munoz	Resident Accounts Coordinator, University Housing
Bob Neal	Senior Manager, Network Services
Linh Ong	Accountant, Accounting and Financial Systems
Rita Peth	Manager, Purchasing
Ninh Pham-Hi	Director, Internal Control/Information Security Officer
Jim Renelle	Support Services Lieutenant, UPD
Paul Siegel	Director, Accounting and Financial Systems
Marlene Trifilo	Manager, Cashiering Services
Kristy Wilce	Administration and Finance Operations Specialist, University Housing

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.



San José State
UNIVERSITY

**Office of the Vice President
for Administration and
Finance**

One Washington Square
San José, CA 95192-0006
Voice: 408-924-1500
Fax: 408-924-1515
<http://www.sjsu.edu>

RECEIVED
UNIVERSITY AUDITOR

JUN 28 2007

THE CALIFORNIA STATE
UNIVERSITY

June 27, 2007

Mr. Larry Mandel
University Auditor
The California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802

**Campus Response to FISMA AUDIT (06-11) at
San José State University**

Enclosed is San José State University's response to the FISMA Audit.
The campus is committed to addressing the issues identified in this
audit report.

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

A handwritten signature in cursive script that reads "Rose L. Lee".

ROSE L. LEE
Vice President for Administration and Finance

Enclosure

c: Don W. Kassing, President
Ninh Pham-Hi, Director, Internal Control

The California State University:

Chancellor's Office, Bakersfield, Channel
Islands, Chico, Dominguez Hills, East Bay,
Fresno, Fullerton, Humboldt, Long Beach,
Los Angeles, Maritime Academy, Monterey
Bay, Northridge, Pomona, Sacramento, San
Bernardino, San Diego, San Francisco, San
José, San Louis Obispo, San Marcos,
Sonoma, Stanislaus

FISMA
SAN JOSÉ STATE UNIVERSITY

Audit Report 06-11
May 18, 2007

CASH RECEIPTS

SATELLITE CASHIERING

Recommendation 1

We recommend that the campus:

- a. Prepare documented reconciliations of UPD parking permit inventories by permit number at the end of each academic term and reconcile permits sold to revenues collected at UPD.
- b. Ensure that cash drawers are counted in between employee shifts in order to localize accountability for cash receipts.
- c. Prepare documented reconciliations to TouchNet and PeopleSoft for parking citation and permit revenues collected/recorded into the T2 PowerPark system.
- d. Reconcile the annual physical count of pharmacy inventory to perpetual inventory records, including identification and resolution of variances.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will:

- a. Prepare documented reconciliations of UPD parking permit inventories by permit number at the end of each academic term and reconcile permits sold to revenues collected at UPD.
- b. Ensure that cash drawers are counted in between employee shifts.
- c. Prepare documented reconciliations to TouchNet and PeopleSoft for parking citation and permit revenues collected/recorded into the T2 PowerPark system.
- d. Reconcile the annual physical count of pharmacy inventory to perpetual inventory records, including identification and resolution of variances.

FEE RECONCILIATIONS

Recommendation 2

We recommend that the campus strengthen procedures to ensure that application and state university fee reconciliations are formalized, signed and dated by both preparer and reviewer, and that future reconciliations are timely prepared.

Campus Response

We concur. We will complete compliance action by end of Oct 07. We will strengthen procedures to ensure that application and state university fee reconciliations are formalized, signed and dated by both preparer and reviewer, and that future reconciliations are timely prepared.

ACCOUNTS RECEIVABLE

COST ALLOCATION PLAN

Recommendation 3

We recommend that the campus annually update its cost allocation plan or document the decision not to update the plan, including CFO approval in advance of each fiscal year.

Campus Response

We concur. We will complete compliance action by end of Aug 07. We will annually update the cost allocation plan or document the decision not to update the plan, with formal CFO approval in advance of each fiscal year.

DELINQUENT ACCOUNTS

Recommendation 4

We recommend that the campus:

- a. Enhance communications between human resources and the collections department in order to identify employee accounts receivable and initiate a more timely collection process.
- b. Establish procedures to request that the SCO PPSD flag its records to notify the campus if a separated employee returns to state service.

Campus Response

We concur. We will complete compliance action by end of Sep 07. We will:

- a. Enhance communications between human resources and the collections department in order to identify employee accounts receivable and initiate a more timely collection process.

- b. Establish procedures to request that the SCO PPSD flag its records to notify the campus if a separated employee returns to state service.

PURCHASING

Recommendation 5

We recommend that the campus strengthen monitoring procedures to ensure that open purchase orders are processed or otherwise timely resolved.

Campus Response

We concur. We will complete compliance action by end of Aug 07. We will strengthen monitoring procedures to ensure that open purchase orders are processed or otherwise timely resolved.

OPERATING FUND

Recommendation 6

We recommend that the campus strengthen procedures to improve the timely recovery of travel advances.

Campus Response

We concur. We will complete compliance action by end of Aug 07. We will strengthen procedures to improve the timely recovery of travel advances.

CASH DISBURSEMENTS

CHECK ENDORSEMENTS

Recommendation 7

We recommend that the campus update disbursement system functionality to require the manual review and signature of a second authorized signatory for all checks in excess of \$15,000.

Campus Response

We concur. We will complete compliance action by end of Oct 07. We will update disbursement system functionality to require the manual review and signature of a second authorized signatory for all checks in excess of \$15,000.

VENDOR MASTER FILE

Recommendation 8

We recommend that the campus restrict vendor update permissions from individuals responsible for processing payments.

Campus Response

We concur. We will complete compliance action by end of Aug 07. We will restrict vendor update permissions from individuals responsible for processing payments.

BANK AND SCO ACCOUNT RECONCILIATIONS

Recommendation 9

We recommend that the campus strengthen procedures to ensure that bank and SCO account reconciliations are prepared in a timely manner.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will strengthen procedures to ensure that bank and SCO account reconciliations are prepared in a timely manner.

PAYROLL AND PERSONNEL

EMPLOYMENT ELIGIBILITY VERIFICATION

Recommendation 10

We recommend that the campus strengthen procedures to ensure that I-9 forms are completed within three business days of the date of employment.

Campus Response

We concur. We will complete compliance action by end of Aug 07. We will strengthen procedures to ensure that I-9 forms are completed within three business days of the date of employment.

EMPLOYEE SEPARATION

Recommendation 11

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

Campus Response

We concur. We will complete compliance action by end of Sep 07. We will review and strengthen employee separation procedures to ensure complete clearance documentation.

EMPLOYEE LEAVE ACCOUNTING**Recommendation 12**

We recommend that the campus establish procedures to ensure the appropriate maintenance and adjustment of vacation leave balances in excess of allowable maximum accruals.

Campus Response

We concur. We will complete compliance action by end of Oct 07. We will establish procedures to ensure the appropriate maintenance and adjustment of vacation leave balances in excess of allowable maximum accruals.

FIXED ASSETS**HOME USE PERMITS****Recommendation 13**

We recommend that the campus enforce adherence to procedures for utilization of home use permits for off-campus use of university equipment.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will enforce adherence to procedures for utilization of home use permits for off-campus use of university equipment.

PROPERTY DISPOSITION**Recommendation 14**

We recommend that the campus:

- a. Strengthen procedures to ensure that property survey reports are completed and properly filed for the disposition of fixed assets.
- b. Ensure that the sale of state assets is conducted in accordance with campus policies.
- c. Ensure that all dispositions are removed from the property ledger in a timely manner.
- d. Document contractual terms with third-party auction houses to specify agreed upon details for payment, merchandise shipment, and the return of unsold equipment.

- e. Ensure that funds received from the sale of state assets are properly receipted and deposited to General Fund accounts.
- f. Develop procedures to require that departmental custodians of salvaged equipment document the transfer of custody to the facilities, development and operations department for final disposition.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will:

- a. Strengthen procedures to ensure that property survey reports are completed and properly filed for the disposition of fixed assets.
- b. Ensure that the sale of state assets is conducted in accordance with campus policies.
- c. Ensure that all dispositions are removed from the property ledger in a timely manner.
- d. Document contractual terms with third-party auction houses to specify agreed upon details for payment, merchandise shipment, and the return of unsold equipment.
- e. Ensure that funds received from the sale of state assets are properly receipted and deposited to General Fund accounts.
- f. Develop procedures to require that departmental custodians of salvaged equipment document the transfer of custody to the facilities, development and operations department for final disposition.

EQUIPMENT INVENTORY

Recommendation 15

We recommend that the campus:

- a. Perform a physical count of all property and reconcile the count with accounting records at least once every three years.
- b. Develop and maintain a property register for acquisitions of non-capitalized property valued less than \$5,000 and ensure that these assets are properly tagged and accounted for.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will:

- a. Implement schedule to perform a physical count of all property and reconcile the count with accounting records at least once every three years.
- b. Develop and maintain a property register for acquisitions of non-capitalized property valued less than \$5,000 and ensure that these assets are properly tagged and accounted for.

STOLEN EQUIPMENT ASSETS

Recommendation 16

We recommend that the campus strengthen controls over the accountability of equipment assets and adhere to campus procedures for the investigation of personal confidential information contained on computers reported as lost or stolen.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will strengthen controls over the accountability of equipment assets and adhere to campus procedures for the investigation of personal confidential information contained on computers reported as lost or stolen.

FISCAL INFORMATION TECHNOLOGY

INFORMATION SECURITY ORGANIZATION

Recommendation 17

We recommend that the campus designate one individual with oversight responsibility for campus-wide information security, including policies and procedures, training, monitoring, incident response, and reporting. An alternate method to help 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. We will complete compliance action by end of Nov 07. We will ensure campuswide participation in information security practices via 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.

INFORMATION SECURITY PROCEDURES

Recommendation 18

We recommend that the campus make information security management more of a priority and allocate more resources, directives, focus, and accountability to ensure that risks are mitigated and internal controls are clearly established and implemented. Further, the campus should enhance its security plan to include all outstanding security projects, and as soon as possible, implement information security processes to ensure that appropriate security practices are in place campus-wide.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will emphasize and allocate more resources, directives, focus, and accountability to ensure that information security risks are

mitigated and internal controls are clearly established and implemented. We will document our security plan to include all outstanding security projects, and implement information security processes to ensure that appropriate security practices are in place campus-wide.

DESKTOP PATCH MANAGEMENT AND ANTI-VIRUS UPDATES

Recommendation 19

We recommend that the campus expand the use of existing technologies to ensure that all computers connecting to the network are appropriately patched and anti-virus definitions maintained current. Administrator privileges to desktop computers should be disallowed to ensure that automatic system updates cannot be turned off, or regular audits should be performed and documented to ensure that the most current updates are installed on computers necessitating administrator privileges.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will expand existing technologies to ensure that all computers connecting to the network are appropriately patched and anti-virus definitions maintained current. We will implement risk-control solutions over the issue of Administrator privileges to desktop computers.

NETWORK SECURITY

Recommendation 20

We recommend that the campus:

- a. Expand the use of available technologies to force logon to the network and to prevent unpatched computers from gaining access to network resources.
- b. Reduce the number of independently managed network domains and implement technologies to ensure that security policies are enforced on a consistent basis.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will:

- a. Expand the use of available technologies to force logon to the network and to prevent unpatched computers from gaining access to network resources.
- b. Reduce the number of independently managed network domains and implement technologies to ensure that security policies are enforced on a consistent basis.

E-MAIL MANAGEMENT

Recommendation 21

We recommend that the campus:

- a. Conduct an assessment to identify e-mail systems used by the campus.
- b. Establish policies and procedures for the proper security and management of all e-mail systems.
- c. Establish monitoring and oversight to ensure that e-mail systems are properly administered.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will:

- a. Conduct an assessment to identify e-mail systems used by the campus.
- b. Establish policies and procedures for the proper security and management of all e-mail systems.
- c. Establish monitoring and oversight to ensure that e-mail systems are properly administered.

PASSWORD SECURITY

Recommendation 22

We recommend that the campus amend its password controls to require that passwords be changed periodically and password syntax controls consistently implemented to ensure appropriate security of campus data.

Campus Response

We concur. We will complete compliance action by end of Nov 07. We will strengthen password controls, including the practices of periodic password change and consistent password syntax requirement.

SENSITIVE DATA AUTHORIZATION

Recommendation 23

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

Campus Response

We concur. We will complete compliance action by end of Sep 07. We will strengthen the access request process to include proper authorization from the campus president or vice president of administrative systems and finance.

TRUST FUNDS

Recommendation 24

We recommend that the campus strengthen:

- a. Controls to ensure that trust fund agreements are prepared and updated to support each trust account.
- b. Campus procedures to ensure that only the specific trust funds with negative balances are charged interest.

Campus Response

We concur. We will complete compliance action by end of Sep 07. We will:

- a. Strengthen controls to ensure that trust fund agreements are prepared and updated to support each trust account.
- b. Strengthen campus procedures to ensure that only the specific trust funds with negative balances are charged interest.


THE CALIFORNIA STATE UNIVERSITY
 OFFICE OF THE CHANCELLOR

BAKERSFIELD

July 3, 2007

CHANNEL ISLANDS

CHICO

MEMORANDUM

DOMINGUEZ HILLS

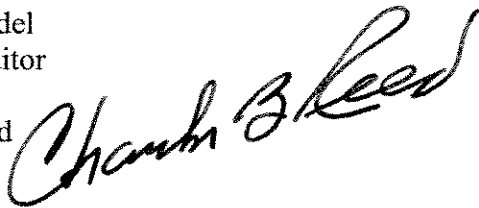
EAST BAY

FRESNO

TO: Mr. Larry Mandel
University Auditor

FULLERTON

FROM: Charles B. Reed
Chancellor



HUMBOLDT

LONG BEACH

SUBJECT: Draft Final Report 06-11 on *FISMA*,
San José State University

LOS ANGELES

MARITIME ACADEMY

MONTEREY BAY

In response to your memorandum of July 3, 2007, I accept the response as submitted with the draft final report on *FISMA*, San José State University.

NORTHRIDGE

POMONA

CBR/jt

SACRAMENTO

Enclosure

SAN BERNARDINO

cc: Mr. Don W. Kassing, President
Ms. Rose L. Lee, Vice President, Administration and Finance

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS