

FISMA

**CALIFORNIA STATE UNIVERSITY,
STANISLAUS**

**Audit Report 07-03
July 31, 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 Henry Mendoza
Glen O. Toney

Staff

University Auditor: Larry Mandel
Senior Director: Janice Mirza
IT Audit Manager: Greg Dove
Senior Auditors: Tanaiia Hall and Linda Rathfelder
Internal Auditor: Ann Casey

BOARD OF TRUSTEES

THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction	4
Purpose	4
Scope and Methodology	4

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Cash Receipts.....	6
Main and Satellite Cashiering	6
Fee Reconciliations	9
Accounts Receivable.....	10
Collections.....	10
Write-Offs	11
Cash Disbursements.....	12
Payroll and Personnel	13
New Hires	13
Employee Separation.....	14
Fiscal Information Technology	15
Desktop Patch Management and Anti-Virus Updates	15
Network Security.....	16
Information Security Procedures	18
E-mail Management	19

APPENDICES

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

ABBREVIATIONS

CMS	Common Management Systems
CSU	California State University
CSUS	California State University, Stanislaus
FISMA	Financial Integrity and State Manager's Accountability Act
HR	Human Resources
OIT	Office of Information Technology
RMP	Revenue Management Program
SAM	State Administrative Manual
SCO	State Controller's Office
STO	State Treasurer's Office
SUAM	State University Administrative Manual

EXECUTIVE SUMMARY

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

California State University, Stanislaus (CSUS) management is responsible for establishing and maintaining adequate internal control. This responsibility, in accordance with Government Code, Sections 13402 et seq., includes documenting internal control, communicating requirements to employees, and assuring that internal control is functioning as prescribed. In fulfilling this responsibility, estimates and judgments by management are required to assess the expected benefits and related costs of control procedures.

The objectives of accounting and administrative control are to provide management with reasonable, but not absolute, assurance that:

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

We visited the CSUS campus from March 5 2007, through April 27, 2007, and made a study and evaluation of the accounting and administrative control in effect as of April 27, 2007. This report represents our biennial review.

Our study and evaluation revealed certain conditions that, in our opinion, could result in errors and irregularities if not corrected. Specifically, the campus did not maintain adequate internal control over the following areas: cash receipts, accounts receivable, cash disbursements, payroll and personnel, and fiscal information technology. These conditions, along with other weaknesses, are described in the executive summary and body of this report.

In our opinion, except for the effect of the weaknesses described above, CSUS's accounting and administrative control in effect as of April 27, 2007, taken as a whole, was sufficient to meet the objectives stated above.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments,

unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

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

CASH RECEIPTS [6]

Cash control weaknesses were found at main cashiering and all three satellite cashiering areas visited. At main cashiering, cashiering duties were not always properly segregated, access to the drop box keys was not restricted, parking permit distribution lacked oversight, and checks received not payable to the university were not prelisted and transferred under the control of transfer receipts. Further, the main cashiering safe was not adequately controlled, and documentation of individuals with access to safes was outdated. These were repeat findings from the prior FISMA audit. At public safety, cashiers shared a single cash drawer, which hampered accountability over shortages and overages. At housing and residential life, press-numbered manual receipts were not always used in sequential order and usage was not reconciled. At university extended education, checks and credit card receipts were stored in a folder kept in an open area. Lastly, fee reconciliations were not always timely prepared or complete. A review of the application fee reconciliations for the fall 2005 to fall 2006 terms disclosed that the fall 2005 reconciliation was prepared and approved 11 months after the end of the fall 2005 term and the reconciliations for fall 2005, winter 2005, spring 2006, and fall 2006 all reflected unexplainable and unreconciled variances.

ACCOUNTS RECEIVABLE [10]

Collection letters were not consistently employed in the pursuit of delinquent third-party, employee, and student accounts receivables. There was no evidence of collection letters being sent in 30-day intervals for 5 of the 25 third-party receivables and 17 of the 18 employee receivables reviewed. In addition, collection letters were not consistently sent in 30-day intervals for 4 of the 14 student receivables reviewed and in eight instances, no collection letters were sent. Further, the campus did not seek discharge from accountability from the State Controller's Office for those accounts over \$1,000 and deemed uncollectible. This is a repeat finding from prior FISMA audit.

CASH DISBURSEMENTS [12]

Long-outstanding checks were not processed in a timely manner. The most recent list of outstanding checks at December 2006 showed 55 checks older than one year totaling \$13,026 and dated between August 2005 and December 2005.

PAYROLL AND PERSONNEL [13]

Federal Form I-9, Employment Eligibility Verification, was not always timely completed, and personnel transaction forms were not always properly approved. A review of 15 new hire transactions disclosed seven instances where I-9 forms were not completed within the required three business days and five instances where payroll transaction forms were not certified by an approving authority in faculty affairs. In addition, employee separation procedures did not ensure timely payment of wages due. A review of ten employee separations disclosed that the final salary payment was not issued within 72 hours of the effective separation date in four instances. This is a repeat finding from the prior FISMA audit.

FISCAL INFORMATION TECHNOLOGY [15]

The campus did not have a reliable process for providing desktop software patch management or ensuring anti-virus definitions are installed consistently and promptly on all computers. Network management did not prevent/detect rogue wireless access points, campus 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. The campus had not given management of information security the attention that it required. There was no information security plan or consistent oversight of the information security process, and no specific 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 support their computer systems. Further, existing practices did not ensure that appropriate security restrictions were being applied to all systems attached to the campus network by all departments that individually support their computer systems. Lastly, the campus had not established policies and procedures for managing the multiple e-mail systems in use. A review of e-mail systems disclosed that the campus allowed independent e-mail systems, but did not enforce effective management over those systems.

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 1, 2005, to December 31, 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 April 27, 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

MAIN AND SATELLITE CASHIERING

Cash control weaknesses were found at main cashiering and all three satellite cashiering areas visited.

The satellite cashiering locations reviewed included public safety, housing and residential life, and university extended education.

Main Cashiering

- ▶ The lead cashier performed cashiering duties, reconciled her own daily receipts without managerial review, and prepared the bank deposit.
- ▶ Keys to the drop box were kept on a key ring in an open basket in the cashiering area.
- ▶ Management did not oversee the distribution of parking permits to the cashiers. Instead, the cashiers withdrew permits from the inventory while completing the log themselves.
- ▶ The safe was kept unlocked throughout the day even though the door to the room where the safe was located remained unlocked and open. In addition, the safe was located in a high traffic area, which was accessible to an unknown number of individuals. This is a repeat finding from the prior Financial Integrity and State Manager's Accountability Act (FISMA) audit.
- ▶ Checks received not payable to the university were not prelisted before transferring to the proper payee. In addition, a transfer receipt for accountability was not utilized.
- ▶ Campus documentation of individuals with access to safes required updating because the housing and residential life safe was not listed and did not reflect the dates of the last combination changes. This is a repeat finding from the prior FISMA audit.

Public Safety

Although cashiers had individual logon codes for Banner, they shared a single cash drawer. As a result, shortages or overages were not easily attributed to the appropriate individual.

Housing and Residential Life

Press-numbered manual receipts were not always utilized in sequential order and usage was not reconciled.

University Extended Education

Checks and credit card receipts were stored in a folder and kept in an open area.

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

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

SAM §8020.1 states that all incoming mail receipts consisting of cash and negotiable instruments not payable to the state agency will be prelisted by the person opening the mail to localize accountability of these assets.

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

SAM §8020 states that an inventory control will be kept for press-numbered receipts and a numeric file of copies of receipts and voided receipts will be kept for audit purposes.

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

The director of student financial services stated that segregation of duties and management oversight of parking permits was not possible due to lack of manpower, while the drop box keys were maintained in close proximity to cashiers for ease of use, and the physical area of cashiers was restricted to authorized personnel only. He further stated that management stressed its concerns about the physical layout and security of the main cashiering area including the location of the safe; however, the campus declined to make improvements. He stated that housing and residential life made no attempt to keep the manual receipts in sequential order since these receipts were only temporary until the transaction could be recorded in Banner, and the responsible manager had failed to maintain a current and accurate listing of the safes. Lastly, the director of student financial services stated that the main cashiering, public safety, and university extended education cashiers did not follow written procedures regarding prelisting checks not payable to the university, using separate cash drawers, and safeguarding of payments.

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

Recommendation 1

We recommend that the campus:

- a. Review main cashiering activities, including the distribution of parking permits, and take appropriate action to segregate duties or establish effective mitigating controls.
- b. Establish and implement procedures to ensure that drop box keys are restricted to only authorized main cashiering personnel.
- c. Require that the safe at main cashiering be kept locked when not in use and update the written records of individuals with knowledge of the safe combinations to include the names of persons with current knowledge and the date the combination was last changed at housing and residential life.
- d. Ensure that main cashiering logs all checks received not payable to the university and uses transfer receipts to transfer the checks to the proper payee.
- e. Prohibit public safety cashiers from sharing cash drawers in order to localize accountability over receipts.
- f. Implement an inventory control system for housing and residential life press-numbered receipts.
- g. Ensure that all university extended education receipts are adequately safeguarded in cash drawers or other secure mechanism until deposited.

Campus Response

We concur. The campus will implement procedural changes on or before August 31, 2007. Copies of procedures will be forwarded by November 15, 2007, for the following:

- a. We are reviewing the cashiering policy and procedures to include the Revenue Management Program (RMP). Due to limited staffing, on occasion the lead cashier performs cashiering duties, reconciles her own daily receipts, and prepares the bank deposit. On these occasions, the director of student financial services or designee will perform a cross verification of the lead cashier's drawer reconciliation. Procedures are in place to ensure the safeguarding of cash and cash equivalents. Public safety provides the main cashier's office parking permit inventories by permit number for each academic term. The inventories are accepted and logged by the lead cashier. The director of student financial services will issue and log out inventories. The permits are sold by main cashier's office only. The unique permit number is recorded into the cashiering system as the decal is sold. Financial services accounts receivable personnel reconcile all parking permit sales by term to the general ledger. Unsold parking permit inventories are reconciled and returned to public safety biannually by the lead cashier.

- b. The keys to the drop box will be kept in the safe to assure accessibility to authorized personnel only.
- c. The safe is separated by a keypad entry door. When authorized personnel are not in the room, the door will remain closed and locked to assure access by authorized personnel only. The updating of written records of individuals with knowledge to the safe combination will be maintained.
- d. Main cashiering will maintain cashiering logs on all checks received not payable to the university and use transfer receipts to transfer the check to the proper payee in the event that this occurs.
- e. Public safety is a satellite cashiering location. Procedures dictate, and staff has been instructed, against the sharing of cash drawers. Additional cash drawers were immediately created to assure accountability over receipts.
- f. The department of housing and residential life took immediate action addressing audit items to ensure that campus specific practices are duly recorded.
 - i. When daily cashiering receipts for the department of housing and residential life exceed \$3,000, new procedures dictate that two department employees are assigned to escort the cash to the main cashier's office.
 - ii. The department of housing and residential life checks the sequential order for hand receipts on a daily basis and records this action in a daily log.
- g. University extended education immediately implemented a procedural change to securely store university receipts in a locked cash drawer restricted to authorized personnel.

FEE RECONCILIATIONS

Fee reconciliations were not always timely prepared or complete.

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

- ▶ The fall 2005 reconciliation was prepared and approved in November 2006, 11 months after the end of the fall 2005 term.
- ▶ The reconciliations for fall 2005, winter 2005, spring 2006, and fall 2006 all reflected unexplainable and unreconciled variances. The variances were \$20,780, \$2,185, \$(9,561), and \$(91,047), respectively.

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

The director of student financial services stated that enrollment services did not provide timely and accurate waiver and application fee data causing the reconciliations to be untimely and incomplete. He further stated that the implementation of the PeopleSoft Student California State University (CSU) Mentor process should eliminate late, unverifiable, and inaccurate data from enrollment services.

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:

- a. Reconcile application fees received timely.
- b. Complete the reconciliations by identifying and resolving all material variances.

Campus Response

We concur. The campus will reconcile application fees and strengthen review procedures to make every effort in identifying and resolving all material reconciliation differences in a timely manner. The campus has immediately implemented the procedure. Copies of the procedures will be forwarded November 15, 2007.

ACCOUNTS RECEIVABLE

COLLECTIONS

Collection letters were not consistently employed in the pursuit of delinquent third-party, employee, and student accounts receivables.

Our review of delinquent accounts receivables disclosed that:

- ▶ There was no evidence of collection letters being sent in 30-day intervals for 5 of the 25 third-party receivables reviewed and for 17 of the 18 employee receivables reviewed.
- ▶ Collection letters were not consistently sent in 30-day intervals for 4 of the 14 student receivables reviewed and in eight instances, no collection letters were sent.

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.

SAM §8776.6 states that once the address of the debtor is known, the accounting office will send a sequence of three collection letters at 30-day intervals. If a reply or payment is not received within 30 days after sending the first letter, the accounting office will send a second letter. This follow-up letter will reference the original request for payment letter and will be stated in a stronger tone. If a response is still not received from the debtor, a third letter will be sent 30 days later. This last letter will include references to prior letters and will state what further actions may be taken in the collection process.

The director of student financial services stated that the third-party receivables pertained to grants and contracts for which collection and follow-up procedures had not been established. He further stated that during the period under review, the grants and contracts department had undergone changes in staffing. He also stated that collection letters were prepared inconsistently for the delinquent student receivables because the computer query used to indicate the past-due accounts requiring letters did not always run in a timely manner. The director of general accounting stated that collection letters were not sent for employee receivables due to staff resources and the extremely heavy workload resulting from the systemwide implementation of the RMP, Wells Fargo Bank, and the subsequent Common Management Systems (CMS)/RMP software updates.

Less than maximum effort in the pursuit of delinquent accounts receivable reduces the likelihood of collection, increases the amount of resources expended on collection efforts, and negatively impacts cash flow.

Recommendation 3

We recommend that the campus establish and implement procedures to use a series of three 30-day collection letters for all delinquent accounts receivables.

Campus Response

We concur. The campus has reestablished procedures for the prompt follow-up of accounts receivables, and in the usage of the issuance of the sequence of three 30-day collection letters for all delinquent receivables: third party, including grants and contracts; employee; and student accounts.

Copies of the procedures will be forwarded November 15, 2007.

WRITE-OFFS

The campus did not seek discharge from accountability from the State Controller's Office (SCO) for those accounts over \$1,000 and deemed uncollectible. This is a repeat finding from the prior FISMA audit.

Executive Order 616, *Discharge of Accountability*, dated April 19, 1994, states in part that campuses will be obligated to comply with the collection efforts as outlined in SAM §8776.6, which includes collection procedures that assure prompt follow-up on receivables.

SAM §8776.6 provides procedures and guidelines regarding adequate collection efforts and follow-up on receivables, including specific requirements for filing applications for Discharge From Accountability (form STD. 27) with the SCO.

The director of student financial services stated that in past years the campus had been unsuccessful in obtaining discharge from the SCO; however, the campus was seeking advice from other CSU campuses on best practices for submitting accounts for discharge.

Inadequate control over accounts receivables 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 reestablish procedures to submit applications for discharge from accountability to the SCO for accounts exceeding \$1,000.

Campus Response

We concur. The campus write-off procedure was reviewed and procedures reestablished on June 25, 2007. All old accounts receivables over \$1,000 will be submitted to the SCO for discharge from accountability. Copies of the procedures will be forwarded November 15, 2007.

CASH DISBURSEMENTS

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

We reviewed the most recent list of outstanding checks at December 2006 and noted 55 checks older than one year totaling \$13,026 and dated between August 2005 and December 2005.

SAM §8042 states that checks have a one-year period of negotiability, unless specific provisions of law require cancellation in a different period of time. Further, agencies will send a stop payment request form to the State Treasurer's Office (STO) for all uncashed checks timed to arrive at least one week prior to the end of the one-year period of negotiability. Upon confirmation from the STO of stop payment request for uncashed checks, agencies will cancel the checks and remit the amount to an escheat revenue account in the fund from which the checks were drawn.

The director of general accounting stated that during the period from August 2006 to February 2007, staff resources and workloads were extremely heavy due to the systemwide implementation of RMP,

Wells Fargo Bank, and the subsequent CMS/RMP software updates, which delayed the normal timeliness of long-outstanding check processing.

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

Recommendation 5

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

Campus Response

We concur. The campus has reestablished procedures with the implementation of the RMP. Wells Fargo Bank policy states that checks have a six-month period of negotiability. All outstanding checks at the six-month period are reviewed during the reconciliation process and cancelled in a timely manner according to the reestablished procedures. All SCO outstanding checks have been reviewed and cancelled according to established procedures. Copies of the procedures will be forwarded November 15, 2007.

PAYROLL AND PERSONNEL

NEW HIRES

Federal Form I-9, Employment Eligibility Verification, was not always timely completed, and personnel transaction forms were not always properly approved.

Our review of 15 new hire transactions disclosed that:

- ▶ In seven instances, I-9 forms processed in faculty affairs were not completed within the required three business days.
- ▶ In five instances, payroll transaction forms for faculty affairs were not certified by an approving authority.

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 SCO Personnel Letter 02-006 states that transactions that are decentrally keyed at the campus may be documented on any campus generated form or report as long as there is an authorized

signature on the document. In addition, campuses are to maintain the signed copy of the document used for processing personnel/payroll transactions in the employee's file for audit purposes.

The associate vice president of faculty affairs stated that although offer (i.e., appointment) letters clearly stipulate that the new employee must contact the office of faculty affairs to complete required hiring documents, some new employees disregarded this instruction or failed to provide the required documents during their initial processing interview. He further stated that in some cases, the employee was appointed late due to last minute changes in the course schedule, which made the late hiring unavoidable. He also noted that non-certification of the payroll transaction forms was an oversight.

Untimely completion of employment eligibility verification increases the risk of non-compliance with federal employment regulations, while the lack of properly approved personnel transaction forms increases the risk of inappropriate personnel transactions.

Recommendation 6

We recommend that the campus strengthen personnel procedures to ensure timely completion of Form I-9 and proper authorization of personnel transactions.

Campus Response

We concur. Form I-9 processing and proper authorization of personnel transaction guidelines are being reviewed and developed to ensure data is received in a timely manner. Faculty affairs is now implementing a new PeopleSoft module. This module will allow faculty affairs to abbreviate the time required to identify potential employees and move them through the recruitment/hiring process. As part of this implementation, faculty affairs will be able to issue a letter (well in advance of the actual hiring effective date) instructing the candidate to initiate processing at the earliest possible moment, but no later than the legal 72-hour time frame. Departments will be copied on these letters, and both faculty affairs and the individual department will track response to them, including follow-up telephone contacts. The subsequent official appointment letter (and concomitant authorization for the hiring transaction) will not be issued until I-9s (and other related hiring documents) are completed before/within the required time frame. Copies of the procedures will be forwarded November 15, 2007.

EMPLOYEE SEPARATION

Employee separation procedures did not ensure timely payment of wages due. This is a repeat finding from the prior FISMA audit.

Our review of ten employee separations disclosed that in four instances, final salary payments were not issued within 72 hours of the effective separation date.

California Labor Code §201 and CSU directive HR 2003-15, *Payment of Wages at Separation – Update*, dated August 6, 2003, state that an employee that resigns from employment must be paid wages earned no later than 72 hours from the date of separation.

The budget manager stated that final salary payments were not timely issued due to oversight.

Insufficient administration of employee separations increases the risk of late wage payments and non-compliance with labor code regulations.

Recommendation 7

We recommend that the campus strengthen employee separation procedures to ensure the timely payment of wages.

Campus Response

We concur. We are working to remedy the situation and will strengthen employee separation procedures. Upon notice of a termination/resignation, the campus issues an estimated check the same day and reconciles the final check through the SCO payroll system. Contract part-time faculty and temporary staff appointments expirations are processed through the SCO pay cycle in a timely manner. Separation wages will be paid in a timely manner. Copies of procedures will be forwarded by November 15, 2007.

FISCAL INFORMATION TECHNOLOGY

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 director of networking and communication services stated that the technology had been installed to require all computers connecting to the network to be properly patched and protected, 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.

Recommendation 8

We recommend that the campus expand the use of existing technologies to ensure that all computers connecting to the network be appropriately patched and virus threats mitigated. Where possible, administrator privileges to desktop computers should be disallowed to ensure that automatic system updates cannot be turned off.

Campus Response

We concur. The following actions will be taken:

- a. Windows computers purchased after September 1, 2007, will be delivered with a standard software image with all automatic software updates activated for both the operating system and anti-virus/anti-spyware programs.
- b. By October 31, 2007, an assessment will be completed to determine the best means of extending use of our existing "Clean Access" management software to include all staff and faculty computers (it is currently used only for student computers used within the residence halls).
- c. Based on the outcome of (b) above, "Clean Access" will be deployed campus-wide by the end of June 30, 2008.
- d. If necessary, administrator privileges will be disallowed to ensure that automatic system updates cannot be turned off.

NETWORK SECURITY

Network management did not prevent/detect rogue wireless access points, campus ports (outlets) 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 §4842.2 states that appropriate risk management procedures should be implemented to provide control of access to information assets. Effective network security practices enforcement of authentication standards and proper restriction on all network access points.

The director of networking and communication services stated that the campus was on a decentralized network, different departments were responsible for individual implementation, and network tools had recently been obtained to assist in restricting access, enforcing consistent authentication policies, and detecting unauthorized devices, although the tools had not yet been fully deployed.

Network ports that do not require authentication increase 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 9

We recommend that the campus:

- a. Either reduce the number of independently managed network domains and implement technologies to ensure that security policies are enforced on a consistent basis or implement procedures to ensure security enforcement on all independently managed servers.
- b. Implement procedures to detect and remove unauthorized devices like rogue wireless access points.
- c. Expand the use of available technologies to force logon to the network and to prevent unpatched computers from gaining access to network resources.
- d. At a minimum, create a written plan with target dates to address these issues due to the complexity and potentially lengthy time frame to implement these controls.

Campus Response

We concur. The following actions will be taken:

- a. By December 1, 2007, an assessment will be completed of the security status of all independently managed servers. The preferred outcome of this assessment will be to transfer to office of information technology (OIT) management responsibility for the maintenance of the system using OIT's existing protocols for addressing security concerns. Otherwise, any independent system will be required to conform to published security guidelines applicable to OIT-managed servers.
- b. Unauthorized wireless access points will be eliminated from the campus as a by-product of the deployment of the new Aruba wireless network currently being installed at California State University, Stanislaus in cooperation with the chancellor's office. Completion is scheduled for August 31, 2008.
- c. The response to recommendation 8 will address the need to force logon to the network and ensure systems are properly patched.
- d. These issues are being addressed as part of the overall campus security plan for June 30, 2008.

INFORMATION SECURITY PROCEDURES

The campus had not given management of information security the attention that it required.

We found that there was no information security plan or consistent oversight of the information security process, and no specific 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 support their computer systems. Further, existing practices did not ensure that appropriate security restrictions were being applied to all systems attached to the campus network by all departments that individually support their computer systems.

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.

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 vice president of information technology stated that an information security position had been requested and that a campus-wide security strategy was currently being developed. He further stated that security management and oversight had previously been divided among various groups, but that there was no individual to ensure that suggested practices were being consistently 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 10

We recommend that the campus:

- a. Make information security management a priority and implement specific directives, focus, and accountability to ensure that risks are mitigated and internal controls are clearly established and implemented.
- b. 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.
- c. 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. The following actions will be taken:

The existing draft information security policies document will be presented to the appropriate campus groups for review during the fall 2007 semester and final approval June 30, 2008. The functions associated with the information security officer role will be assigned to a senior manager within OIT by October 1, 2007, to ensure proper focus and accountability in this area. To help implement security policies and procedures, an additional staff support position will be created and recruitment to fill the position will begin during the fall 2007 semester.

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 vice president of information technology stated that the campus did not require all employees to use a centralized e-mail system, but allowed them to forward e-mail to secondary e-mail systems that were not managed or controlled by business and financial affairs, 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 11

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. The following actions will be taken:

- a. By October 1, 2007, an assessment will be conducted of all e-mail systems on campus.
- b. In conjunction with the security policy review noted in recommendation 10, the campus will establish policies and procedures for e-mail system security.
- c. The student and other independent e-mail systems will be consolidated with the existing staff/faculty system by December 31, 2007, for students and August 31, 2008, for other independent e-mail systems.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Hamid Shirvani	President
Julia Areias	Extended Education Specialist
Sandy Barnhart	Shipping Clerk
Julie Benevedes	Director, General Accounting
Frank Borrelli	Property Clerk, Property Control
Melody Bughi	Procurement Card Administrator
Carol Castillo	Director, Procurement Services/Purchasing
Debbie DaRosa	Lead Buyer, Purchasing
April Dunham-Filson	Accountant, Accounting
D'Ette Gonzalez	Payroll Technician, Payroll Office
Bety Gonzalez De Brito	Accounting Technician, Student Accounts Receivable
Jean Greche Conde	Director, Housing and Residential Life
Delfin Guillory	Accounts Receivable and Collections Team Lead, Student Accounts Receivable
Nancy Havens	Assistant Vice President, Financial Services
Trish Hendrix	Accounting Technician, Accounting
Sara Hoek	Senior Human Resources Technician, Human Resources
Charles Holmberg	Director, Administrative Technology Support
Jennifer Humphrey	Assistant Director, Housing and Residential Life
Steven Jaureguy	Director, Public Safety/Police Chief, Public Safety/University Police Services
Elisa Johnson	Administrative Assistant, Financial Services
Jacque Keeney	Payroll Technician, Payroll Office
David Klein	Director, Networking and Communication Services
Mary Kobayashi Lee	Director, Human Resources
Michelle Legg	Budget Manager, Financial Services
Dosie Lewis	Cashier Team Lead, Cashier's Office
Toni Martinez	Faculty Benefits Coordinator
Wendy Miller	Faculty Affairs Specialist
Donna Moore	Accountant, Accounting
Stacey Morgan Foster	Vice President, Student Affairs
Donevon Murrell	Support Services Supervisor, Public Safety/University Police Services
Gabriel Njock	Information Technology Consultant
Becka Paulsen	Assistant Vice President, Financial Services (At time of review)
Jim Phillips	Director, Student Financial Services
Jon Potter	Community Service Supervisor, Public Safety/University Police Services
Jose Rios	Administrative Support Coordinator, Information Technology
Sherri Rivera	Payroll Technician, Payroll Office
Robert Rosas	Shipping and Receiving Clerk, Shipping Receiving/Facilities Warehouse
Christine Sanders	Administrative Coordinator, Parking Management Bureau
Mary Stephens	Vice President, Business and Finance
Ted Wendt	Associate Vice President, Faculty Affairs
Carl Whitman	Vice President, Information Technology

STATEMENT OF INTERNAL CONTROLS

A. INTRODUCTION

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

B. INTERNAL CONTROL DEFINITION

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

1. Internal Accounting Controls

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

2. Operational Controls

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

C. INTERNAL CONTROL OBJECTIVES

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

D. INTERNAL CONTROL SYSTEMS LIMITATIONS

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



CALIFORNIA STATE UNIVERSITY, STANISLAUS

VICE PRESIDENT FOR BUSINESS & FINANCE

August 29, 2007

RECEIVED
UNIVERSITY AUDITOR

AUG 30 2007

THE CALIFORNIA STATE
UNIVERSITY

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

Dear Larry,

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

Any question concerning the response should be directed to Nancy Havens, Associate Vice President for Financial Management at (209) 667-3866 or via email at nhavens@csustan.edu.

Sincerely,

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

Mary Stephens
Vice President for Business and Finance

Attachment

cc: President Shirvani
Associate Vice President Havens

E-mail: adouglas@calstate.edu

FISMA

**CALIFORNIA STATE UNIVERSITY,
STANISLAUS**

**Audit Report 07-03
July 31, 2007**

CASH RECEIPTS

MAIN AND SATELLITE CASHIERING

Recommendation 1

We recommend that the campus:

- a. Review main cashiering activities, including the distribution of parking permits, and take appropriate action to segregate duties or establish effective mitigating controls.
- b. Establish and implement procedures to ensure that drop box keys are restricted to only authorized main cashiering personnel.
- c. Require that the safe at main cashiering be kept locked when not in use and update the written records of individuals with knowledge of the safe combinations to include the names of persons with current knowledge and the date the combination was last changed at housing and residential life.
- d. Ensure that main cashiering logs all checks received not payable to the university and uses transfer receipts to transfer the checks to the proper payee.
- e. Prohibit public safety cashiers from sharing cash drawers in order to localize accountability over receipts.
- f. Implement an inventory control system for housing and residential life press-numbered receipts.
- g. Ensure that all university extended education receipts are adequately safeguarded in cash drawers or other secure mechanism until deposited.

Campus Response

We concur. The campus will implement procedural changes on or before August 31st. Copies of procedures will be forwarded by November 15, 2007 for the following:

Cashiering activities:

We are reviewing the cashiering policy and procedures to include the Revenue Management Program.

- a. Due to limited staffing, on occasion the lead cashier performs cashiering duties, reconciles her own daily receipts, and prepares the bank deposit. On these occasions, the director of student financial services or designee will perform a cross verification the lead cashiers drawer reconciliation.

Procedures are in place to ensure the safeguarding of cash and cash equivalents. Public Safety provides the Main Cashiers Office parking permit inventories by permit number for each academic term. The inventories are accepted and logged by the lead cashier. The director of student financial services will issue and log out inventories. The permits are sold by Main Cashiers Office only. The unique permit number is recorded into the cashiering system as the decal is sold. Financial Services Accounts Receivable personnel reconcile all parking permit sales by term to the General Ledger. Unsold parking permit inventories are reconciled and returned to Public Safety biannually by the lead cashier.

- b. The keys to the drop box will be kept in the safe to assure accessibility to authorized personnel only.
- c. The safe is separated by a keypad entry door. When authorized personnel are not in the room, the door will remain closed and locked to assure access by authorized personnel only. The updating of written records of individuals with knowledge to the safe combination will be maintained.
- d. Main Cashiering will maintain cashiering logs on all checks received not payable to the university and use transfer receipts to transfer the check to the proper payee in the event that this occurs.
- e. Public Safety is a satellite cashiering location. Procedures dictate, and staff have been instructed against the sharing of cash drawers. Additional cash drawers were immediately created to assure accountability over receipts.
- f. The Department of Housing and Residential Life took immediate action addressing audit items to ensure that campus specific practices are duly recorded.
 - i. When daily cashiering receipts for the Department of Housing and Residential Life exceed \$3,000 new procedures dictate that two department employees are assigned to escort the cash to the Main Cashiers Office.
 - ii. The Department of Housing and Residential Life checks the sequential order for hand receipts on a daily basis and records this action in a daily log.
- g. University Extended Education immediately implemented a procedural change to securely store University receipts in a locked cash drawer restricted to authorized personnel.

FEE RECONCILIATIONS

Recommendation 2

We recommend that the campus:

- a. Reconcile application fees received timely.
- b. Complete the reconciliations by identifying and resolving all material variances.

Campus Response

We concur. The campus will reconcile application fees and strengthen review procedures to make every effort in identifying and resolving all material reconciliation differences in a timely manner. The campus has immediately implemented the procedure. Copies of the procedures will be forwarded November 15, 2007.

ACCOUNTS RECEIVABLE

COLLECTIONS

Recommendation 3

We recommend that the campus establish and implement procedures to use a series of three 30-day collection letters for all delinquent accounts receivables.

Campus Response

We concur. The campus has reestablished procedures for the prompt follow-up of accounts receivables, and in the usage of the issuance of the sequence of three 30-day collection letters for all delinquent receivables.

1. Student accounts
2. Third party, including grants and contracts
3. Employee

Copies of the procedures will be forwarded November 15, 2007.

WRITE-OFFS

Recommendation 4

We recommend that the campus reestablish procedures to submit applications for discharge from accountability to the SCO for accounts exceeding \$1,000.

Campus Response

We concur. The campus write-off procedure was reviewed and procedures reestablished on June 25, 2007. All old accounts receivables over \$1,000 will be submitted to the SCO for discharge of accountability. Copies of the procedures will be forwarded November 15, 2007.

CASH DISBURSEMENTS**Recommendation 5**

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

Campus Response

We concur. The campus has reestablished procedures with the implementation of the Revenue Management Program. Wells Fargo Bank policy states that checks have a six-month period of negotiability. All outstanding checks at the six-month period are reviewed during the reconciliation process and cancelled in a timely manner according to the reestablished procedures. All SCO outstanding checks have been reviewed and cancelled according to established procedures. Copies of the procedures will be forwarded November 15, 2007.

PAYROLL AND PERSONNEL**NEW HIRES****Recommendation 6**

We recommend that the campus strengthen personnel procedures to ensure timely completion of Form I-9 and proper authorization of personnel transactions.

Campus Response

We concur. Form I-9 processing and proper authorization of personnel transaction guidelines are being reviewed and developed to ensure data is received in a timely manner. Faculty Affairs is now implementing a new PeopleSoft module. This module will allow Faculty Affairs to abbreviate the time required to identify potential employees and move them through the recruitment/hiring process. As part of this implementation, Faculty Affairs will be able to issue a letter (well in advance of the actual hiring effective date) instructing the candidate to initiate processing at the earliest possible moment, but no later than the legal 72-hour timeframe. Departments will be copied on these letters, and both Faculty Affairs and the individual department will track response to them, including follow-up telephone contacts. The subsequent official appointment letter (and concomitant authorization for the hiring transaction) will not be issued until I-9s (and other related hiring documents) are completed before/within the required timeframe. Copies of the procedures will be forwarded November 15, 2007.

EMPLOYEE SEPARATION

Recommendation 7

We recommend that the campus strengthen employee separation procedures to ensure the timely payment of wages.

Campus Response

We concur. We are working to remedy the situation and will strengthen employee separation procedures. Upon notice of a termination/resignation, the campus issues an estimated check the same day and reconciles the final check through the State Controller's Office payroll system. Contract Part-time Faculty and Temporary staff appointments expirations are processed through the State Controller's Office pay cycle in a timely manner. Separation wages will be paid in a timely manner. Copies of procedures will be forwarded by November 15, 2007.

FISCAL INFORMATION TECHNOLOGY

DESKTOP PATCH MANAGEMENT AND ANTI-VIRUS UPDATES

Recommendation 8

We recommend that the campus expand the use of existing technologies to ensure that all computers connecting to the network be appropriately patched and virus threats mitigated. Where possible, administrator privileges to desktop computers should be disallowed to ensure that automatic system updates cannot be turned off.

Campus Response

We concur. The following actions will be taken:

1. Windows computers purchased after September 1, 2007 will be delivered with a standard software image with all automatic software updates activated for both the operating system and anti-virus/anti-spyware programs.
2. By October 31, 2007 an assessment will be completed to determine the best means of extending use of our existing "Clean Access" management software to include all staff and faculty computers (it is currently used only for student computers used within the residence halls).
3. Based on the outcome of (2) above, "Clean Access" will be deployed campus-wide by the end of June 30, 2008.
4. If necessary, administrator privileges will be disallowed to ensure that automatic system updates cannot be turned off.

NETWORK SECURITY

Recommendation 9

We recommend that the campus:

- a. Either reduce the number of independently managed network domains and implement technologies to ensure that security policies are enforced on a consistent basis or implement procedures to ensure security enforcement on all independently managed servers.
- b. Implement procedures to detect and remove unauthorized devices like rogue wireless access points.
- c. Expand the use of available technologies to force logon to the network and to prevent unpatched computers from gaining access to network resources.
- d. At a minimum, create a written plan with target dates to address these issues due to the complexity and potentially lengthy time frame to implement these controls.

Campus Response

We concur. The following actions will be taken:

- a. By December 1, 2007 an assessment will be completed of the security status of all independently-managed servers. The preferred outcome of this assessment will be to transfer to OIT management responsibility for the maintenance of the system using OIT's existing protocols for addressing security concerns. Otherwise, any independent system will be required to conform to published security guidelines applicable to OIT-managed servers.
- b. Unauthorized wireless access points will be eliminated from the campus as a by-product of the deployment of the new Aruba wireless network currently being installed at Stanislaus in cooperation with the Chancellor's Office. Completion is scheduled for August 31, 2008.
- c. The response to Recommendation 8 will address the need to force logon to the network and ensure systems are properly patched.
- d. These issues are being addressed as part of the overall campus security plan for June 30, 2008.

INFORMATION SECURITY PROCEDURES

Recommendation 10

We recommend that the campus:

- a. Make information security management a priority and implement specific directives, focus, and accountability to ensure that risks are mitigated and internal controls are clearly established and implemented.

- b. 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.
- c. 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 inter-departmental executive council with responsibility and authority to address information security issues, in conjunction with a campus-wide working committee to oversee security implementation and monitoring.

Campus Response

We concur. The following actions will be taken:

The existing draft information security policies document will be presented to the appropriate campus groups for review during the fall 2007 semester and final approval June 30, 2008.

The functions associated with the Information Security Officer role will be assigned to a senior manager within OIT by October 1, 2007 to ensure proper focus and accountability in this area. To help implement security policies and procedures, an additional staff support position will be created and recruitment to fill the position will begin during the fall 2007 semester.

E-MAIL MANAGEMENT

Recommendation 11

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. The following actions will be taken:

- a. By October 1, 2007 an assessment will be conducted of all e-mail systems on campus.
- b. In conjunction with the security policy review noted in Recommendation 10, the campus will establish policies and procedures for e-mail system security.
- c. The student and other independent e-mail systems will be consolidated with the existing staff/faculty system by December 31, 2007 for students and August 31, 2008 for other independent e-mail systems.



THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

September 25, 2007

CHANNEL ISLANDS

CHICO

MEMORANDUM

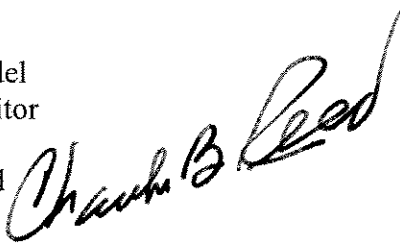
DOMINGUEZ HILLS

EAST BAY

FRESNO

TO: Mr. Larry Mandel
University Auditor

FULLERTON

FROM: Charles B. Reed
Chancellor 

HUMBOLDT

LONG BEACH

SUBJECT: Draft Final Report 07-03 on *FISMA*,
California State University, Stanislaus

LOS ANGELES

MARITIME ACADEMY

MONTEREY BAY

In response to your memorandum of September 25, 2007, I accept the response as submitted with the draft final report on *FISMA*, California State University, Stanislaus.

NORTHRIDGE

POMONA

SACRAMENTO

CBR/amd

SAN BERNARDINO

Enclosure

SAN DIEGO

cc: Dr. Hamid Shirvani, President
Ms. Mary Stephens, Vice President, Business and Finance

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS