

FISMA

SAN DIEGO STATE UNIVERSITY

**Audit Report 07-01
June 19, 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
IT Audit Manager: Greg Dove
Senior Auditor: Danette Adams

BOARD OF TRUSTEES

THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction.....	3
Purpose	3
Scope and Methodology	3

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Cash Receipts.....	5
Payroll and Personnel	6
Employee Separation.....	6
Employment Eligibility Verification	7
Fixed Assets	8
Fiscal Information Technology	9
Encryption of Sensitive Data.....	9
E-mail Management	9
Program Change Control.....	10

APPENDICES

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

ABBREVIATIONS

CIO	Chief Information Officer
CSU	California State University
FISMA	Financial Integrity and State Manager's Accountability Act
IVC	Imperial Valley Campus
SAM	State Administrative Manual
SDSU	San Diego State University

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 Diego State University (SDSU) 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 SDSU campus from February 5, 2007, through March 28, 2007, and made a study and evaluation of the accounting and administrative control in effect as of March 28, 2007. This report represents our biennial review.

Our study and evaluation did not reveal any significant internal control problems or weaknesses that would be considered pervasive in their effects on accounting and administrative controls. However, we did identify other reportable weaknesses that are described in the executive summary and body of this report.

In our opinion, SDSU's accounting and administrative control in effect as of March 28, 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 [5]

Cash control weaknesses were found at the Imperial Valley Campus (IVC) satellite location. Security and accountability over press-numbered receipts were not adequately controlled. Specifically, the IVC cashiering office did not keep press-numbered receipts in a locked secure location, the numerical sequence of manual press-numbered receipts was not accounted for, and an inventory control system was not in place. One cash drawer was shared by multiple employees and a single password was utilized to process transactions. Further, cash handling functions were not adequately segregated because a single employee was designated as custodian of the petty cash fund, performed cashiering functions, tallied batch receipts, and performed all daily deposit activities.

PAYROLL AND PERSONNEL [6]

Employee separation procedures did not ensure complete clearance documentation. A review of ten employee separations disclosed no evidence that the employees received clearance checklists or that the employee clearance process ensured the completion of online clearance forms. In addition, 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 hires disclosed that the campus did not complete employment eligibility verification for three employees within the required time frame.

FIXED ASSETS [8]

Property survey board approval was not always obtained prior to asset disposal. A review of 20 property survey reports disclosed that in 13 instances, asset disposals were completed and recorded in the campus property system prior to authorization by the property survey board.

FISCAL INFORMATION TECHNOLOGY [9]

The campus did not encrypt sensitive personal information stored on the student administration and financial aid systems. The campus allowed independent e-mail systems, but had not established policies and procedures for managing those systems. Additionally, existing practices did not prevent enrollment services personnel with programming responsibilities from making unauthorized changes to production programs and data.

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 2005 to December 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 March 28, 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

Cash control weaknesses were found at the Imperial Valley Campus (IVC) satellite location.

We found that:

- ▶ Security and accountability over press-numbered receipts were not adequately controlled. The IVC cashiering office did not keep press-numbered receipts in a locked secure location. Instead, the receipts were kept in an unlocked drawer. In addition, the numerical sequence of manual press-numbered receipts was not accounted for and an inventory control system was not in place.
- ▶ One cash drawer was shared by multiple employees and a single password was utilized to process transactions.
- ▶ Cash handling functions were not adequately segregated because a single employee was designated as custodian of the petty cash fund, performed cashiering functions, tallied batch receipts, and performed all daily deposit activities.

State Administrative Manual (SAM) §8020 states that an inventory control will be kept for press-numbered receipts

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

SAM §8021 requires that a separate series of transfer receipts be used to localize accountability for cash or negotiable instruments to a specific employee from the time of its receipt to its deposit.

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.

The IVC director of business and financial services stated she had oversight for the satellite location and that due to the very limited number of staff in the cashiering office, the limited number of transactions processed, and her close oversight, she felt that there was minimal risk from sharing passwords, a single cash drawer, and other cashiering duties.

Inadequate control and segregation of duties over cash receipts increase campus exposure to loss from irregular activities.

Recommendation 1

We recommend that the campus:

- a. Secure press-numbered receipts when not in use and establish an inventory control system over the receipts, including accountability over their numerical sequence.
- b. Localize accountability for cash receipts and implement the use of unique passwords.
- c. Either segregate cash handling functions or establish mitigating controls.

Campus Response

We concur. The university has updated its IVC procedures for appropriate control and accountability of press-numbered and cash receipts. In addition, unique user IDs and passwords have been established and cash handling functions have been segregated.

PAYROLL AND PERSONNEL

EMPLOYEE SEPARATION

Employee separation procedures did not ensure complete clearance documentation.

Our review of ten employee separations dated between July 2005 and December 2006 disclosed that:

- ▶ None of the employees reviewed received clearance checklists or had clearance forms on file. This is a repeat finding from the prior Financial Integrity and State Manager's Accountability Act (FISMA) audit.
- ▶ There was no evidence that campus online clearance forms were completed to provide notice of employees' impending departure to appropriate campus offices.

San Diego State University (SDSU) *Employee Clearance Procedures*, dated December 5, 2006, require employees to complete a checkout process. This process includes an employee clearance checklist and the completion of an online form by supervisors/department coordinators, which notifies appropriate offices to cancel access or authorization granted to employees. This process should be completed before employment with SDSU terminates.

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.

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

The compensation and payroll services manager stated that the current online clearance process identified the steps needed for proper clearance, but did not include a written record to the employee's personnel file.

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

Recommendation 2

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

Campus Response

We concur. The university has strengthened procedures for the online clearance process to include a written record to the separating employee's personnel file. Furthermore, mandatory training has been provided to university departments.

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 July 2005 and December 2006 disclosed that in three instances, the campus did not complete employment eligibility verification within the required three days.

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

The compensation and payroll services manager stated that because of new collective bargaining settlement restrictions on offering positions particularly in graduate assistant and teaching associate areas, departments were waiting longer to submit employment paperwork to allow time to determine whether classes remained open at the start of the semester.

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

Recommendation 3

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

Campus Response

We concur. The university has conducted mandatory department coordinator training to ensure that I-9 forms are completed in a timely manner. Also, additional new hire sign-in sessions have been established for the fall 2007 semester to give departments the ability to have employees promptly complete new hire paperwork, including the I-9 form.

FIXED ASSETS

Property survey board approval was not always obtained prior to asset disposal.

Our review of 20 property survey reports dated between July 2005 and December 2006 disclosed that in 13 instances, asset disposals were completed and recorded in the campus property system prior to authorization by the property survey board.

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

The director of business services stated that entries into the property system to retire fixed assets were made as close to the retirement date as possible to meet the expected timelines.

Insufficient control over fixed asset disposal and property accounting increases the risk of misstated property records.

Recommendation 4

We recommend that the campus strengthen controls to ensure that authorization is obtained prior to asset disposal and deletion from the property system.

Campus Response

We concur. The university has changed its practices to ensure that authorization is obtained prior to asset disposal and deletion from the property system. Written desktop procedures will be finalized by September 21, 2007.

FISCAL INFORMATION TECHNOLOGY

ENCRYPTION OF SENSITIVE DATA

The campus did not encrypt sensitive personal information stored on the student administration and financial aid 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 chief information officer (CIO) stated that the servers for the student administration and financial aid systems had been secure and placed behind campus firewalls to help minimize the likelihood of a system breach, but that not all files containing sensitive data had been encrypted.

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

Recommendation 5

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

Campus Response

The university has alternate security controls within its student administration and financial aid applications, which accomplish protection of its information assets. The university's current controls are in compliance with laws and regulations and are consistent with CSU systemwide student system applications controls. The university accepts the risk inherent in not encrypting sensitive personal information. Encryption of sensitive information will continue to be evaluated as a security protocol within these application areas.

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 CIO stated that the campus did not require all employees to use a centralized e-mail system and allowed them to forward e-mail to secondary e-mail systems that were not managed or controlled by business and financial affairs. He further stated 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 6

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 procedures to ensure that e-mail systems are properly administered.

Campus Response

We concur.

- a. The university completed an assessment to identify campus e-mail systems, which are externally accessible in February 2007. This process was conducted in conjunction with the campus implementation of a closed border network firewall.
- b. The university has recently completed a vulnerability management program, as part of its computing security plan, which includes policies and procedures that describe proper security and management of e-mail systems.
- c. The university will establish monitoring and oversight procedures to ensure the proper security administration of e-mail systems by December 17, 2007.

PROGRAM CHANGE CONTROL

Existing practices did not prevent enrollment services personnel with programming responsibilities from making unauthorized changes to production programs and data.

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 executive director of enrollment services stated that formal, written quality assurance procedures were being developed, which would preclude programmers from making changes directly to production programs and data.

Since programmers have the capability to make changes directly to production copies of programs and data, management cannot be assured that all changes made are authorized and, consequently, that internal controls are not compromised.

Recommendation 7

We recommend that the campus:

- a. Implement procedures to effectively restrict programmers from update access to production copies of programs and data.
- b. Formalize and implement the quality assurance procedures under development.

Campus Response

We concur. The university will implement appropriate program change control and quality assurance procedures within student administration and financial aid applications by December 17, 2007.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Stephen L. Weber	President
Soheyla Akhlaghi	Accounting Technician
Cathleen Austin	Manager, Accounts Payable
Scott Burns	Associate Vice President, Financial Operations
Mikahil Burstein	Director SIMS/R, Enrollment Services
Paul Carlisle	San Diego State University Card Program Administrator
Micki Carlson	Accounting Technician
Kevin Carter	Director of Information Systems, Student Affairs
Valerie Carter	Director, Audit and Tax
Norma Casas	Analyst, Audit and Tax
Leslie Chase	Manager, Financial Reporting
Sandra Cook	Executive Director, Enrollment Services
David Del Rio	Manager, Material Receiving
John Denune	Technology Security Officer
Alma Escobedo	Accounting Technician
La Dedra Ewings	Accounting Technician
Cathy Garcia	Manager, Contract and Procurement Management
Javier Gudino	Director, Enrollment Services
Matt Iraci	Pharmacist
Lorretta Leavitt	University Controller
Virginia Litonjua	Office Operations Manager
Liz Lockwood	Accounting Technician
Irma Martinez	Director, Business and Financial Services, Imperial Valley Campus
Diana Mazzone	Lead Cashier
Dana McCoy	Manager, Accounting Services
Judi Mitchell	Manager, Compensation and Payroll Services
Marsha Morgan	Manager, Pharmacy Operations
Jeanette Nevandro	Operations Supervisor, College of Extended Studies
Robert Newhouse	Director, University Computer Operations
Mary Ann Patty	Manager, University Cashier's Office
Lawrence Peralez	Director, Business Services
Rich Pickett	Chief Information Officer
Chip Pierce	Assistant Director, Systems, Financial Aid and Scholarship
Jan Pierce	Administrative Support Coordinator
Kimberlee Reilly	Acting Manager, Student Financial Services
Elizabeth Reynertson	Benefits Administrator
Destiny Roelofsz	Trust Accountant
Sally Roush	Vice President, Business and Financial Affairs
Raul Ruiz	Receiving Clerk
Ken Savage	Systems Specialist, University Computer Operations
Jeff Seabrook	Information Technology Consultant, Business Services
Felecia Vlahos	Information Security Officer

APPENDIX A: PERSONNEL CONTACTED

Name

Title

Jeff Wal

Accountant

Cyndie Winrow

Director, Business Information Systems

Lisa Winters

Assistant Manager, Compensation and Payroll

Laurey Wisnosky

Benefit Services Specialist

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

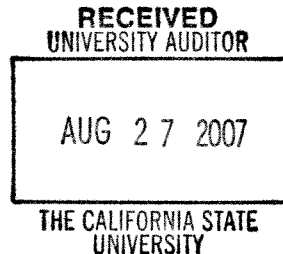
There are inherent limitations that should be recognized in considering the potential effectiveness of any system of internal accounting and related operational control. In the performance of most control procedures, errors can result from misunderstanding of instruction, mistakes of judgment, carelessness, 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.

Office of the President
San Diego State University



5500 Campanile Drive
San Diego, CA 92182 · 8000
Tel: 619 594 · 5204
Fax: 619 594 · 8894

August 23, 2007



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

Dear Mr. Mandel:

Attached is San Diego State University's response to Report Number 07-01, *FISMA*. For ease of reference, the report's recommendations have been included with our responses. Documentation of policy and control changes will follow under separate cover.

Should you have any questions or require additional information, please contact Valerie Carter, Audit and Tax Director, at 619-594-5901.

Sincerely,

A handwritten signature in black ink, appearing to read "Steve Weber".

Stephen L. Weber
President

Attachment

- c: Sally F. Roush, Vice President for Business and Financial Affairs
- Scott Burns, Associate Vice President, Financial Operations
- Valerie J. Carter, Director, Audit and Tax

FISMA**SAN DIEGO STATE UNIVERSITY****Audit Report 07-01****June 19, 2007****CASH RECEIPTS****Recommendation 1**

We recommend that the campus:

- a. Secure press-numbered receipts when not in use and establish an inventory control system over the receipts, including accountability over their numerical sequence.
- b. Localize accountability for cash receipts and implement the use of unique passwords.
- c. Either segregate cash handling functions or establish mitigating controls.

Campus Response

We concur. The University has updated its Imperial Valley Campus procedures for appropriate control and accountability of press-numbered and cash receipts. In addition, unique user IDs and passwords have been established and cash handling functions have been segregated.

PAYROLL AND PERSONNEL**EMPLOYEE SEPARATION****Recommendation 2**

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

Campus Response

We concur. The University has strengthened procedures for the on-line clearance process to include a written record to the separating employee's personnel file. Furthermore, mandatory training has been provided to University departments.

EMPLOYMENT ELIGIBILITY VERIFICATION

Recommendation 3

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

Campus Response

We concur. The University has conducted mandatory Department Coordinator training to ensure that I-9 forms are completed in a timely manner. Also, additional new hire sign-in sessions have been established for the fall 2007 semester to give departments the ability to have employees promptly complete new hire paperwork, including the I-9 form.

FIXED ASSETS

Recommendation 4

We recommend that the campus strengthen controls to ensure that authorization is obtained prior to asset disposal and deletion from the property system.

Campus Response

We concur. The University has changed its practices to ensure that authorization is obtained prior to asset disposal and deletion from the property system. Written desktop procedures will be finalized by September 21, 2007.

FISCAL INFORMATION TECHNOLOGY

ENCRYPTION OF SENSITIVE DATA

Recommendation 5

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

Campus Response

The University has alternate security controls within its Student Administration and Financial Aid applications which accomplish protection of its information assets. The University's current controls are in compliance with laws and regulations and are consistent with CSU system-wide student system applications controls. The University accepts the risk inherent in not encrypting sensitive personal information. Encryption of sensitive information will continue to be evaluated as a security protocol within these application areas.

E-MAIL MANAGEMENT

Recommendation 6

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 procedures to ensure that e-mail systems are properly administered.

Campus Response

We concur.

- a. The University completed an assessment to identify campus e-mail systems which are externally accessible in February 2007. This process was conducted in conjunction with the campus implementation of a closed border network firewall.
- b. The University has recently completed a Vulnerability Management Program, as part of its computing security plan, which includes policies and procedures that describe proper security and management of e-mail systems.
- c. The University will establish monitoring and oversight procedures to ensure the proper security administration of e-mail systems by December 17, 2007.

PROGRAM CHANGE CONTROL

Recommendation 7

We recommend that the campus:

- a. Implement procedures to effectively restrict programmers from update access to production copies of programs and data.
- b. Formalize and implement the quality assurance procedures under development.

Campus Response

We concur. The University will implement appropriate program change control and quality assurance procedures within Student Administration and Financial Aid applications by December 17, 2007.



THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

August 30, 2007

CHANNEL ISLANDS

CHICO

MEMORANDUM

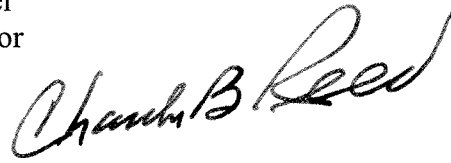
DOMINGUEZ HILLS

EAST BAY

FRESNO

TO: Mr. Larry Mandel
University Auditor

FULLERTON

FROM: Charles B. Reed
Chancellor


HUMBOLDT

LONG BEACH

SUBJECT: Draft Final Report 07-01 on *FISMA*,
San Diego State University

LOS ANGELES

MARITIME ACADEMY

MONTEREY BAY

In response to your memorandum of August 30, 2007, I accept the response as submitted with the draft final report on *FISMA*, San Diego State University.

NORTHRIDGE

POMONA

CBR/jt

SACRAMENTO

Enclosure

SAN BERNARDINO

cc: Mr. Scott Burns, Associate Vice President, Financial Operations
Dr. Stephen L. Weber, President

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS