## CONTENTS

### INTRODUCTION

<table>
<thead>
<tr>
<th>Purpose</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope and Methodology</td>
<td>1</td>
</tr>
<tr>
<td>Background</td>
<td>2</td>
</tr>
<tr>
<td>Opinion</td>
<td>3</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
</tbody>
</table>

### OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

<table>
<thead>
<tr>
<th>Cash Receipts</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Technology</td>
<td>5</td>
</tr>
<tr>
<td>Disaster Recovery Plan</td>
<td>5</td>
</tr>
<tr>
<td>Mainframe Security</td>
<td>7</td>
</tr>
<tr>
<td>Program Change Control</td>
<td>8</td>
</tr>
<tr>
<td>Data Center Access</td>
<td>9</td>
</tr>
</tbody>
</table>
APPENDICES

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

ABBREVIATIONS

CSU  California State University
DRP  Disaster Recovery Plan
FISMA Financial Integrity and State Manager’s Accountability Act
IT   Information Technology
SAM  State Administrative Manual
INTRODUCTION

PURPOSE

The principal audit objective was to assess the adequacy of controls and systems to ensure that:

- Cash receipts are processed in accordance with laws, regulations and management policies.
- Receivables are promptly recognized and balances are periodically evaluated.
- Purchases are made in accordance with laws, regulations and management policies.
- Revolving fund disbursements are authorized and processed in accordance with laws, regulations, and management policies.
- Cash disbursements are properly authorized and made in accordance with established procedures, and adequate segregation of duties exists.
- Payroll/personnel criteria for hiring employees, establishing compensation rates and authorizing disbursements are controlled, and access to personnel and payroll records and processing areas are restricted.
- Purchase and disposition of fixed assets are controlled and assets are promptly recorded in the subsidiary records.
- Physical computer controls are in place and functioning.
- Investments are adequately controlled and securities are safeguarded.
- Trust funds are established in accordance with State University Administrative Manual guidelines.

SCOPE AND METHODOLOGY

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 2000-2001 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 2001 to February 2002. Our primary focus was on internal controls. Specifically, we reviewed and tested:

- Procedures for receipting and storing cash, segregation of duties involving cash receipting and recording of cash receipts.
- Establishment of receivables and adequate segregation of duties regarding billing and payment of receivables.
Approval of purchases, receiving procedures and reconciliation of expenditures to State Controller's balances.

Limitations on the size and types of revolving fund disbursements.

Use of petty cash funds, periodic cash counts, and reconciliation of bank accounts.

Authorization of personnel/payroll transactions and accumulation of leave credits in compliance with state policies.

Posting of the property ledger, monthly reconciliation of the property to the general ledger, and physical inventories.

Access restrictions to automated accounting systems and proper documentation of the systems.

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 the date of our report. 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.

BACKGROUND

In 1983, the California Legislature passed the Financial Integrity and State Manager's Accountability Act of 1983 (FISMA). This act required state agencies to establish and maintain a system of internal accounting and administrative control. To ensure that the requirements are fully complied with, the head of each agency is required to prepare and submit a report on the adequacy of the system of internal accounting and administrative control following the end of each odd-numbered fiscal year. The Office of the University Auditor of the California State University (CSU) is currently responsible for conducting such audits within the CSU.

This report represents our biennial review.
OPINION

We visited the CSU Chico campus from January 14, 2002, through March 8, 2002, and made a study and evaluation of the accounting and administrative control in effect as of March 8, 2002. Our study and evaluation were conducted in accordance with the 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.

CSU Chico 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.

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

In our opinion, the accounting and administrative control at CSU Chico in effect as of March 8, 2002, 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 change 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.
EXECUTIVE SUMMARY

The purpose of this section is to provide 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]

The campus did not have a procedure to periodically request local banks to search for unauthorized bank accounts that use the campus name, address, and federal identification number. Establishing a process to periodically search for unauthorized bank accounts reduces the risk of liability associated with improper accounts.

INFORMATION TECHNOLOGY [5]

DISASTER RECOVERY PLAN [5]

The information technology (IT) disaster recovery plan (DRP) did not contain sufficient information to ensure that data processing services could be recovered in a timely manner. With a detailed IT DRP, corresponding business continuation procedures, and frequent off-site backup tape storage, the campus will be better able to restore computer operations and critical information within a reasonable time frame, thereby reducing the impact of a disaster on normal business operations.

MAINFRAME SECURITY [7]

Some mainframe security (RACF) parameters were not set to provide effective protection, and many sensitive libraries were not sufficiently protected. Appropriate security settings and protection of libraries improve security and help prevent unauthorized access to, and misuse of, computer resources.

PROGRAM CHANGE CONTROL [8]

Existing practices did not prevent all persons with programming responsibilities from making unauthorized changes to production programs and data for the student information system. Internal controls are enhanced when programmers do not have the capability to make changes directly to production copies of programs and data.

DATA CENTER ACCESS [9]

Doors that provide entry to the data center had traditional key locks, which may not appropriately restrict access to the data center to only those persons who have responsibility for maintaining the computer systems. Effectively controlling access to the data center minimizes the risk of accidental or intentional damage or theft of equipment or data that is essential to continued campus operations.
OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

CASH RECEIPTS

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

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

State Administrative Manual (SAM) §20050 states that a satisfactory system of internal accounting and administrative control shall include a plan of organization that provides segregation of duties appropriate for proper safeguarding of state agency assets.

The director of student financial services stated that meetings were held with the director of financial accounting and reporting about contacting local banks on this matter, but no action was ever taken.

Not establishing a process to periodically search for unauthorized bank accounts increases the risk of the campus being associated with improper bank accounts.

Recommendation 1

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

Campus Response

We concur. We will implement procedures to periodically search for unauthorized bank accounts at local banks. Anticipated Completion Date: November 2002

INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

The information technology (IT) disaster recovery plan (DRP) did not contain sufficient information to ensure that data processing services could be recovered in a timely manner.

Specifically, we noted that the current disaster recovery plan did not address end-user recovery procedures, had not been tested, and provided for backup tapes to only be sent off-site on a weekly basis.
SAM §4843.1 requires each state agency to establish and maintain both an operational recovery plan to protect its information assets in the event of a disaster or serious disruption to its operations, and the agency’s plans for resuming operation following a disaster affecting those applications.

Executive Order No. 696, Implementation of The California State University Emergency Preparedness Program, dated January 29, 1999, states, in part, that each campus president is delegated the responsibility for the implementation of a multi-hazard emergency program on campus, and shall ensure that management activities, including but not limited to, maintenance and regular updating of the institutional multi-hazard emergency plan, and determination, acquisition and maintenance of facilities, equipment, and related supplies required for emergency preparedness are accomplished.

The director of computing services stated that high-level plans were in place to acquire the necessary hardware, and data recovery procedures were documented; however, comprehensive detailed recovery policies and procedures had not been completed. She further stated that weekly backups may be appropriate depending on the campus needs for data recovery.

Without a detailed IT DRP, corresponding business continuation procedures, and frequent off-site storage of backup tapes, the campus may not be able to restore computer operations and critical information within a reasonable time frame, which could severely impact the ability of the campus to conduct normal business operations.

Recommendation 2

We recommend that the campus:

a. Enhance the IT DRP by adding detailed procedures for all sections outlined in SAM, develop campus business continuity plans to sustain operations during an extended outage of data processing services, and add an assumptions list that should be shared with the business users to enhance their understanding of what services will and will not be restored as part of the IT recovery plan and that reflects the status of data files at the time of restoration.

b. Conduct a business impact assessment to determine the maximum length of time that the departments could operate without data processing services and identify the equipment and information that would be needed to sustain operations during an outage of data processing services.

c. Develop written manual operating and recovery procedures for business units to assist operations during an extended outage of data processing services, such as recreation of up to one week of lost data and procedures for entering data collected manually during a prolonged system outage.

d. Determine if only weekly off-site storage of tapes, which represents a potential loss of up to one week’s worth of data, is sufficient to adequately recover campus business operations. Consider more frequent off-site storage during critical processing times such as online registration.
Campus Response

CSU Chico recognizes the deficiencies in the existing DRP and will enhance the plan using the recommendations as a guide in developing more comprehensive recovery processes and procedures. A project lead will be assigned by September 1st; the development of the project plan and identification of project team members will begin in September. Though a comprehensive DRP is recognized as essential to the timely and successful recovery from a catastrophic disaster, this planning effort will take a substantial amount of time. Anticipated Completion Date: June 2003

MAINFRAME SECURITY

Some mainframe security (RACF) parameters were not set to provide effective protection, and many sensitive libraries were not sufficiently protected.

Specifically, we noted:

- Protect All, which requires data sets to be RACF protected, was not in effect.
- Tape DSN, which enables protection of data sets stored on tape, was not in effect.
- Security over security propagation, the job entry subsystem, and the batch job handler were not active, which could permit the submission of unauthorized jobs.
- Inactive user IDs were not being automatically revoked.
- Passwords were not required to be changed at an interval of 90 days or less.
- The default password was in effect for the powerful RACF command RVARY.
- Systemwide update and read access was provided to libraries whose names begin with high level “SYS1,” which could result in unauthorized access or reveal sensitive information about the system.

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

The director of computing services stated that the settings had not been recently examined.

Lack of adequate security settings and protection of sensitive libraries increases the risk that programs or data files would not be protected by RACF, information stored on magnetic tape would not be protected, and unlimited access to system resources could be obtained through inappropriate access to sensitive libraries.
Recommendation 3

We recommend that the campus:

a. Activate the aforementioned RACF settings regarding tape data set protection, Protect All, and batch and online job submission.

b. Revoke inactive IDs automatically and require passwords to be changed every 90 days or less.

c. Change the password on the RVARY command.

d. Change the universal access code setting to NONE for sensitive SYS1 libraries in order to reduce the risk of disclosure of system security settings and unauthorized access to powerful system libraries.

Campus Response

a. The RACF settings are being implemented one at a time, starting with Protect All. We do expect process failures. We have chosen this phased approach to minimize the number of process failures at any given time, to minimize the confusion on the cause of process failures, and to minimize the impact on limited technical staff time resources. Anticipated Completion Date: December 2002

b. Inactive IDs will be automatically revoked after 180 days. The password change policy will be changed from 180 days to 90 days. Anticipated Completion Date: October 2002

c. The password has been changed on the RVARY command. Anticipated Completion Date: Completed

d. The universal access code setting for sensitive SYS1 libraries is included in the phased approach for implementing the RACF settings. As noted, the expected completion date is no later than December 31, 2002. Anticipated Completion Date: December 2002

PROGRAM CHANGE CONTROL

Existing practices did not prevent all persons with programming responsibilities from making unauthorized changes to production programs and data for the student information system.

SAM §20050 states that there should be an established system of authorization and record-keeping procedures adequate to provide effective accounting control over assets, liabilities, revenues, and expenditures.

The director of computing services stated that formal change control procedures exist, but due to staffing limitations, it was not practical to remove update access from the programming personnel.
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 4**

We recommend that if the campus cannot effectively restrict all programmers from update access to production copies of programs and data, then a detective control reflecting programs that have been changed should be produced and reviewed by management on a regular basis, and access to data should not be allowed without specific written authorization from management.

**Campus Response**

All programmers must have the capability to make changes to production programs. Chico does not have the technical staff resources to do otherwise. To date, we have not been able to devise an automated detective control that will notify management when a program or data has been changed by technical staff. We understand the basis for the recommendation however, and will implement a manual control by logging all program changes (program ID, change request identifier, programmer, date changed) for comparison to standard source library directory information (program ID, date of change, and user ID used by individual making the change). This process will be implemented in September 2002. Anticipated Completion Date: Completed

**DATA CENTER ACCESS**

Doors that provide entry to the data center had traditional key locks, which may not appropriately restrict access to the data center to only those persons who have responsibility for maintaining the computer systems.

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

The director of computing services stated that a project had been initiated to install a card key locking mechanism, but the project had not been completed.

Ineffective controls over access to the data center increase the risk of accidental or intentional damage or theft to equipment and data that is essential to the continued operation of the campus.

**Recommendation 5**

We recommend that the campus complete the project to install a more restrictive physical security mechanism that will allow the computer services department to appropriately restrict access to the data center to only authorized personnel, which should be limited to the operators and a few key personnel.
Campus Response

The electronic card access project has been implemented. Anticipated Completion Date: Completed
# APPENDIX A:  
**PERSONNEL CONTACTED**

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuel A. Esteban</td>
<td>President</td>
</tr>
<tr>
<td>Brenda Aden</td>
<td>Vice Provost for Human Resources</td>
</tr>
<tr>
<td>Miles Allen</td>
<td>Director, New Technologies Business Process Mapping</td>
</tr>
<tr>
<td>Andi Beach</td>
<td>Manager, Payroll Services</td>
</tr>
<tr>
<td>Paula Brackett</td>
<td>Public Services Supervisor, Student Records and Registration</td>
</tr>
<tr>
<td>Jan Burnham</td>
<td>Director, Student Financial Services</td>
</tr>
<tr>
<td>Dick Chamberlain</td>
<td>Cashiering Supervisor</td>
</tr>
<tr>
<td>Pedro Douglas</td>
<td>Director, Student Health Center</td>
</tr>
<tr>
<td>Denise Gavello</td>
<td>Accounting Technician</td>
</tr>
<tr>
<td>Debbie Gott</td>
<td>Registered Pharmacist, Student Health Center</td>
</tr>
<tr>
<td>Dennis Graham</td>
<td>Vice President, Business and Finance</td>
</tr>
<tr>
<td>Jeannie Graham</td>
<td>Supervisor, Library Circulations</td>
</tr>
<tr>
<td>Pattie Hannemann</td>
<td>Director, Procurement Services</td>
</tr>
<tr>
<td>Charlie Harliss</td>
<td>Manager, Warehouse Operations</td>
</tr>
<tr>
<td>Matthew Horn</td>
<td>Accountant</td>
</tr>
<tr>
<td>Jenny Javor</td>
<td>Accountant</td>
</tr>
<tr>
<td>Bill Jones</td>
<td>University Internal Auditor/Financial Analyst</td>
</tr>
<tr>
<td>Michelle Korte</td>
<td>Director, Financial Accounting and Reporting</td>
</tr>
<tr>
<td>Debbie McElroberts</td>
<td>Director, Computing Services</td>
</tr>
<tr>
<td>Doreen Mendes</td>
<td>Accounting Technician</td>
</tr>
<tr>
<td>Ria Pope</td>
<td>Administrative Assistant, Financial Services</td>
</tr>
<tr>
<td>Sondra Sample</td>
<td>Supervisor, Accounts Payable</td>
</tr>
<tr>
<td>Sandy Smith</td>
<td>Travel Accounting Clerk, Accounts Payable</td>
</tr>
<tr>
<td>Gilbert Tyrrell</td>
<td>Property Clerk</td>
</tr>
<tr>
<td>George Wellman</td>
<td>Associate Vice President, Financial Services</td>
</tr>
<tr>
<td>Paula Wood</td>
<td>Public Services Supervisor, Library Circulations</td>
</tr>
<tr>
<td>Stephanie Yule</td>
<td>Director, Risk Management and Business Services</td>
</tr>
</tbody>
</table>
STATEMENT OF INTERNAL CONTROLS

A. INTRODUCTION

Internal accounting and related operational controls established by the State of California, the CSU 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 which 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 record keeping 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.
September 6, 2002

Mr. Larry Mandel
University Auditor
The California State University
401 Golden Shore
Long Beach, CA 90802-4210

Dear Larry:

The current status of the FISMA Audit report #02-01 recommendations is outlined below. The original audit findings and campus responses have been included for ease of reference.

CASH RECEIPTS

Recommendation 1

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

Campus Response

We concur. We will implement procedures to periodically search for unauthorized bank accounts at local banks.

Anticipated Completion Date: November 2002

INFORMATION TECHNOLOGY

DISASTER RECOVERY PLAN

Recommendation 2

We recommend that the campus:

a. Enhance the IT DRP by adding detailed procedures for all sections outlined in SAM, develop campus business continuity plans to sustain operations during an extended outage of data processing services, and
add an assumptions list that should be shared with the business users to enhance their understanding of what services will and will not be restored as part of the IT recovery plan and that reflects the status of data files at the time of restoration.

b. Conduct a business impact assessment to determine the maximum length of time that the departments could operate without data processing services and identify the equipment and information that would be needed to sustain operations during an outage of data processing services.

c. Develop written manual operating and recovery procedures for business units to assist operations during an extended outage of data processing services, such as recreation of up to one week of lost data and procedures for entering data collected manually during a prolonged system outage.

d. Determine if only weekly off-site storage of tapes, which represents a potential loss of up to one week's worth of data, is sufficient to adequately recover campus business operations. Consider more frequent off-site storage during critical processing times such as online registration.

Campus Response

CSU Chico recognizes the deficiencies in the existing DRP and will enhance the plan using the recommendations as a guide in developing more comprehensive recovery processes and procedures. A project lead will be assigned by September 1st; the development of the project plan and identification of project team members will begin in September. Though a comprehensive DRP is recognized as essential to the timely and successful recovery from a catastrophic disaster, this planning effort will take a substantial amount of time.

Anticipated Completion Date: June 2003

MAINFRAME SECURITY

Recommendation 3

We recommend that the campus:

a. Activate the aforementioned RACF settings regarding tape data set protection, protect all, and batch and online job submission.
b. Revoke inactive IDs automatically and require passwords to be changed every 90 days or less.

c. Change the password on the RVARY command.

d. Change the universal access code setting to NONE for sensitive SYS1 libraries in order to reduce the risk of disclosure of system security settings and unauthorized access to powerful system libraries.

Campus Response

a. The RACF settings are being implemented one at a time, starting with Protect All. We do expect process failures. We have chosen this phased approach to minimize the number of process failures at any given time, to minimize the confusion on the cause of process failures, and to minimize the impact on limited technical staff time resources.

Anticipated Completion Date: December 2002

b. Inactive IDs will be automatically revoked after 180 days. The password change policy will be changed from 180 days to 90 days.

Anticipated Completion Date: October 2002

c. The password has been changed on the RVARY command.

Anticipated Completion Date: Completed

d. The universal access code setting for sensitive SYS1 libraries is included in the phased approach for implementing the RACF settings. As noted, the expected completion date is no later than December 31, 2002.

Anticipated Completion Date: December 2002

PROGRAM CHANGE CONTROL

Recommendation 4

We recommend that if the campus cannot effectively restrict all programmers from update access to production copies of programs and data, then a detective control reflecting programs that have been changed should be produced and reviewed by management on a regular basis, and access to data should not be allowed without specific written authorization from management.
Campus Response

All programmers must have the capability to make changes to production programs. Chico does not have the technical staff resources to do otherwise. To date, we have not been able to devise an automated detective control that will notify management when a program or data has been changed by technical staff. We understand the basis for the recommendation however, and will implement a manual control by logging all program changes (program ID, change request identifier, programmer, date changed) for comparison to standard source library directory information (program ID, date of change, and user ID used by individual making the change). This process will be implemented in September 2002.

Anticipated Completion Date: Completed

DATA CENTER ACCESS

Recommendation 5

We recommend that the campus complete the project to install a more restrictive physical security mechanism that will allow the computer services department to appropriately restrict access to the data center to only authorized personnel, which should be limited to the operators and a few key personnel.

Campus Response

The electronic card access project has been implemented.

Anticipated Completion Date: Completed

If you have any questions regarding the above responses, please let us know.

Sincerely,

Dennis C. Graham
Vice President for Business and Finance

cc: Manuel A. Esteban
    George Wellman
    Debbie McElroberts
    Bill Jones
September 25, 2002

MEMORANDUM

TO: Mr. Larry Mandel
    University Auditor

FROM: Charles B. Reed
      Chancellor

SUBJECT: Draft Final Report Number 02-01 on FISMA,
         California State University, Chico

In response to your memorandum of September 25, 2002, I accept the response
as submitted with the draft final report on FISMA, California State University,
Chico.

CBR/ac

Enclosure

cc: Dr. Manuel A. Esteban, President
    Mr. Dennis C. Graham, Vice President for Business and Finance