

**INFORMATION SECURITY**  
**SAN FRANCISCO STATE UNIVERSITY**

**Audit Report 08-22**  
**September 3, 2009**

---

**Members, Committee on Audit**

Melinda Guzman, Chair  
Raymond W. Holdsworth, Vice Chair  
Herbert L. Carter    Carol R. Chandler  
Kenneth Fong    Margaret Fortune  
George G. Gowgani    William Hauck  
Henry Mendoza

---

**Staff**

University Auditor: Larry Mandel  
Senior Director: Michelle Schlack  
IT Audit Manager: Greg Dove

---

**BOARD OF TRUSTEES**  
**THE CALIFORNIA STATE UNIVERSITY**

---

## CONTENTS

Executive Summary .....	1
Introduction.....	3
Background .....	3
Purpose.....	4
Scope and Methodology .....	6

---

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance.....	8
Information Security Plan .....	8
Information Security Organization .....	8
Employee Separation .....	9
Decentralized Computing .....	10
Server Environments.....	10
Incident Response .....	11
Server Management .....	12
Technical Vulnerabilities.....	13
E-Mail Systems .....	14
System Development and Change Management .....	15
Web Application Development and Maintenance .....	15
Web Application Vulnerabilities .....	16
Systems Security and Monitoring.....	16
Threat Management .....	16
Configuration Changes .....	17
Granting of Administrative Access.....	18
Routing and Switching Devices.....	19
Network Access .....	19
Password Standards .....	20
Vulnerability Management .....	21
Network Architecture .....	21
Protected Data.....	22

## **APPENDICES**

APPENDIX A:	Personnel Contacted
APPENDIX B:	Campus Response
APPENDIX C:	Chancellor's Acceptance

---

## **ABBREVIATIONS**

AD	Active Directory
CSU	California State University
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITRP	Infrastructure Terminal Resources Project
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol

---

## EXECUTIVE SUMMARY

As a result of a systemwide risk assessment conducted by the Office of the University Auditor, the Board of Trustees, at its January 2008 meeting, directed that *Information Security* be reviewed. The Office of the University Auditor had not previously reviewed *Information Security* as a separate subject area audit.

We visited the San Francisco State University campus from September 22, 2008, through November 7, 2008, and audited the procedures in effect at that time.

Our study and evaluation identified issues that, if left unattended, could continuously impact the overall control environment. We identified a series of problems that were listed individually in this report; however, the underlying root cause of many of the problems identified was the overall organization of information technology (IT) services using a decentralized campus computing environment that was not consistently managed in the same professional manner as the services provided by the campus IT department.

In our opinion, the operational and administrative controls of information security in effect as of November 7, 2008, taken as a whole, were not sufficient to meet many of the objectives for a secured computing environment. While much of the campus IT department control environment was satisfactory and provided appropriate safeguards over the critical financial and student systems, the decentralized computing environments that were not under the purview of campus IT require significant improvement and management oversight.

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.

Our audit did not examine all aspects of information security, but was designed to assess the controls over management, increase awareness, and recommend implementation for significant security topics that are prevalent in the California State University computing environment.

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

### SECURITY GOVERNANCE [8]

The campus information security plan did not include projected timelines for addressing information security issues. The campus committees that address information security lacked the necessary structure to ensure the deployment, implementation, control, and project reporting of information security committee objectives. Employee separation documentation did not include a reminder to the separating parties of their ongoing legal responsibility for maintaining the security of protected data.

## **DECENTRALIZED COMPUTING [10]**

Decentralized departmental and college server environments that contained protected data were not always adequately secured and had user accounts that were not properly utilized or maintained. Further, decentralized departmental and college IT personnel did not consistently report security events and incidents to a centralized security office. In addition, decentralized departmental and college server environments lacked policies and guidance for server management. Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the campus IT team and were not held to the same programming standard, code review, or security configuration standards. The campus had not developed policies and procedures for the multiple e-mail systems used by decentralized departments.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [15]**

Change management procedures for application development did not ensure adequate documentation of approval, testing, and user acceptance; appropriately limit developer abilities; adequately secure applications from known vulnerabilities; and coordinate application security acceptance with the information security officer. Further, web application vulnerabilities existed on the website selected for testing.

## **SYSTEM SECURITY AND MONITORING [16]**

The campus did not actively monitor intrusion security events. Policies and procedures had not been developed to address the periodic review and approval of configuration changes for systems and devices and the granting and management of privileged access to accounts. Routing and switching devices were not always properly configured or adequately secured, and the campus did not adequately secure the campus local area network. The campus password policy and password settings were not enforced and extended to all departments and systems on campus. The campus lacked a standard process to detect and remediate vulnerabilities. Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources.

## **PROTECTED DATA [22]**

The campus could not provide evidence documenting the deletion of protected data from campus computers, and the campus asset management system did not track the disposition of computers procured for under \$1,000.

---

## INTRODUCTION

### **BACKGROUND**

State Administrative Manual Section 5300 states that information security means the protection of information and information systems, equipment, and people from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and availability of information regardless of its form (electronic, print, or other media) is critical to ensure business continuity and protection against unauthorized access, use, disclosure, disruption, modification, or destruction. Pursuant to Government Code Section 11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, procedures, and filing requirements issued by the Office of Information Security and Privacy Protection, California Office of Information Security.

The California State University (CSU) *Information Security Policy*, dated August 2002, states that the Board of Trustees of the CSU is responsible for protecting the confidentiality of information in the custody of the CSU; the security of the equipment where this information is processed and maintained; and the related privacy rights of the CSU students, faculty, and staff concerning this information. It is also the collective responsibility of the CSU, its executives, and managers to ensure:

- ▶ The integrity of the data.
- ▶ The maintenance and currency of the applications.
- ▶ The preservation of the information in case of natural or manmade disasters.
- ▶ Compliance with federal and state regulations, including intellectual property and copyright.

The *Information Security Policy* further 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 and/or that contain mission critical data, including departmental, divisional, and other ancillary systems and equipment.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) published an information security standard in 2005 as ISO/IEC 17799:2005 *Information Technology - Security Techniques - Code of Practice for Information Security Management*. This standard was subsequently renumbered as ISO/IEC 27002:2005 in July 2007 in order to bring it into line with the other ISO/IEC 27000-series standards, also known as the Information Security Management System (ISMS) Family of Standards. The ISMS Family of Standards comprises information security standards published jointly by the ISO and the IEC.

The CSU contracted with Unisys in 2006 to perform a series of on-site Information Security Assessment Reviews at nine campuses and the chancellor's office. This assessment was designed to perform a basic review of CSU information security as benchmarked against the industry-accepted standard, ISO 17799:2005, as well as all applicable state and federal laws.

The CSU also contracted with CH2MHill in 2007 for the development of comprehensive information security policies and standards. These policies and standards address the following areas: information security roles and responsibilities; risk management; acceptable use; personnel security; privacy; security awareness and training; third-party services security; information technology (IT) security; configuration management and change control; access control; asset management; management of information systems; information security incident management; physical security; business continuity and disaster recovery; and legal and regulatory compliance. The Information Technology Advisory Committee, composed of the chief information officers from each campus, and the Information Security Advisory Committee, composed of the information security officers from each campus, was integrally involved in this policy development process in order to ensure that the final product was an appropriate fit for the CSU. This project began in September 2007 with the expectation that these policies and standards were to be completed by August 2008 for subsequent adoption and official systemwide distribution in late 2008. This timeline has now been extended an additional six months. Due to the pending status of this project during the time frame of the information security audits, these policies and standards were not used for evaluation of the campuses information security posture.

At San Francisco State University, the information technology security office is responsible for establishing information security policies, procedures, and an information security plan. The office also serves as a central point of contact and provides technical security support and network security services. However, a significant level of technology decentralization exists, and the overall responsibility for the management of many campus systems resides with the departmental IT managers, who are independent of the campus IT department.

### **PURPOSE**

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration of information security and to determine the adequacy of controls over the related processes to evaluate adherence to an industry-accepted standard, ISO 17799/27002, *Code of Practice for Information Security Management*, and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

Within the overall audit objective, specific goals included determining whether:

- ▶ Certain essential administrative and managerial internal controls are in place, including delegations of authority and responsibility, formation of oversight committees, executive-level reporting, and documented policies and procedures.
- ▶ A management framework is established to initiate and control the implementation of information security within the organization; and management direction and support for information security is communicated in accordance with business requirements and relevant laws and regulations.

- ▶ All assets are accounted for and have a nominated owner/custodian who is granted responsibility for maintenance and control to achieve and maintain appropriate protection of organizational assets; and information is appropriately classified to indicate the need, priorities, and expected degree of protection when handling the information.
- ▶ Security responsibilities are addressed prior to employment so that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work; and procedures are in place to ensure that users' separation from the organization is managed and that the return of all equipment and the removal of all access rights are completed.
- ▶ Responsibilities and procedures for the management of information processing and service delivery are defined; and technical security controls are integrated within systems and networks.
- ▶ Access rights to networks, systems, applications, business processes, and data are controlled based on business and security requirements by means of user identification and authentication.
- ▶ Formal event reporting and escalation procedures are in place for information security events and weaknesses; and communication is accomplished in a consistent and effective manner, allowing timely corrective action to be taken.
- ▶ The design, operation, use, and management of information systems are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.
- ▶ Web application development and change management processes and procedures are adequate to ensure that application security and accessibility is considered during the design phase, testing includes protection against known vulnerabilities, and production servers are adequately protected.
- ▶ E-mail systems are properly configured and managed so 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 a central location to facilitate campus-wide communications.
- ▶ The operational security of selected operating systems is adequate to prevent the exploitation of vulnerabilities on the internal network by individuals who gain access to it from dial-in connections, the Internet, and hosts on the internal network.
- ▶ The Internet firewall system is sufficient to identify and thwart attacks from the external Internet and filter unwanted network traffic.
- ▶ Selected routing and switching devices are properly managed and configured to effectively provide the designated network security or traffic controls.
- ▶ Systems connected to the Internet do not make publicly available any information that may provide enticement to penetrate the Internet gateway.

- ▶ Web application vulnerabilities that provide the potential for an unauthorized party to subvert controls and gain access to critical and proprietary information, use resources inappropriately, interrupt business, or commit fraud are identified and addressed.

## **SCOPE AND METHODOLOGY**

The proposed scope of the audit, as presented in Attachment B, Audit Agenda Item 2 of the January 22-23, 2008, meeting of the Committee on Audit, stated that information security would include reviewing the systems and managerial/technical measures for ongoing evaluation of data/information collected; identifying confidential, private, or sensitive information; authorizing access; securing information; detecting security breaches; and evaluating security incident reporting and response. Information security includes the activities/measures undertaken to protect the confidentiality, integrity, and access/availability of information, including measures to limit collection of information, control access to data and ensure that individuals with access to data do not utilize the data for unauthorized purposes, encrypt data in storage and transmission, and implement physical and logical security measures for all data repositories. Potential impacts include inappropriate disclosures of information; identity theft; adverse publicity; excessive costs; inability to achieve institutional objectives and goals; and increased exposure to enforcement actions by regulatory agencies.

In addition to the interviews and inquiry procedures affecting the operation and support of the network devices reviewed by the Office of the University Auditor, we also contracted with KPMG to perform a technical security assessment that included running diagnostic software designed to identify improper configuration of selected systems, servers, and network devices. The purpose of the technical security assessment was to determine the effectiveness of technology and security controls governing the confidentiality, integrity, and availability of selected campus assets. The assessment contained an internal component (within the campus network) and an external component (via the Internet) while encompassing a review of the security standards and processes that govern the San Francisco State University campus. Specifically, this configuration testing included assessment of the following technologies:

- ▶ Selected operating system platforms.
- ▶ Border firewall settings.
- ▶ Selected routing and switching devices.
- ▶ Internet footprint analysis.
- ▶ Website vulnerability assessment.

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 operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the internal administrative, compliance, and operational/technical controls over the management of information security. Specifically, we reviewed and tested:

- ▶ Information security policies and procedures.
- ▶ Information security organizational structure and management framework.
- ▶ Information asset management accountability and classification.
- ▶ Human resources security responsibilities.
- ▶ Administrative and technical security procedures, information processing, and service delivery.
- ▶ Access controls over networks, systems, applications, business processes, and data.
- ▶ Incident response, escalation, and reporting procedures.
- ▶ Compliance with relevant statutory, regulatory, and contractual security requirements.
- ▶ Web application security and applicable change management procedures.
- ▶ E-mail systems management and configuration.
- ▶ Operational security of selected operating system platforms.
- ▶ Security configurations of border firewall settings.
- ▶ Security configurations of selected routing and switching devices.
- ▶ Internet footprints of systems connected to the Internet.
- ▶ Website vulnerabilities stemming from exposures in the server's operating system, server administration practices, or flaws in the web application's programming.

Our testing and methodology was designed to provide a managerial level review of key information security practices, which included detailed testing of a limited number of network and computing devices. Our review did not examine all aspects of information security, selected emerging technologies were excluded from the scope of the review, and our testing approach was designed to provide a view of the security technologies used to protect only key computing resources.

---

# **OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES**

## **SECURITY GOVERNANCE**

### **INFORMATION SECURITY PLAN**

The campus information security plan did not include projected timelines for addressing information security issues.

The information security officer stated that unresolved budgetary issues had delayed the establishment of expected project completion dates.

Failure to establish timelines for campus compliance with the information security plan impacts the campus' ability to monitor progress toward providing security provisions related to protected data.

#### **Recommendation 1**

We recommend that the campus include projected timelines for achieving compliance in its information security plan.

#### **Campus Response**

We concur. The plan will be updated by January 2010 to show target start, deployment, and completion dates. The dates in the plan will be subject to change due to continuing state budget impacts and resource constraints.

### **INFORMATION SECURITY ORGANIZATION**

The campus committees that address information security lacked the necessary structure to ensure the deployment, implementation, control, and project reporting of information security committee objectives.

We found that:

- ▶ None of the committees had delegated authority for addressing and resolving information security issues.
- ▶ The committees were administered by various colleges rather than directed by the information security officer.
- ▶ Committee meeting minutes were not formal and did not include the assignment of responsibility for addressing security issues. The minutes also lacked documented action items and the disposition of items that were discussed in the meetings.

- ▶ Security incidents and project statuses were not consistently reported to the information security officer.

The information security officer stated that the various committees were already established to address information technology (IT) security as well as a structure for IT governance; however, there was continuing work for campus and executive staff to refine reporting committees and processes.

The lack of clearly defined roles and responsibilities for information security committees increases the risk that campus information security activities are not aligned with management intent, information security priorities are not properly established, and campus resources are not aligned to ensure that security risks are identified and addressed in a structured time frame.

### **Recommendation 2**

We recommend that the campus implement an effective structure for campus information security committees that includes:

- a. Formal delegation of authority for addressing and resolving information security issues.
- b. Administration of committee meetings by the information security officer.
- c. Formal minutes that document committee assignment and disposition of information security issues.
- d. Consistent reporting of security incidents to the information security officer.

### **Campus Response**

We concur. The recommendations related to information security committees and structure are part of a new campus IT governance structure which was in process at the time of the audit and will be implemented by March 2010. Formal delegation and the administration of committees will be addressed as well as the requirement for formal minutes and formal reporting.

## **EMPLOYEE SEPARATION**

Employee separation documentation did not include a reminder to the separating parties of their ongoing legal responsibility for maintaining the security of protected data.

The director of academic personnel/human resources management systems stated that the campus was unaware of any requirement to remind separated employees of their responsibility to uphold confidentiality agreements.

Failure to notify separating employees of their ongoing legal responsibility to maintain the security of protected data increases the risk of their non-compliance with statutory information security requirements for any remaining access to, or unauthorized custody of, protected data.

### **Recommendation 3**

We recommend that the campus include a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data.

#### **Campus Response**

We concur. Human resources will incorporate a reminder to separating employees by February 2010.

## **DECENTRALIZED COMPUTING**

### **SERVER ENVIRONMENTS**

Decentralized departmental and college server environments that contained protected data were not always adequately secured and had user accounts that were not properly utilized or maintained.

Our review disclosed that:

- ▶ One college stored sensitive student data on removable storage devices that were not tracked or encrypted.
- ▶ Departmental servers on the campus network were not always in compliance with campus policy for protecting sensitive data and for adequate security hardening.
- ▶ User accounts on departmental servers were not always in compliance with the campus password policy. We found that group accounts were used and that accounts for terminated employees were not consistently deleted.

The information security officer stated that the problems identified were due to some decentralized business units not consistently following campus policy and standards.

Inadequate security safeguards for server environments increase the risk that the campus network environment may be compromised, which could result in the inappropriate disclosure of protected data.

### **Recommendation 4**

We recommend that the campus implement monitoring controls to ensure that decentralized departmental and college server environments that contain protected data are adequately secured. Such controls should include, but not be limited to, provisions for tracking and encrypting removable storage devices, hardening the servers, assigning user accounts that comply with the campus password policy, and deleting accounts for terminated employees.

### **Campus Response**

We concur. The campus will continue to conduct surveys of decentralized departments for compliance by April 2010.

### **INCIDENT RESPONSE**

Decentralized departmental and college IT personnel did not consistently report security events and incidents to a centralized security office.

We found that:

- ▶ The existing decentralized help desk support process did not provide a method for the comprehensive collection and reporting of all security-related events and incidents.
- ▶ The existing decentralized process for reporting security incidents to the university police only addressed theft. It did not account for other security incidents that should be tracked and recorded by the information security officer, such as malware or spyware that must be removed from computers.

The information security officer stated that the lack of consistent reporting of security events was due to the campus having several decentralized IT environments with varied interpretations as to the severity and impact of security incidents.

Failure to ensure that information security incidents are effectively captured and monitored by a centralized entity weakens the campus security posture and increases the risk that compromised systems could inadvertently affect the campus network environment; it also decreases the campus' ability to analyze the causes of such incidents and to determine whether campus-wide solutions are warranted.

### **Recommendation 5**

We recommend that the campus implement a method to centrally collect information on all information security-related incidents and to ensure the adequacy of the remediation actions.

### **Campus Response**

We concur. We will implement a method to centrally collect information security incidents and periodically review the adequacy of remediation actions by February 2010.

## **SERVER MANAGEMENT**

Decentralized departmental and college server environments lacked policies and guidance for server management.

We found that:

- ▶ Some college IT support groups did not follow server security hardening standards.
- ▶ Server incident logs, including those for campus IT, were not retained and did not always capture all relevant security events; and log reviews were not consistently performed.
- ▶ Some decentralized IT support groups allowed widespread administrative level access to desktops and laptops and did not have sufficient mechanisms to ensure compliance with software licensing or ensure that installed applications did not violate campus policy or introduce security risks.
- ▶ The decentralized IT support groups maintained a plethora of local computer rooms but did not consistently provide sufficient adequate environmental controls for computing equipment. Some essential departmental servers were stored in staff offices.

The information security officer stated that the identified problems were due to some decentralized business units not consistently following campus policy and standards. She also stated that consistent review of logs was done by various departments and colleges under the current decentralized structure but was not always consistently implemented by all campus departments.

The lack of adequate security safeguards for server environments could compromise the campus network environment and result in the inappropriate disclosure of protected data.

### **Recommendation 6**

We recommend that the campus:

- a. Develop server management policies and guidance for decentralized departmental and college server environments. Such policies and guidance should include, but not be limited to, procedures to ensure that all servers are afforded sufficient security hardening; that server event logs are captured, retained and reviewed; and that administrative level access is granted only on an exception basis.
- b. Complete a risk assessment to identify essential departmental and college servers and place essential departmental and college servers in their respective computer rooms and ensure that those rooms include adequate physical and environmental controls.
- c. Perform and document periodic reviews of security event logs to assist in identifying potential network vulnerabilities and breaches of campus systems. These reviews should take into

consideration the use of tools and analytical methods and should define personnel responsibilities, reviewing frequency, and reporting/escalating processes.

### **Campus Response**

We concur. The campus will implement a policy to require that decentralized departments create and review their server security event logs on a routine basis by April 2010.

## **TECHNICAL VULNERABILITIES**

Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. These systems were not maintained by the campus IT team and were not held to the same programming standard, code review, or security configuration standards.

Our external testing of selected servers disclosed 72 vulnerabilities on a multitude of servers. We provided specific details of these vulnerabilities to the campus.

Additionally, the campus did not always adequately manage the deployment of servers in the decentralized computing environment, nor did it provide professional standards and guidance related to this deployment. The decentralized servers were not consistently patched, there was no baseline security standard for server security or application security, and professional application development standards and methodologies were absent or inadequate.

The information security officer stated that the departments and colleges had hired IT staff to manage and administer their IT assets and that they were responsible for patching and securing their systems.

Server vulnerabilities increase the risk of a remote attack on the server that could lead to server disablement, loss of protected confidential information, and the execution of malicious programs that could disable other network resources.

### **Recommendation 7**

We recommend that the campus repair all of the technical vulnerabilities that we identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Implement a comprehensive, centralized patch management process.
- b. Develop and implement a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This process would also include the review of web application code on existing enterprise delivery systems on a periodic basis to identify potential or known vulnerabilities.

- c. Develop and implement a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the de-centralized IT units with a baseline standard for securing servers prior to allowing them to become Internet-facing.

### **Campus Response**

We concur. The campus will require decentralized departments to demonstrate that they are routinely patching their systems; the information security officer will identify security baseline standards for web development, server security, and web application security; and require that decentralized departments demonstrate that they have deployed procedures in compliance with the identified standards by May 2010.

### **E-MAIL SYSTEMS**

The campus had not developed policies and procedures for the multiple e-mail systems used by decentralized departments.

The information security officer stated that the existence of multiple e-mail systems was primarily due to departmental and college desire for specific calendaring functionality.

The lack of policies and procedures for the administration of e-mail systems increases the risk that the various IT business units may not be performing leading security practices over spam and phishing and makes it more difficult to ensure emergency notification lists are current. Should the campus become involved in legal discovery proceedings, it may also risk being unable to recover e-mails because they have not been appropriately retained.

### **Recommendation 8**

We recommend that the campus develop and implement policies and procedures to address the administration of the e-mail systems used by decentralized departments.

### **Campus Response**

We concur. A new centralized campus-wide email system is in active deployment and will be fully deployed by March 2010. New policies have already been developed to address security and administration issues.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

### **WEB APPLICATION DEVELOPMENT AND MAINTENANCE**

Change management procedures for application development required improvement.

We noted the following deficiencies in our review of selected departments and colleges that perform some degree of application development:

- ▶ Written approval was not required for projects put into production.
- ▶ Testing criteria for the security of web applications was not documented.
- ▶ User acceptance was not documented.
- ▶ Programmers had unlimited access to source code.
- ▶ Processes for determining whether applications were adequately secured from known vulnerabilities prior to being moved into production were inconsistent.
- ▶ Application security acceptance was not coordinated with the information security officer.

The information security officer stated that the issues cited were due primarily to a decentralized environment and lack of funds to purchase automated testing tools to ensure compliance for web application development security. She also stated that a campus-wide change management process to help elevate and provide visibility of all development activities was underway.

The lack of a formal process for software development increases the risk of unapproved software development and introduction of unknown security risks to the campus network environment.

#### **Recommendation 9**

We recommend that the campus develop and implement a process for centralized oversight to ensure that departmental IT managers implement a formal change management process for software development for critical applications and systems containing level one protected data.

#### **Campus Response**

We concur. The division of information technology will issue guidance on application development and verify that decentralized IT departments have implemented procedures to adhere to the campus guidelines for web application development and deployment by June 2010.

## **WEB APPLICATION VULNERABILITIES**

Web application vulnerabilities existed on the website selected for testing.

The web application we reviewed allowed TRACE and TRACK methods, password auto complete in the browser for user credential, and cross-site scripting.

The information security officer stated that these vulnerabilities were caused by the lack of funds to purchase testing tools and implement a campus-wide automated patch management solution.

Web application vulnerabilities increase the risk that a remote attacker may be able to access protected confidential information or execute malicious programs on the server that could disable additional network resources.

### **Recommendation 10**

We recommend that the campus repair the one website with vulnerabilities that we identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Develop and implement a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This process would also include the review of web application code on existing enterprise delivery systems on a periodic basis to identify potential or known vulnerabilities.
- b. Implement a comprehensive, campus-wide patch management process.

### **Campus Response**

We concur. We will remediate the vulnerabilities identified by obtaining an attestation from the responsible department by February 2010. The information security officer will request that the decentralized departments verify that they are in compliance with campus practices for testing web applications for vulnerabilities by June 2010.

## **SYSTEMS SECURITY AND MONITORING**

### **THREAT MANAGEMENT**

The campus did not actively monitor intrusion security events.

We found that network devices were not configured to automatically respond to network security events by restricting or blocking traffic from potential threats. In addition, the campus had not

performed an assessment to determine if approved modems that operate on analog phone lines were properly secured.

The information security officer stated that server-based intrusion detection had not been implemented due to budget and resource constraints and the postponement of a systemwide solution from the chancellor's office. She also stated that tools for automated testing of modems were also impacted by the same budgetary constraints.

Inadequate procedures for the monitoring of, and response to, security incidents increase the risk of loss and inappropriate use of state resources and also increase campus exposure to information security breaches. Unsecured modems can result in unauthorized access to network resources and could lead to unauthorized access to protected data.

### **Recommendation 11**

We recommend that the campus implement an intrusion detection system to monitor and respond to potential security threats and that it assess all campus modem usage for adequate security.

### **Campus Response**

We concur. The campus will implement a level of monitoring and review of potential intrusions to the campus network by May 2010. The campus will implement an internal process for the review of analog line requests and their use to connect modems by May 2010.

## **CONFIGURATION CHANGES**

Policies and procedures had not been developed to address the periodic review and approval of configuration changes for systems and devices.

Specifically, policies and procedures did not address:

- ▶ Firewalls.
- ▶ Switches.
- ▶ Routers.
- ▶ Server/operating systems.

We noted that periodic reviews of these systems and devices informally occurred at regular intervals as part of network operational responsibilities; however, this informal process was not adequate to ensure that these network devices adhered to the latest configuration standards and updates.

The information security officer stated that the campus had implemented the systemwide change management standard for all network devices except campus-wide servers and operating systems, and that the campus was in the process of implementing a campus-wide change management template and process.

The lack of formal policies and procedures for reviewing system and device configuration changes decreases accountability for changes made to critical assets and increases the risk of inconsistent and deprecated configuration standards, both of which may permit malicious activity to go undetected.

### **Recommendation 12**

We recommend that the campus:

- a. Develop policies and procedures and also establish a formal process for the periodic review of system configuration changes that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.
- b. Incorporate into these change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance of configuration reviews.

### **Campus Response**

We concur. The campus will require that the decentralized IT departments are following campus guidance by attesting that they have a formal sign-off process by May 2010. We have already implemented the ITRP-approved change management processes and formal sign-off process for network devices.

## **GRANTING OF ADMINISTRATIVE ACCESS**

Policies and procedures had not been developed to address the granting and management of privileged access to accounts.

The information security officer stated that the cause is primarily a desire by decentralized departments and colleges to have their own oversight of account administration.

The lack of policies and procedures for the granting and management of privileged access may lead to inadequate segregation of duties or failure to follow the principle of least privilege in the granting of access to accounts.

### **Recommendation 13**

We recommend that the campus develop and document policies and procedures to address the granting and management of privileged access to accounts. The campus should also develop and implement a procedure to track, review, and periodically audit this type of access.

### **Campus Response**

We concur. To improve oversight, the campus will issue guidelines for decentralized departments to implement practices that incorporate periodic review of privileged access (i.e., system administrator access) by April 2010.

## **ROUTING AND SWITCHING DEVICES**

Routing and switching devices were not always properly configured or adequately secured. The specific vulnerabilities identified have been provided to the campus separately.

The senior director of network and operations stated that many network devices were old and did not currently support the recommended upgrades. He also stated that the campus is dependent on the systemwide network project to achieve the requested functionality and security.

These configuration and security vulnerabilities increase the risk that a remote attacker may be able to gain access to network resources, compromise protected confidential information, or execute malicious programs on the server that could disable additional network resources.

### **Recommendation 14**

We recommend that the campus repair all of the network device vulnerabilities that we identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the live network environment to identify potential or known vulnerabilities.
- c. Develop procedures for ensuring ongoing compliance with the campus patch management process for all machines that have access to internal network resources.

### **Campus Response**

We concur. We will establish a basic security baseline configuration standard that includes patch management for network devices and obtain attestations from individual departments by February 2010. Achieving enhanced security capabilities will be dependent on ITRP funding.

## **NETWORK ACCESS**

The campus did not adequately secure the campus local area network (LAN).

We found that the campus permitted automatic wired access via any operable Ethernet jack to any machines without requiring registration or confirmation of adequate security updates. In addition, user authentication was not required; consequentially, users could access normally protected areas of the campus internal network.

The information security officer stated that limited campus resources prevented the campus from implementing true network access control.

Inadequate control over access to the campus network increases the risk of loss and inappropriate use of state resources and increases campus exposure to information security breaches.

#### **Recommendation 15**

We recommend that the campus develop and implement a plan to require user authentication prior to granting access to the LAN network or implement mitigating controls that prevent unauthorized users from connecting to the network.

#### **Campus Response**

We concur. We already require authentication on our wireless network and will develop a plan to implement similar capabilities on our wired network to prevent and monitor users connected to the network by February 2010.

### **PASSWORD STANDARDS**

The campus password policy and password settings were not enforced and extended to all departments and systems on campus.

We noted that applications that do not authenticate via the Active Directory (AD) domain or through the Lightweight Directory Access Protocol (LDAP) do not always include effective password controls.

The information security officer stated that the campus had guidance on password standards and was changing the provisioning and de-provisioning of privileged user access into a centrally managed model, and that not all campus applications yet authenticate to LDAP or AD because many maintain decentralized solutions and may desire to keep them.

The lack of a consistent password policy increases the risk that password parameters within campus systems will be insufficient, which could increase the risk of unauthorized access to network resources and confidential information.

#### **Recommendation 16**

We recommend that the campus implement monitoring controls to ensure that its existing password policy and password settings are enforced throughout the campus.

#### **Campus Response**

We concur. The division of information technology will obtain attestations that the decentralized IT units have turned on the password features of their respective environments by March 2010.

## **VULNERABILITY MANAGEMENT**

The campus lacked a standard process to detect and remediate vulnerabilities.

We noted that:

- ▶ There was no formal process to ensure that vulnerabilities detected through individual department scans were appropriately addressed and resolved. While documentation existed on the handling of various vulnerabilities, this process was decentralized and was not consistent across the campus.
- ▶ Departments were not consistently performing periodic vulnerability scans.
- ▶ Incident management procedures for the various colleges and departments were not adequate to ensure that all vulnerabilities were reported to the campus information security officer.

The information security officer stated that department and college server administrators were responsible for performing their own scans and for patching systems, and that reporting of specific campus vulnerabilities was being done on a voluntary basis.

Failure to detect and remediate vulnerabilities may lead to compromised network resources and loss of protected confidential information, while the lack of centralized reporting and tracking could result in a delay in identifying and resolving campus-wide problems.

### **Recommendation 17**

We recommend that the campus develop a plan to detect and remediate vulnerabilities on all machines connected to the campus network and that it implement a process for the centralized collection and reporting of vulnerabilities.

### **Campus Response**

We concur. We will develop a plan for the ongoing detection, centralized reporting, and remediation of vulnerabilities of all machines on the network by June 2010.

## **NETWORK ARCHITECTURE**

Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources.

Normally, Internet-accessible devices are segmented into a demilitarized zone so that if these devices are compromised, they are separated from other internal network resources.

The information security officer stated that the campus had migrated to a server farm architecture where assets have the capability to be segmented by data level and function, but the migration of

department and college servers or of data to an alternate centralized business intelligence model was under review.

Inadequate segmentation of publicly accessible devices from internal resources increases the risk that compromised devices could be used to pivot to other network targets and launch attacks against internal resources.

### **Recommendation 18**

We recommend that the campus review its current network topology and determine if Internet-accessible devices should be logically separated from devices residing within the internal network.

### **Campus Response**

We concur. We will review the current network topology and determine the need for greater logical separation by February 2010.

## **PROTECTED DATA**

The campus could not provide evidence documenting the deletion of protected data from campus computers, and the campus asset management system did not track the disposition of computers procured for under \$1,000.

The campus' policy stated that the hard drives on all computers and laptops should be wiped clean prior to their disposition. However, we found that each division/college had separate processes for wiping hard drives and that these processes did not require documentation. Moreover, since the campus tracks only computers that were procured for over \$1,000, there was no assurance that the hard drives on computers procured for less than \$1,000 were properly wiped prior to their disposition.

The information security officer stated that the campus had a process for wiping the hard drives of all computers using industry-approved software when those computers were disposed of or re-deployed or physical destruction when they were routed to the recycle stream, but that it did not require formal documentation of this practice.

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

**Recommendation 19**

We recommend that the campus:

- a. Revise its current policy for asset disposal to include documented evidence that the hard drives on division/college equipment are properly wiped prior to disposal.
- b. Implement procedures to track and monitor all computers and mass storage devices that are subject to disposal or recycling.

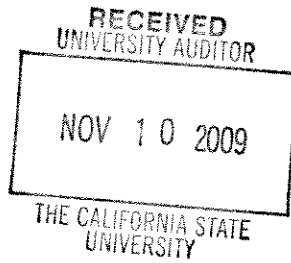
**Campus Response**

We concur. We will update our existing Property Survey Request Form to capture detail regarding disposal such as an attestation by the user/department that they used a campus-approved destruction and/or trusted overwrite method described in campus policy by January 2010.

---

## APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Robert A. Corrigan	President
Sheldon Axler	Dean, College of Science and Engineering
Tina Easter	System Administrator, College of Science and Engineering
Mig Hoffman	Information Security Officer
John Kim	Associate Vice President, Academic Resources
Phoebe Kwan	Director, Computing Services
Franz Lozano	University Budget Officer
Henry McCoy	Director, Academic Personnel/ Human Resources Management Systems
Leroy M. Morishita	Vice President, Administration and Finance
Mark Osborne	Interim Internal Audit (At time of review)
Jon Rood	Chief Information Officer
Alastair Smith	Director, Student Health
Don Taylor	Dean, College of Health and Human Services
Jack Tse	Senior Director, Network and Operations Management
Jo Volkert	Associate Vice President, Enrollment Management
Larry Ware	Associate Vice President, Fiscal Affairs



OFFICE OF THE PRESIDENT

1600 Holloway Avenue  
San Francisco, CA 94132

phone: 415/338-1381

fax: 415/338-6210

web: www.sfsu.edu

November 9, 2009

Mr. Larry Mandel  
University Auditor  
The California State University  
401 Golden Shore  
Long Beach, California 90802-4275

Dear Mr. Mandel:

We have reviewed the Office of the University Auditor Report #08-22 on Information Security at San Francisco State University. Our revised responses to the recommendations are attached which will also be forwarded to your staff electronically. We are taking actions to implement the recommendations.

Questions regarding the responses may be directed to Leroy M. Morishita, Executive Vice President and CFO for Administration & Finance, at 415/338-2521 or Mark Osborne or Franz Lozano in Internal Audit at 415/338-2763.

Sincerely,

A handwritten signature in black ink, appearing to read "Robert A. Corrigan".

Robert A. Corrigan  
President

MO/FL/id

Attachments

cc: Leroy M. Morishita, Executive Vice President and CFO, Administration & Finance  
Jonathan Rood, CIO & Associate Vice President Division of Information Technology  
Phoebe Kwan, Executive Director, Division of Information Technology  
K. Mig Hofman, Information Security Officer, Division of Information Technology  
Jack Tse, Senior Director, Network and Operations Management, DOIT  
Agnes Wong Nickerson, Interim Associate Vice President, Fiscal Affairs  
Mark Osborne, Interim Internal Auditor

**INFORMATION SECURITY**  
**SAN FRANCISCO STATE UNIVERSITY**  
**Audit Report 08-22**

**SECURITY GOVERNANCE**

**INFORMATION SECURITY PLAN**

**Recommendation 1**

We recommend that the campus include projected timelines for achieving compliance in its information security plan.

**Campus Response**

We concur. The plan will be updated by January 2010 to show target start, deployment and completion dates. The dates in the plan will be subject to change due to continuing state budget impacts and resource constraints.

**INFORMATION SECURITY ORGANIZATION**

**Recommendation 2**

We recommend that the campus implement an effective structure for campus information security committees that includes:

- a. Formal delegation of authority for addressing and resolving information security issues.
- b. Administration of committee meetings by the information security officer.
- c. Formal minutes that document committee assignment and disposition of information security issues.
- d. Consistent reporting of security incidents to the information security officer.

**Campus Response**

We concur. The recommendations related to Information Security committees and structure are part of a new campus IT Governance structure which was in-process at the time of the audit and will be implemented by March 2010. Formal delegation and the administration of committees will be addressed as well as the requirement for formal minutes and formal reporting.

## **EMPLOYEE SEPARATION**

### **Recommendation 3**

We recommend that the campus include a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data.

### **Campus Response**

We concur. HR will incorporate a reminder to separating employees by February 2010.

## **DECENTRALIZED COMPUTING**

### **SERVER COMPUTING ENVIRONMENTS**

#### **Recommendation 4**

We recommend that the campus implement monitoring controls to ensure that decentralized departmental and college server environments that contain protected data are adequately secured. Such controls should include, but not be limited to, provisions for tracking and encrypting removable storage devices, hardening the servers, assigning user accounts that comply with the campus password policy, and deleting accounts for terminated employees.

#### **Campus Response**

We concur. The campus will continue to conduct surveys of decentralized departments for compliance by April 2010.

### **INCIDENT RESPONSE**

#### **Recommendation 5**

We recommend that the campus implement a method to centrally collect information on all information security-related incidents and to ensure the adequacy of the remediation actions.

#### **Campus Response**

We concur. We will implement a method to centrally collect information security incidents and periodically review the adequacy of remediation actions by February 2010.

### **SERVER MANAGEMENT**

#### **Recommendation 6**

We recommend that the campus:

- a. Develop server management policies and guidance for decentralized departmental and college server environments. Such policies and guidance should include, but not be limited to, procedures to ensure that all servers are afforded sufficient security hardening;

that server event logs are captured, retained and reviewed; and that administrative level access is granted only on an exception basis.

- b. Complete a risk assessment to identify essential departmental and college servers and place essential departmental and college servers in their respective computer rooms and ensure that those rooms include adequate physical and environmental controls.
- c. Perform and document periodic reviews of security event logs to assist in identifying potential network vulnerabilities and breaches of campus systems. These reviews should take into consideration the use of tools and analytical methods and should define personnel responsibilities, reviewing frequency, and reporting/escalating processes.

### **Campus Response**

We concur. The campus will implement a policy to require that decentralized departments create and review their server security event logs on a routine basis by April 2010.

## **TECHNICAL VULNERABILITIES**

### **Recommendation 7**

We recommend that the campus repair all of the technical vulnerabilities that we identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Implement a comprehensive, centralized patch management process.
- b. Develop and implement a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This process would also include the review of web application code on existing enterprise delivery systems on a periodic basis to identify potential or known vulnerabilities.
- c. Develop and implement a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the de-centralized IT units with a baseline standard for securing servers prior to allowing them to become Internet-facing.

### **Campus Response**

We concur. The campus will require decentralized departments to demonstrate that they are routinely patching their systems; the ISO will identify security baseline standards for web development, server security and web application security; and require that decentralized departments demonstrate that they have deployed procedures in compliance with the identified standards by May 2010.

## **E-MAIL SYSTEMS**

### **Recommendation 8**

We recommend that the campus develop and implement policies and procedures to address the administration of the e-mail systems used by decentralized departments.

### **Campus Response**

We concur. A new centralized campus-wide email system is in active deployment and will be fully deployed by March 2010. New policies have already been developed to address security and administration issues.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

### **WEB APPLICATION DEVELOPMENT AND MAINTENANCE**

#### **Recommendation 9**

We recommend that the campus develop and implement a process for centralized oversight to ensure that departmental IT managers implement a formal change management process for software development for critical applications and systems containing level one protected data.

#### **Campus Response**

We concur. The Division of Information Technology will issue guidance on application development, and verify that decentralized IT departments have implemented procedures to adhere to the campus guidelines for web application development and deployment by June 2010.

### **WEB APPLICATION VULNERABILITIES**

#### **Recommendation 10**

We recommend that the campus repair the one website with vulnerabilities that we identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Develop and implement a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This process would also include the review of web application code on existing enterprise delivery systems on a periodic basis to identify potential or known vulnerabilities.
- b. Implement a comprehensive, campus-wide patch management process.

**Campus Response**

We concur. We will remediate the vulnerabilities identified by obtaining an attestation from the responsible department by February 2010. The ISO will request that the decentralized departments verify that they are in compliance with campus practices for testing web applications for vulnerabilities by June 2010.

**SYSTEMS SECURITY AND MONITORING**

**THREAT MANAGEMENT**

**Recommendation 11**

We recommend that the campus implement an intrusion detection system to monitor and respond to potential security threats and that it assess all campus modem usage for adequate security.

**Campus Response**

We concur. The campus will implement a level of monitoring and review of potential intrusions to the campus network by May 2010. The campus will implement an internal process for the review of analog line requests and their use to connect modems by May 2010.

**CONFIGURATION CHANGES**

**Recommendation 12**

We recommend that the campus:

- a. Develop policies and procedures and also establish a formal process for the periodic review of system configuration changes that will assist management with assigning accountability and responsibility for identifying potentially mis-configured network devices.
- b. Incorporate into these change management policies and procedures a formal sign-off process by appropriate campus personnel to ensure compliance of configuration reviews.

**Campus Response**

We concur. The campus will require that the decentralized IT departments are following campus guidance by attesting that they have a formal sign-off process by May 2010. We have already implemented the ITRP-approved change management processes and formal signoff process for network devices.

## GRANTING OF ADMINISTRATIVE ACCESS

### Recommendation 13

We recommend that the campus develop and document policies and procedures to address the granting and management of privileged access to accounts. The campus should also develop and implement a procedure to track, review, and periodically audit this type of access.

### Campus Response

We concur. To improve oversight, the campus will issue guidelines for decentralized departments to implement practices that incorporate periodic review of privileged access (i.e. system administrator access) by April 2010.

## ROUTING AND SWITCHING DEVICES

### Recommendation 14

We recommend that the campus repair all of the network device vulnerabilities that we identified and presented in detail to the campus.

In addition, we recommend that the campus:

- a. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the live network environment to identify potential or known vulnerabilities.
- c. Develop procedures for ensuring ongoing compliance with the campus patch management process for all machines that have access to internal network resources.

### Campus Response

We concur. We will establish a basic security baseline configuration standard that includes patch management for network devices and obtain attestations from individual departments by February 2010. Achieving enhanced security capabilities will be dependent on ITRP funding.

## NETWORK ACCESS

### Recommendation 15

We recommend that the campus develop and implement a plan to require user authentication prior to granting access to the LAN network or implement mitigating controls that prevent unauthorized users from connecting to the network.

**Campus Response**

We concur. We already require authentication on our wireless network and will develop a plan to implement similar capabilities on our wired network to prevent and monitor users connected to the network by February 2010.

**PASSWORD STANDARDS**

**Recommendation 16**

We recommend that the campus implement monitoring controls to ensure that its existing password policy and password settings are enforced throughout the campus.

**Campus Response**

We concur. The Division of Information Technology will obtain attestations that the decentralized IT units have turned on the password features of their respective environments by March 2010.

**VULNERABILITY MANAGEMENT**

**Recommendation 17**

We recommend that the campus develop a plan to detect and remediate vulnerabilities on all machines connected to the campus network and that it implement a process for the centralized collection and reporting of vulnerabilities.

**Campus Response**

We concur. We will develop a plan for the ongoing detection, centralized reporting and remediation of vulnerabilities of all machines on the network by June 2010.

**NETWORK ARCHITECTURE**

**Recommendation 18**

We recommend that the campus review its current network topology and determine if Internet-accessible devices should be logically separated from devices residing within the internal network.

**Campus Response**

We concur. We will review the current network topology and determine the need for greater logical separation by February 2010.

## PROTECTED DATA

### Recommendation 19

We recommend that the campus:

- a. Revise its current policy for asset disposal to include documented evidence that the hard drives on division/college equipment are properly wiped prior to disposal.
- b. Implement procedures to track and monitor all computers and mass storage devices that are subject to disposal or recycling.

### Campus Response

We concur. We will update our existing *Property Survey Request Form* to capture detail regarding disposal such as an attestation by the user/department that they used a campus-approved destruction and/or trusted overwrite method described in campus policy by January 2010.

  
**THE CALIFORNIA STATE UNIVERSITY**  
 OFFICE OF THE CHANCELLOR

BAKERSFIELD

December 9, 2009

CHANNEL ISLANDS

CHICO

**MEMORANDUM**

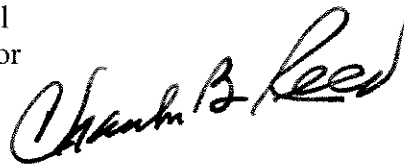
DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FROM: Charles B. Reed  
Chancellor



FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 08-22 on *Information Security*,  
San Francisco State University

LONG BEACH

LOS ANGELES

In response to your memorandum of December 9, 2009, I accept the response as submitted with the draft final report on *Information Security*, San Francisco State University.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

Enclosure

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS