

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**SACRAMENTO**

**Audit Report 09-36**  
**December 7, 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  
Senior Auditor: Alec Lu

---

**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
Security Organization .....	8
Information Security Awareness Training.....	9
Access Control .....	9
Decentralized Computing .....	11
Server Environments.....	11
Technical Vulnerabilities.....	13
System Development and Change Management .....	14
Web Application Development and Maintenance.....	14
Web Application Vulnerabilities .....	16
Systems Security and Monitoring .....	17
Configuration Changes .....	17
Control of User Access .....	18
Vulnerability Management .....	19
Application Control .....	20
Password Standards .....	21
Network Access .....	21
Granting of Administrative Access.....	22
Firewalls and Routing and Switching Devices .....	23
Network Architecture .....	24
Operating Systems Vulnerabilities .....	25
Review of Security Event Logs .....	26
Baseline Security Standards.....	27
Protected Data.....	27
Assessment and Inventory of Protected Information.....	27
Lost/Stolen Computers .....	28
Disposition of Protected Data.....	29
Incident Response Management .....	29

## **APPENDICES**

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

---

## **ABBREVIATIONS**

CMS	Common Management System
CSU	California State University
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
RDP	Remote Desktop Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
Telnet	Telecommunication Network

---

## 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 California State University, Sacramento campus from June 1, 2009, through July 10, 2009, 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. Also, the campus environment did not lend itself to timely creation and issuance of campus-wide IT policies.

In our opinion, the operational and administrative controls of information security in effect as of July 10, 2009, 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 was deficient in its ability to monitor and enforce campus-wide information security policies, procedures, and guidelines. Security awareness training had not been completed by all employees with access to campus information resources. The campus process for provisioning user computer accounts required improvement.

## **DECENTRALIZED COMPUTING [11]**

Administration of decentralized departmental server environments required improvement. Technical vulnerabilities existed on a variety of decentralized systems throughout the campus.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [14]**

Change management procedures for web application development required improvement. Web application vulnerabilities existed on the web application selected for testing.

## **SYSTEMS SECURITY AND MONITORING [17]**

The campus lacked policies and procedures that defined a formal periodic review of configuration changes. The administration of user access profiles required improvement. The administration of user access profiles required improvement. The management of campus vulnerabilities required improvement. The campus had not assessed the risk of local administrative accounts on their systems. The campus did not adhere to password best practices. Campus administration of wireless networks required improvement. The process for the granting and management of privileged system-level access to accounts required improvement. Firewalls and routing and switching devices in the central and decentralized program centers were not always properly configured or adequately secured. Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources. Technical vulnerabilities existed on selected operating systems. The campus lacked a formal process for the review of security event logs. The campus lacked a formal process to identify and monitor all IT resources on the campus network, and baseline security standards for the administration of decentralized servers and desktops had not been developed.

## **PROTECTED DATA [27]**

The campus had not recently completed a university-wide assessment to identify sensitive data on all servers and workstations. The campus lacked a formal process to ensure that lost/stolen computers were properly reported to the information security office to determine the disposition of sensitive information on computers and whether further action is required. The campus' process for ensuring that all sensitive information on computers and laptops was properly deleted required improvement. The campus' security incident handling procedures for compromised electronic resources required improvement.

---

## 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.

It 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 which 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. 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 California State University, Sacramento, the office of information technology services has overall responsibility for the management of campus systems and networks. However, a significant level of decentralization has shifted many critical IT responsibilities to ancillary departmental units throughout the campus.

## **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 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, that testing includes protection against known vulnerabilities, and that the 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 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 a review of 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 assure 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 retained contractors 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 CSU Sacramento 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**

### **SECURITY ORGANIZATION**

The campus was deficient in its ability to monitor and enforce campus-wide information security policies, procedures, and guidelines.

We noted that:

- ▶ Central information technology (IT) did not have a process in place to ensure that decentralized departments were in compliance with campus-wide security policies, procedures, and guidelines.
- ▶ The information security office issued security policies and procedures but relevant users either did not consistently follow these practices, did not know of these practices, or believed that these practices were not applicable to their areas.

The information security officer stated that both the central IT department and the chief information officer position at the campus were relatively new and that they had lacked clear lines of authority. He further stated that information security policies and procedures were recently adopted by the president and that the central IT team was focusing on other security initiatives and guidelines to meet best practices.

Failure to monitor and enforce campus-wide policies and standards limits the campus' ability to direct a comprehensive information security program. Such oversights increase the campus' exposure to security breaches and the risk of inappropriate use of computing resources.

#### **Recommendation 1**

We recommend that the campus improve its process to monitor and enforce campus-wide information security policies, procedures, and guidelines. An effective approach would be to require critical and business systems, including all network infrastructure, to be migrated and managed by central IT.

#### **Campus Response**

We concur with the recommendation regarding improvement of our ability to monitor and enforce information security policies and processes campus-wide. We will develop a campus-wide organizational and management structure for IT that ensures that the chief information officer and information security officer provide management and oversight to all aspects of the monitoring and enforcement of campus-wide information security. This reorganization of IT will provide for the recommended migration of all critical and business IT systems and network activity under the management of the campus-wide IT organization. We will also develop a policy giving the information security officer, under the authority of the chief information officer, all needed authority

for evaluation, enforcement, and implementation of all required information security policies and procedures campus-wide, including for auxiliary and self-support units. Both policy development and the reorganization of the management structure for IT will be completed by September 30, 2010.

## **INFORMATION SECURITY AWARENESS TRAINING**

Security awareness training had not been completed by all employees with access to campus information resources.

The information security officer stated that the campus had implemented security awareness training for employees with access to confidential systems and were waiting for the rollout of the systemwide training program to provide security awareness training to all employees.

Failure to provide employees with information security awareness training increases the risk of mismanagement of protected data, which increases the campus' exposure to security breaches and could compromise the campus' compliance with statutory information security requirements.

### **Recommendation 2**

We recommend the campus ensure that all employees with access to campus information resources complete information security awareness training.

### **Campus Response**

The campus concurs and will have the information security officer work with campus human resources to implement mandatory information security awareness training for all employees campus-wide, including those in auxiliary organizations. Continued special attention will be paid to IT and functional employees with access to confidential information. Training will be included in mandatory employee orientation programs no later than May 1, 2010, and will be provided or certified for existing employees no later than September 30, 2010.

## **ACCESS CONTROL**

The campus process for provisioning user computer accounts required improvement.

We noted the following deficiencies:

- ▶ The process did not ensure that access privileges of transferred employees were promptly changed to reflect only the new job responsibilities.
- ▶ The process did not ensure that individuals who had access through multiple roles within the university (i.e. staff, student, or faculty) had that access removed appropriately upon termination of each specific role.

- ▶ Users were not immediately deactivated from the campus active directory when employment ended.

The information security officer stated that access control had been a problem in the past and that the campus had mitigated some of the risks within critical systems like the Common Management Systems (CMS) with a monthly de-provisioning process, an annual review, and additional training. However, he also stated that the complexity of the computing environment had limitations that made it difficult to immediately deactivate all employee access upon termination.

Failure to remove the access of employees when their employment status changes increases the risk that users may retain access that is incompatible with their job functions.

### **Recommendation 3**

We recommend that the campus:

- a. Revise the current process to ensure that user privileges are modified or old access is deactivated for intracampus employee transfers.
- b. Develop a process that includes user provisioning and de-provisioning to ensure that access is granted, removed, or deactivated when employment status with the university changes.
- c. Immediately deactivate terminated employees from the active directory when they are no longer physically present on campus.

### **Campus Response**

The campus concurs and will implement a comprehensive and mandatory campus-wide identity management policy requiring campus-wide implementation and monitoring of all recommended access controls by a central identity management system, no later than September 30, 2010.

Specifically, we will:

- a. Ensure that all account creation and provisioning campus-wide is completed only under the authority of the central IT organization and the campus-wide information security officer, under the management of the centrally controlled identity management system.
- b. Have the central IT organization work with human resources to develop and implement a process to both identify intracampus employee transfers campus-wide and to modify/deactivate associated privileges in a timely manner using the central identity management system.
- c. Using the same process noted under item 3b, identify and implement a campus-wide process to identify all employment status changes and to remove/deactivate associated account privileges in a timely manner when appropriate.

- d. Using the same process noted under item 3b, implement a process to immediately deactivate the account privileges of employees on or before their last active work day at the university.

## **DECENTRALIZED COMPUTING**

### **SERVER ENVIRONMENTS**

Administration of decentralized departmental server environments required improvement.

Our review of various departments and colleges disclosed that:

- ▶ Backup copies of sensitive information were not encrypted nor were they stored off-site. The backup was done to nearby servers.
- ▶ Encryption had not been used for the storage of sensitive information on servers.
- ▶ Password standards did not meet best practices.
- ▶ Shared administrative accounts were used to manage departmental servers.
- ▶ Designated information technology professionals did not have complete oversight and authority for all equipment within their respective colleges.
- ▶ There was no formal process (e.g., data retention, standardized configuration, monitoring and review processes) in place to manage logs within program centers.
- ▶ Effective patch management processes were not in place to ensure that virus definitions and patches were current.
- ▶ Formal change management processes or procedures did not exist.

The information security officer stated that the decentralized nature of the campus computing environment and lack of staff resources contributed to these deficiencies.

Failure to effectively administer decentralized servers increases the risk that the servers may be compromised, resulting in potential loss of confidential data in the event of a security breach, and contributes to inefficient use of campus resources.

#### **Recommendation 4**

We recommend that the campus:

- a. Ensure that backups from decentralized servers containing sensitive data are properly encrypted and stored off-site.

- b. Encrypt desktop and/or laptop computer drives that contain sensitive information.
- c. Ensure that password standards meet a minimum security baseline.
- d. Comply with their policy to prohibit sharing of administrative accounts.
- e. Ensure that designated information technology professionals have appropriate authority and oversight over all equipment and technologies in the college computing environments.
- f. Develop formal log management procedures to ensure logs are retained and reviewed regularly.
- g. Ensure that patch management processes effectively keep virus definitions and patches current.
- h. Develop a formal change management process to ensure that changes to systems are tested, reviewed, and approved.

### **Campus Response**

We concur that the administration of Sacramento State's decentralized server environments requires significant improvement and also concur with the statement noted in the Executive Summary that "Establishing controls that would prevent all [the] limitations [of decentralized environments] would not be cost effective." We therefore fully concur with Recommendation #1 that an effective approach to mitigating these problems is to require that all critical and business systems be migrated and managed by central IT.

We will create and implement a policy and procedures requiring that all campus servers and network systems/devices be managed by and registered with the central IT organization by September 30, 2010. Oversight will be provided by the information security office staff to ensure compliance with all recommended information security policies and procedures and certification by senior IT management.

Specifically, the policy and procedures will ensure:

- a. Proper storage and encryption of all backups containing sensitive data campus-wide.
- b. Encryption of all sensitive information on servers and desktop and laptop computers campus-wide.
- c. Use of minimum campus-wide password policies for all computer and network access campus-wide.
- d. Non-sharing of administrative accounts and segregation and oversight of access where needed.
- e. Oversight by the chief information officer, information security officer and designees over all computer and network equipment and processes remaining in program center environments.

- f. Maintenance, retention, and review of all security logs as defined by university policy, with timely mitigation of problems required.
- g. Mandatory, comprehensive, and timely patch management and virus protection for all computer and network devices campus-wide.
- h. Comprehensive and mandatory change management processes for all computer and network devices, with formal review by the Information Security Officer or designees prior to deployment of all changes.

## **TECHNICAL VULNERABILITIES**

Technical vulnerabilities existed on a variety of decentralized systems throughout the campus. The central IT team did not maintain these systems and they were not held to the same programming standard and code review or security configuration standards.

Our external testing of selected servers disclosed 33 vulnerabilities on a variety of servers. We provided specific details of these vulnerabilities to the campus.

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

The information security officer stated that the lack of centralized IT oversight and direction had permitted the majority of these vulnerabilities to propagate in the decentralized computing environments.

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 5**

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This process would include the review of existing web

application code on a periodic basis or new code prior to deployment into the production environment to identify potential vulnerabilities.

- c. Develop a campus-wide application development standard with which all developers of Internet-facing applications for the campus must comply.
- d. Provide all the decentralized program centers with a security baseline standard for securing servers.

### **Campus Response**

The campus concurs and will repair all technical vulnerabilities identified and presented during the audit, by September 30, 2010. In addition, we will implement a policy requiring use of campus-wide monitoring and security management software to implement comprehensive patch management on all computer desktops, laptops, servers and other applicable computer and network devices. Utilizing the server management, registration, and compliance processes detailed in Recommendation #4, we will:

- Require identification of all vulnerable application code, periodic review of existing application code, and review of application vulnerability prior to code deployment.
- Develop, require compliance with, and monitor compliance with published application development standards.
- Develop policies requiring compliance with a set of minimum server and application security standards.

All of the above actions will be completed by September 30, 2010.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

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

Change management procedures for web application development required improvement.

We noted the following deficiencies in our review of selected campus departments that perform application development:

- ▶ Written approval was not required to move projects into production.
- ▶ Testing criteria for the security of web applications were not defined.
- ▶ User acceptance testing was not documented.
- ▶ Developers had unlimited access to production source code.
- ▶ Developers had the ability to move applications into production without management approval.

- ▶ No standard process ensured that web applications were tested for technical vulnerabilities before being moved into production.

The information security officer stated that the decentralized nature of the campus computing environment made it difficult to enforce web application development practices. He also stated that the new web development group created to address these issues lacked a mandate to enforce compliance. He further stated that the current vulnerability management tools did not allow for web application scanning.

The lack of formal change management procedures increases the risk that web application projects may be unauthorized, inconsistent with user expectations, and contain vulnerabilities.

### **Recommendation 6**

We recommend that the campus:

- a. Require documented approval of all web application projects prior to placement into production.
- b. Establish and document testing criteria for web applications, including but not limited to, input and output validation tests, and tests of vulnerabilities that are commonly exploited.
- c. Establish a documented process for user acceptance testing of web applications.
- d. Ensure that web application source code is protected by limiting access to only those employees who need it as part of their job responsibilities.
- e. Limit developers' ability to move web applications into production, or create procedures so that management monitors changes to production.
- f. Ensure that web application development is formally reviewed and approved centrally prior to final acceptance and implementation to ensure that web applications meet security standards established by the campus.

### **Campus Response**

We concur. By September 30, 2010, we will develop a mandatory campus-wide security policy requiring that all web application code be housed only on centrally managed university servers and monitored in the central data center. In addition, by the same date, the campus will require compliance with all related audit recommendations, including documented approval of all applicable web application projects, documented testing of web application code for vulnerabilities, documented user acceptance testing, access to source code by only authorized personnel, central management monitoring and control of all moves and changes of such code in production, and central management monitoring and control of all web application development prior to deployment of applications.

## **WEB APPLICATION VULNERABILITIES**

Web application vulnerabilities existed on the web application selected for testing.

The web application reviewed allowed access to the administration console without adequate authentication. It also allowed cross-site scripting and contained temporary files, which could expose unintended information to anyone using the web application.

The information security officer stated that these vulnerabilities were caused by various factors including programming oversight and delay in patching servers and/or applications.

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 other network resources.

### **Recommendation 7**

We recommend that the campus repair the website vulnerabilities that were identified and presented to it in detail.

In addition, we recommend that the campus:

- a. Formalize a security standard that requires the review of applications for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the periodic review of existing web application code and of new code prior to deployment into the production environment to minimize the potential deployment of code susceptible to known vulnerabilities.

### **Campus Response**

We concur and will correct all identified website vulnerabilities by September 30, 2010. In addition, we will:

- a. Implement a formal campus-wide security policy and standard requiring central review of all web applications for security prior to deployment, as part of the web development policy noted under Recommendation #6 above.
- b. Ensure implementation of campus-wide web patch management, as detailed in our response to comprehensive patch management under Recommendation #4, in a manner requiring mitigation and patch management specifically for all web application code vulnerabilities.

All of the above actions will be completed by September 30, 2010.

## SYSTEMS SECURITY AND MONITORING

### CONFIGURATION CHANGES

The campus lacked policies and procedures that defined a formal periodic review of configuration changes for the following systems and devices:

- ▶ Firewalls.
- ▶ Switches.
- ▶ Routers.
- ▶ Operating systems.

Informal periodic reviews of these systems and devices 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 network infrastructure and security project lead of network and telecommunications services stated that due to the low attrition rate of employees, he did not consider it necessary to formalize policies and procedures to review configuration changes.

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

#### Recommendation 8

We recommend that the campus:

- a. Develop policies and procedures that establish a formal review of system configurations in order to assist management with determining accountability for potentially misconfigured network devices and with assigning responsibility for identifying and remediating configuration problems.
- 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

The campus concurs and will develop and implement a mandatory campus-wide security policy requiring registration of all devices connected to the network with the information security office by September 30, 2010. This policy will define mandatory campus-wide network configuration requirements, as well as accountability for the configuration and remediation of vulnerabilities for each device. This policy will also require that all campus network devices be compliant with all applicable institutional network policies and practices, with formal sign-off required by the chief information officer to ensure compliance.

## **CONTROL OF USER ACCESS**

The administration of user access profiles required improvement.

Our review of several applications that contained confidential data outside of CMS disclosed that:

- ▶ User confidentiality agreements were not completed and retained, indicating formal approval for access to protected data.
- ▶ The campus had not consistently performed periodic management reviews for validating system access and/or permissions.
- ▶ One system contained an account that was shared by multiple users.

The information security officer stated that campus central IT had not required formal documentation of the periodic review of these systems as part of the risk assessment process.

Failure to adequately administer user accounts increases the risk of inappropriate access.

### **Recommendation 9**

We recommend that the campus:

- a. Ensure that user confidentiality agreements are completed and retained for those users with access to protected data.
- b. Conduct and document periodic reviews of user access to systems containing protected data on an annual basis, at minimum.
- c. Ensure user accountability by removing shared and anonymous accounts.

### **Campus Response**

We concur. By September 30, 2010, we will develop and implement a mandatory campus-wide information security policy requiring that all user accounts and access profiles campus-wide be provisioned only using the central campus-wide identity management and authentication process. This policy will also require use of a single university Active Directory domain by all program centers, including for provisioning and de-provisioning of accounts and access profiles. In addition:

- a. User confidentiality agreements will be required of all users with access to critical and level one data, with special attention to IT and functional staff with elevated access.
- b. We will develop a process for an annual campus-wide review of user access controls for all IT systems identified as containing protected data, including systems in decentralized and auxiliary program centers.

- c. We will develop a mandatory campus-wide policy prohibiting the use of shared accounts and requiring a policy of one official campus-wide account per authorized user.

All of the above actions will be completed by September 30, 2010.

## **VULNERABILITY MANAGEMENT**

The management of campus vulnerabilities required improvement.

We noted that:

- ▶ While the campus had a process to scan most campus servers, certain program centers had not been scanned.
- ▶ The information security office did not have a clearly defined timeline for the remediation of vulnerabilities.
- ▶ Program centers had not developed formal steps and timelines for the remediation of vulnerabilities.
- ▶ The campus had not developed a set of standards for non-compliance for critical systems.

The information security officer stated that the campus was unable to scan certain servers because they were not on the centrally managed network and their network devices did not meet current campus technology standards. He also stated that security vulnerability scans and remediation had not been mandated as part of the campus information security program.

Failure to adequately identify vulnerabilities may lead to a network compromise and potential loss of protected confidential information.

### **Recommendation 10**

We recommend that the campus:

- a. Complete a thorough scan of decentralized program centers and centrally managed systems to ensure complete coverage of all campus vulnerabilities.
- b. Develop a clearly defined timeline for the remediation of vulnerabilities for central IT as well as for all program centers.
- c. Develop standards for non-compliance to ensure vulnerabilities are appropriately addressed.

### **Campus Response**

We concur. By September 30, 2010, we will develop and implement an information security policy and standard requiring all servers to be scanned and proactive mitigation to be performed on identified critical and severe security vulnerabilities. The policy will give the information security officer, under the authority of the chief information officer, all needed authority to set remediation timelines and sanctions for non-compliant systems campus-wide. The primary mechanism for addressing vulnerability management will be the central management and hosting of all vulnerable systems by the central IT organization, as noted under our responses to Recommendations #1 and #4.

### **APPLICATION CONTROL**

The campus had not assessed the risk of local administrative accounts on their systems.

Local administrative accounts on desktops in which users have the ability to install their own applications pose several risks including, but not limited to:

- ▶ Applications installed may violate campus and California State University (CSU) policy.
- ▶ Applications installed may expose the campus network to other vulnerabilities.

The information security officer stated that this had been an ongoing issue and that the campus had formerly lacked the tools to respond appropriately to customer needs for application installations.

Local administrative accounts, in which users have the ability to install their own applications, increase the risk that applications may violate CSU policy and/or expose the campus network to other vulnerabilities.

### **Recommendation 11**

We recommend that the campus assess the risk of having local administrative accounts and remove access if there is no business purpose for such use.

### **Campus Response**

The campus concurs and will develop and implement a mandatory campus-wide policy formally limiting the use of local administrative accounts on workstations to the minimum situations requiring such accounts for business purposes. A process will also be developed to remove existing local administrative access when it does not conform with this policy. Both of these actions will be completed by September 30, 2010.

## **PASSWORD STANDARDS**

The campus did not adhere to password best practices.

We noted the following:

- ▶ The campus did not have a standard password policy that it extended to and enforced for all departments and/or applications on campus.
- ▶ Certain systems did not require passwords to meet complexity requirements.
- ▶ Most accounts were set up with non-expiring passwords.

The chief information officer stated that the greatest barriers to the use of best practice password standards are lack of control over decentralized account management practices, lack of a single campus-wide active directory domain, and limitations in available password technology.

Failure to adhere to password best practices increases the risk of easily guessed passwords and possible unauthorized access to network resources and confidential information.

### **Recommendation 12**

We recommend the campus establish and implement a standard password policy and ensure that all departments comply with that policy.

### **Campus Response**

We concur and will develop and implement a standard password policy campus-wide, by September 30, 2010. We acquired and implemented a comprehensive password change application and are in the process of using that application to enforce password hardening and aging for all students, all employees, and all accounts.

In order to ensure campus-wide adherence to this password policy, and as noted in Recommendation #11, we will also institute a policy requiring the use of only a single university-wide Active Directory domain with a single, unified password policy. This policy will be completed by September 30, 2010.

## **NETWORK ACCESS**

Campus administration of wireless networks required improvement.

Specifically, we noted that the campus allowed sessions of unlimited duration for anonymous users.

The information security officer stated that the campus did not consider limiting sessions during the implementation of wireless network access on campus because doing so would have conflicted with

the goal of providing access to the campus community. He further stated his belief that the campus had implemented enough compensating controls for the amount of related risk.

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 13**

We recommend that the campus consider session time-outs to mitigate the risks of attacks through an open network.

### **Campus Response**

We concur with the use of network session time-outs. We will implement mandatory time-outs for inactive wireless network connections campus-wide, and will implement a requirement that all computer users utilize appropriate time-outs in computer labs and on their desktops and laptops. In addition, the campus will perform a periodic campus-wide wireless audit to detect rogue access points and eliminate or remediate based on business needs and compensating controls. All of these actions will be completed by September 30, 2010.

## **GRANTING OF ADMINISTRATIVE ACCESS**

The process for the granting and management of privileged system-level access to accounts required improvement.

The chief information officer stated that the campus has a formal process for the granting of privileged system-level access for CMS administrative access; however, due to a previous lack of automated access controls, the process had not yet been extended to non-CMS systems.

The lack of a formal process for the granting and management of privileged access to non-CMS systems may lead to inadequate segregation of duties, the granting of accounts not based on the principle of least privilege, and/or unauthorized access.

### **Recommendation 14**

We recommend that the campus:

- a. Establish a formal process for the granting and management of privileged system-level access to accounts within non-CMS systems.
- b. Develop a method to track, review, and periodically audit this type of access.

### **Campus Response**

We concur. As of November 2009, the campus implemented a process for formal campus-wide review, monitoring, and compliance with segregation of duties and access controls over the granting of privileged access to system-level CMS accounts. The campus is in the process of implementing the use of a similar process for non-CMS system access campus-wide, as addressed in our response to Recommendation #9. Control over privileged system access will be implemented as part of the comprehensive server registration and management process detailed under Recommendation #4. All of these actions will be completed by September 30, 2010.

### **FIREWALLS AND ROUTING AND SWITCHING DEVICES**

Firewalls and routing and switching devices in the central and decentralized program centers were not always properly configured or adequately secured.

Our review of the border firewall and selected routing and switching devices disclosed that:

- ▶ One device did not have time-out connection configured and could allow an attacker to continue using a terminated connection.
- ▶ Two devices were configured with Simple Network Management Protocol (SNMP). SNMP is unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ Three devices were enabled with Telecommunication Network (Telnet). Because Telnet transfers user logins, passwords, and commands across the network in clear text, this could allow a remote attacker to obtain confidential authentication tokens, which could enable remote access to the devices.
- ▶ One device had an older version of the Secure Shell (SSH) protocol enabled, which an attacker could exploit to perform a man-in-the-middle style attack and possibly to execute system commands.

The network infrastructure and security project lead of network and telecommunications services stated that these vulnerabilities were due to staff oversight or the lack of resources to implement the required technology.

These vulnerabilities increase the risk that a remote attacker may be able to exploit network resources, gain access to protected confidential information, or execute malicious programs that could potentially disable other network resources.

### **Recommendation 15**

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

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 network environment to identify potential or known vulnerabilities.

### **Campus Response**

We concur and will repair all identified network infrastructure device vulnerabilities, by September 30, 2010. We further concur with the other recommendations. As previously noted, management and control of all campus-wide network devices will be migrated to central IT. Additionally, the following actions will be taken:

- a. Develop a campus-wide policy defining a security baseline standard for all network infrastructure devices and a process for reviewing all new devices for security vulnerabilities prior to deployment.
- b. As part of the comprehensive patch management process detailed under Recommendations #4 and #7, we will develop a mandated, centrally administered patch management process for all network infrastructure devices.

All of the above actions will be completed by September 30, 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 network infrastructure and security project lead of network and telecommunications services stated that the network had not been segregated due to other priorities on campus.

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 16**

We recommend that the campus review its current network topology and determine the most logical way to separate Internet-accessible devices from other devices within the internal network.

### **Campus Response**

The campus concurs and will conduct a comprehensive campus-wide review of network topology and adopt the architecture that ensures the maximum segregation of Internet-accessible devices from other devices. This review will be done as part of the analysis that will lead to the centralization of all network activity, as noted in Recommendations #1 and #15. In addition, the university will adopt a policy that requires campus-wide adherence to the required network topology. The review, policy, and required network topology will be completed by July 1, 2010.

### **OPERATING SYSTEMS VULNERABILITIES**

Technical vulnerabilities existed on selected operating systems.

Our testing of selected servers disclosed various vulnerabilities. We provided details of these vulnerabilities to the campus. One server was running an old version of retrospect client. One server had a guest account with excessive privileges, another server was running a deprecated operating system, and a third server was vulnerable to an information disclosure flaw. Two servers had TRACE and TRACK methods enabled. One server was running a vulnerable version of Simple Mail Transfer Protocol (SMTP). One server was running a vulnerable version of remote desk protocol (RDP). Finally, several servers had user accounts with non-expiring passwords.

The information security officer stated that the lack of centralized IT oversight and direction had permitted the majority of these vulnerabilities to propagate in the decentralized computing environments.

These vulnerabilities increase the risk of a remote attack that could result to a loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

### **Recommendation 17**

We recommend that the campus repair all the technical vulnerabilities, especially clear text protocols, that were identified and presented to it in detail.

In addition, we recommend that the campus:

- a. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.

### **Campus Response**

The campus concurs and will repair all technical vulnerabilities, especially clear text protocols, that were identified and presented during the audit. The campus will develop a formal campus-wide policy defining a security baseline standard for applications. In addition, the campus will include campus-wide patch management of operating systems and applications as part of the comprehensive patch management process detailed under Recommendations #4 and #7. All of these actions will be completed by September 30, 2010.

### **REVIEW OF SECURITY EVENT LOGS**

The campus lacked a formal process for the review of security event logs.

The information security officer stated that network activity was monitored continuously and that logs are reviewed informally as needed.

The lack of periodic documented reviews of security event logs increases the risk that malicious activity could go undetected or viruses or other malicious code could be embedded within the campus network and its resources. This could lead to an unreported breach of confidential information.

### **Recommendation 18**

We recommend that the campus:

- a. Establish a formal process to regularly review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of campus systems. This process could include the use of tools and analytical methods and should define personnel responsibilities, reviewing frequency, and reporting/escalating processes.
- b. Consider the implementation of security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

### **Campus Response**

We concur. By September 30, 2010, we will specify in a new campus-wide policy the logs subject to these provisions, as well as the process to be used for analysis of logs and mitigation of problems found. Additionally, we will use the comprehensive server registration and compliance process detailed under Recommendation #4 to require implementation, monitoring, and review of security event logs, followed by mitigation of security problems encountered in those logs.

We will also leverage existing centrally managed security event monitoring tools to monitor and notify central administrative staff of critical security events, and this will be completed by September 30, 2010.

## **BASELINE SECURITY STANDARDS**

The campus lacked a formal process to identify and monitor all IT resources on the campus network, and baseline security standards for the administration of decentralized servers and desktops had not been developed.

The information security officer stated that the autonomy over management of the campus' decentralized computing environment, as well as lack of documentation standards, contributed to this oversight.

The inability to identify and monitor all campus IT resources and the lack of baseline standards increases the risk of misconfigured systems and may leave the campus vulnerable to both internal and external attacks that could slow or bring down the network.

### **Recommendation 19**

We recommend that the campus:

- a. Identify all current IT assets (including hardware, software, and their associated operating system versions) on the campus network and implement a process to monitor these for adequate security.
- b. Develop baseline security standards for the decentralized administration of servers and desktop systems.

### **Campus Response**

The campus concurs and will use the policy detailed under Recommendation #4 to define mandatory security standards for all campus servers, desktops, and other computer/network devices. The management and security monitoring software, noted in our response to Recommendation #5, will be used to identify all current IT assets campus-wide. As noted under previous recommendations, our primary approach to ensuring compliance of currently decentralized computer and network devices is to centralize management and control of such devices as quickly as possible. We will also develop a policy for baseline security standards and require compliance with that policy for all campus computer and network devices. All of these actions will be completed by September 30, 2010.

## **PROTECTED DATA**

### **ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION**

The campus had not recently completed a university-wide assessment to identify sensitive data on all servers and workstations.

The information security officer stated that the campus had performed a risk assessment 18 months ago but that it was a manual process and not sustainable for ongoing identification of sensitive data.

He also stated that there had been concerns about user privacy when assessing workstations and they are currently piloting a self-evaluation process.

Inadequate accountability for protected and/or personal confidential information increases the risk of loss and inappropriate use of state resources, and increases campus exposure to information security breaches.

### **Recommendation 20**

We recommend that the campus conduct annual or ongoing university-wide assessments to identify sensitive data on all servers and workstations.

### **Campus Response**

The campus concurs and will develop a policy by September 30, 2010. This policy will require proactive identification of all sensitive and confidential data stored on servers, desktops, and other devices; require that sensitive data be housed only on centrally managed servers and devices in the central data center; and require that all sensitive data found on decentralized systems be reported to the information security officer.

## **LOST/STOLEN COMPUTERS**

The campus lacked a formal process to ensure that lost/stolen computers were consistently reported to the information security office. This in turn prevented the campus from determining whether there was any sensitive information on these computers and whether further action was required.

The information security officer stated that because the campus had an informal process, lost/stolen computers may not have been consistently reported to the information security office.

Inadequate procedures for the reporting and investigation of lost or stolen equipment, which may contain protected data, increases the risk that information security breaches could go unreported, resulting in significant financial penalty and damage to the campus' reputation.

### **Recommendation 21**

We recommend that the campus ensure that all lost/stolen computers are reported to the information security office for an appropriate review and investigation.

### **Campus Response**

We concur with the importance of identifying all lost and stolen computer devices. By September 30, 2010, we will develop a campus-wide policy requiring reporting of the loss of any computer or network device, with special attention to those potentially containing sensitive data.

## **DISPOSITION OF PROTECTED DATA**

The campus' process for ensuring that all sensitive information on computers and laptops was properly deleted required improvement.

We noted that:

- ▶ Certain departments had not consistently wiped hard drives through an approved method.
- ▶ No controls or processes ensured that all hard drives had been wiped prior to their disposition.

The information security officer stated that the individual departments were responsible for wiping their own drives prior to disposition, but that best practices may not have been followed.

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

### **Recommendation 22**

We recommend that the campus develop a process for disposing of computers that ensures adequate hard-drive wiping is performed and sufficiently documented.

### **Campus Response**

We concur and will develop a campus-wide policy requiring controlled disposal of all computer and network devices, with special attention to those containing sensitive information. The policy will include guidelines detailing the procedure required to certify proper disposal. The policy and procedures will be completed by September 30, 2010.

## **INCIDENT RESPONSE MANAGEMENT**

The campus' security incident handling procedures for compromised electronic resources required improvement.

We noted that:

- ▶ The campus had no formal security incident response policy.
- ▶ The campus had no formal guidelines for handling specific types of incidents (i.e., malicious code, denial of service, breach of confidential data, etc.).
- ▶ The campus had no formal process to identify types, frequency, and costs of information security incidents.

- ▶ Security incidents were not formally reported to executive management to ensure support for enhanced controls.
- ▶ The decentralized departments lacked a formal process to report incidents occurring in their areas.

The information security officer stated that the campus lacked a standardized method of incident reporting, which made it difficult to track incidents as they occurred. He further stated that the decentralized nature of the campus environment made it difficult to identify, classify, and respond to all incidents on campus.

Inadequate procedures for monitoring and responding to security incidents increase the risk of loss and inappropriate use of state resources, and increase campus exposure to information security breaches.

### **Recommendation 23**

We recommend that the campus:

- a. Establish a formal security incident response policy.
- b. Develop written guidelines for the handling of specific types of security incidents.
- c. Develop and document procedures to identify the types, volume, and costs of security incidents to ensure that the campus monitors trends and risks.
- d. Establish a documented process for the reporting of types, volumes, and costs of security incidents to executive management to ensure support for enhanced control.
- e. Develop formal incident reporting procedures to ensure complete campus coverage, including the decentralized environments.

### **Campus Response**

The campus concurs and will develop and implement a campus-wide security incident response policy and guidelines for handling specific types of security incidents. The guidelines will document procedures to identify the types, volume, and costs of security incidents to ensure the campus monitors trends and risks, as well as to implement a process to report incidents to central executive management to raise awareness and ensure support. These actions will be completed by September 30, 2010.

---

## APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Alexander Gonzalez	President
Jeff Bingel	Information Technology Consultant, College of Business
Bridgette Bucke	Director, Data Services
Michael Christensen	Interim Associate Vice President, Risk Management Services
Jeff Dillon	Manager, Web Services
Stephen Garcia	Vice President of Administration and Business Affairs/ Chief Financial Officer
Larry Gilbert	Vice President and Chief Information Officer, Information Resources and Technology
James Hayes	Information Technology Consultant, University Library
Yavette Hayward	Internal Auditor, Auditing Services
Doug Jackson	Assistant Vice President, Academic Computing Resources
Ted Koubiar	Director, Operations and Systems Services
Clinton Lee	Director, Business Information Systems
Kathi McCoy	Director of Auditing Services
Meri McGraw	Information Technology Director, University Enterprises, Inc.
Matthew Mills	Information Technology Consultant, College of Arts and Letters
Jason Musselman	Network Security Analyst Network Infrastructure and Security Project Lead, Network and Telecommunications.
Carl Oakes	Director, Network and Telecommunications
Gregory Porter	Head of Curriculum Online Library Services
Mary Reddick	Administrative Support Coordinator, Library Services
Charles Roberts	Director of Library Systems and Information Technology Services
Carlos Rodriguez	Director of Procurement/Contract Services
David Shannon	Information Technology Consultant, Office of Water and Power
Jim Vanderveen	Vice President, Human Resources
David Wagner	Information Security Officer
Jeff Williams	Information Technology Consultant, Engineering and Computer Science
Mike Wimple	



California State University, Sacramento  
Office of the Vice President for Administration  
6000 J Street • Sacramento Hall 272 • Sacramento, CA 95819-6038  
T (916) 278-6312 • F (916) 278-5783 • www.csus.edu/aba

February 9, 2010

RECEIVED  
UNIVERSITY AUDITOR

FEB 12 2010

THE CALIFORNIA STATE  
UNIVERSITY

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

Subject: Campus Response to Recommendations of Information Security Audit,  
Report #09-36

Dear Mr. Mandel:

Please find enclosed California State University, Sacramento's response to the recommendations of the audit. The campus is committed to addressing and resolving the issues identified in the audit report.

If you have any questions or require additional information, please contact Kathi McCoy, Director of Auditing Services, at 916 278-7439.

Sincerely,

A handwritten signature in black ink, appearing to read "Stephen G. Garcia".

Stephen G. Garcia  
Vice President & Chief Financial Officer

SGG: sf

Attachment

cc: Alexander Gonzalez, President  
Larry Gilbert, Vice President & Chief Information Officer  
Kathi McCoy, Director, Auditing Services  
Jeff Williams, Information Security Officer, Information Resources & Technology

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**SACRAMENTO**

**Audit Report 09-36**

**SECURITY GOVERNANCE**

**SECURITY ORGANIZATION**

**Recommendation 1**

We recommend that the campus improve its process to monitor and enforce campus-wide information security policies, procedures, and guidelines. An effective approach would be to require critical and business systems, including all network infrastructure, to be migrated and managed by central IT.

**Campus Response**

We concur with the recommendation regarding improvement of our ability to monitor and enforce information security policies and processes campus-wide. We will develop a campus-wide organizational and management structure for information technology that ensures that the Chief Information Officer and Information Security Officer provide management and oversight to all aspects of the monitoring and enforcement of campus-wide information security. This reorganization of IT will provide for the recommended migration of all critical and business IT systems and network activity under the management of the campus-wide IT organization. We will also develop a policy giving the Information Security Officer, under the authority of the Chief Information Officer, all needed authority for evaluation, enforcement, and implementation of all required information security policies and procedures campus-wide, including for auxiliary and self-support units. Both policy development and the reorganization of the management structure for information technology will be completed by September 30, 2010.

**INFORMATION SECURITY AWARENESS TRAINING**

**Recommendation 2**

We recommend the campus ensure that all employees with access to campus information resources complete information security awareness training.

**Campus Response**

The campus concurs and will have the Information Security Officer work with campus Human Resources to implement mandatory information security awareness training for all employees campus-wide, including those in auxiliary organizations. Continued special attention will be paid to IT and functional employees with access to confidential information. Training will be included in mandatory employee orientation programs no later than May 1, 2010 and will be provided or certified for existing employees no later than September 30, 2010.

## ACCESS CONTROL

### Recommendation 3

We recommend that the campus:

- a. Revise the current process to ensure that user privileges are modified or old access is deactivated for intra-campus employee transfers.
- b. Develop a process that includes user provisioning and de-provisioning to ensure that access is granted, removed, or deactivated when employment status with the university changes.
- c. Immediately deactivate terminated employees from the active directory when they are no longer physically present on campus.

### Campus Response

The campus concurs and will implement a comprehensive and mandatory campus-wide identity management policy requiring campus-wide implementation and monitoring of all recommended access controls by a central identity management system, no later than September 30, 2010.

Specifically, we will:

- a. Ensure that all account creation and provisioning campus-wide is completed only under the authority of the central IT organization and the campus-wide Information Security Officer, under the management of the centrally controlled identity management system.
- b. Have the central IT organization work with Human Resources to develop and implement a process to both identify intra-campus employee transfers campus-wide and to modify/deactivate associated privileges in a timely manner using the central identity management system.
- c. Using the same process noted under item 3b, identify and implement a campus-wide process to identify all employment status changes and to remove/deactivate associated account privileges in a timely manner when appropriate.
- d. Using the same process noted under 3b, implement a process to immediately deactivate the account privileges of employees on or before their last active work day at the university.

## DECENTRALIZED COMPUTING

### SERVER ENVIRONMENTS

#### Recommendation 4

We recommend that the campus:

- a. Ensure that backups from decentralized servers containing sensitive data are properly encrypted and stored off-site.

- b. Encrypt desktop and/or laptop computer drives that contain sensitive information.
- c. Ensure that password standards meet a minimum security baseline.
- d. Comply with their policy to prohibit sharing of administrative accounts.
- e. Ensure that designated information technology professionals have appropriate authority and oversight over all equipment and technologies in the college computing environments.
- f. Develop formal log management procedures to ensure logs are retained and reviewed regularly.
- g. Ensure that patch management processes effectively keep virus definitions and patches current.
- h. Develop a formal change management process to ensure that changes to systems are tested, reviewed, and approved.

**Campus Response**

We concur that the administration of Sacramento State’s decentralized server environments requires significant improvement and also concur with the statement noted in the Executive Summary that “Establishing controls that would prevent all [the] limitations [of decentralized environments] would not be cost effective.” We therefore fully concur with Recommendation #1 that an effective approach to mitigating these problems is to require that all critical and business systems be migrated and managed by central IT.

We will create and implement a policy and procedures requiring that all campus servers and network systems/devices be managed by and registered with the central IT organization by September 30, 2010. Oversight will be provided by the Information Security Office staff to ensure compliance with all recommended information security policies and procedures and certification by senior IT management.

Specifically, the policy and procedures will ensure:

- a. Proper storage and encryption of all backups containing sensitive data campus-wide.
- b. Encryption of all sensitive information on servers, desktop and laptop computers campus-wide.
- c. Use of minimum campus-wide password policies for all computer and network access campus-wide.
- d. Non-sharing of administrative accounts and segregation and oversight of access where needed.
- e. Oversight by the CIO, Information Security Officer and designees over all computer and network equipment and processes remaining in program center environments.
- f. Maintenance, retention, and review of all security logs as defined by university policy, with timely mitigation of problems required.
- g. Mandatory, comprehensive, and timely patch management and virus protection for all computer and network devices campus-wide.

- h. Comprehensive and mandatory change management processes for all computer and network devices, with formal review by the Information Security Officer or designees prior to deployment of all changes.

## **TECHNICAL VULNERABILITIES**

### **Recommendation 5**

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This process would include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment to identify potential vulnerabilities.
- c. Develop a campus-wide application development standard with which all developers of Internet-facing applications for the campus must comply.
- d. Provide all the decentralized program centers with a security baseline standard for securing servers.

### **Campus Response**

The campus concurs and will repair all technical vulnerabilities identified and presented during the audit, by September 30, 2010. In addition, we will implement a policy requiring use of campus-wide monitoring and security management software to implement comprehensive patch management on all computer desktops, laptops, servers and other applicable computer and network devices (5a). Utilizing the server management, registration, and compliance processes detailed in Recommendation #4, we will:

- Require identification of all vulnerable application code, periodic review of existing application code, and review of application vulnerability prior to code deployment (5b);
- Develop, require compliance with, and monitor compliance with published application development standards, (5c), and;
- Develop policies requiring compliance with a set of minimum server and application security standards (5d).

All of the above actions will be completed by September 30, 2010.

## SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

### WEB APPLICATION DEVELOPMENT AND MAINTENANCE

#### Recommendation 6

We recommend that the campus:

- a. Require documented approval of all web application projects prior to placement into production.
- b. Establish and document testing criteria for web applications, including but not limited to, input and output validation tests, and tests of vulnerabilities that are commonly exploited.
- c. Establish a documented process for user acceptance testing of web applications.
- d. Ensure that web application source code is protected by limiting access to only those employees who need it as part of their job responsibilities.
- e. Limit developers' ability to move web applications into production, or create procedures so that management monitors changes to production.
- f. Ensure that web application development is formally reviewed and approved centrally prior to final acceptance and implementation to ensure that web applications meet security standards established by the campus.

#### Campus Response

We concur. By September 30, 2010, we will develop a mandatory campus-wide security policy requiring that all web application code be housed only on centrally managed university servers and monitored in the central data center. In addition, by the same date, the campus will require compliance with all related audit recommendations, including documented approval of all applicable web application projects (6a), documented testing of web application code for vulnerabilities (6b), documented user acceptance testing (6c), access to source code by only authorized personnel (6d), central management monitoring and control of all moves and changes of such code in production (6e), and central management monitoring and control of all web application development prior to deployment of applications (6f).

### WEB APPLICATION VULNERABILITIES

#### Recommendation 7

We recommend that the campus repair the website vulnerabilities that were identified and presented to it in detail.

In addition, we recommend that the campus:

- a. Formalize a security standard that requires the review of applications for security vulnerabilities prior to deployment.

- b. Implement a comprehensive, campus-wide patch management process. This process would include the periodic review of existing web application code and of new code prior to deployment into the production environment to minimize the potential deployment of code susceptible to known vulnerabilities.

#### **Campus Response**

We concur and will correct all identified website vulnerabilities by September 30, 2010. In addition, we will:

- a. Implement a formal campus-wide security policy and standard requiring central review of all web applications for security prior to deployment, as part of the web development policy noted under Recommendation #6 above.
- b. Ensure implementation of campus-wide web patch management, as detailed in our response to comprehensive patch management under Recommendation #4, in a manner requiring mitigation and patch management specifically for all web application code vulnerabilities.

All of the above actions will be completed by September 30, 2010.

## **SYSTEMS SECURITY AND MONITORING**

### **CONFIGURATION CHANGES**

#### **Recommendation 8**

We recommend that the campus:

- a. Develop policies and procedures that establish a formal review of system configurations in order to assist management with determining accountability for potentially misconfigured network devices and with assigning responsibility for identifying and remediating configuration problems.
- 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**

The campus concurs and will develop and implement a mandatory campus-wide security policy requiring registration of all devices connected to the network with the Information Security Office by September 30, 2010. This policy will define mandatory campus-wide network configuration requirements, as well as accountability for the configuration and remediation of vulnerabilities for each device. This policy will also require that all campus network devices be compliant with all applicable institutional network policies and practices, with formal sign-off required by the Chief Information Officer to ensure compliance.

## **CONTROL OF USER ACCESS**

### **Recommendation 9**

We recommend that the campus:

- a. Ensure that user confidentiality agreements are completed and retained for those users with access to protected data.
- b. Conduct and document periodic reviews of user access to systems containing protected data on an annual basis, at minimum.
- c. Ensure user accountability by removing shared and anonymous accounts.

### **Campus Response**

We concur. By September 30, 2010, we will develop and implement a mandatory campus-wide information security policy requiring that all user accounts and access profiles campus-wide be provisioned only using the central campus-wide identity management and authentication process. This policy will also require use of a single university Active Directory domain by all program centers, including for provisioning and de-provisioning of accounts and access profiles. In addition:

- a. User confidentiality agreements will be required of all users with access to critical and level one data, with special attention to IT and functional staff with elevated access.
- b. We will develop a process for an annual campus-wide review of user access controls for all information technology systems identified as containing protected data, including systems in decentralized and auxiliary program centers.
- c. We will develop a mandatory campus-wide policy prohibiting the use of shared accounts and requiring a policy of one official campus-wide account per authorized user.

All of the above actions will be completed by September 30, 2010.

## **VULNERABILITY MANAGEMENT**

### **Recommendation 10**

We recommend that the campus:

- a. Complete a thorough scan of decentralized program centers and centrally managed systems to ensure complete coverage of all campus vulnerabilities.
- b. Develop a clearly defined timeline for the remediation of vulnerabilities for central IT as well as for all program centers.
- c. Develop standards for non-compliance to ensure vulnerabilities are appropriately addressed.

**Campus Response**

We concur. By September 30, 2010, we will develop and implement an information security policy and standard requiring all servers to be scanned (a), and proactive mitigation to be performed on identified critical and severe security vulnerabilities (b). The policy will give the Information Security Officer, under the authority of the Chief Information Officer, all needed authority to set remediation timelines and sanctions for non-compliant systems campus-wide (c). The primary mechanism for addressing vulnerability management will be the central management and hosting of all vulnerable systems by the central IT organization, as noted under our responses to Recommendations #1 and #4.

**APPLICATION CONTROL****Recommendation 11**

We recommend that the campus assess the risk of having local administrative accounts and remove access if there is no business purpose for such use.

**Campus Response**

The campus concurs and will develop and implement a mandatory campus-wide policy formally limiting the use of local administrative accounts on workstations to the minimum situations requiring such accounts for business purposes. A process will also be developed to remove existing local administrative access when it does not conform with this policy. Both of these actions will be completed by September 30, 2010.

**PASSWORD STANDARDS****Recommendation 12**

We recommend the campus establish and implement a standard password policy and ensure that all departments comply with that policy.

**Campus Response**

We concur and will develop and implement a standard password policy campus-wide, by September 30, 2010. We acquired and implemented a comprehensive password change application and are in the process of using that application to enforce password hardening and aging for all students, all employees, and all accounts.

In order to ensure campus-wide adherence to this password policy, and as noted in Recommendation #11, we will also institute a policy requiring the use of only a single university-wide Active Directory domain with a single, unified password policy. This policy will be completed by September 30, 2010.

## NETWORK ACCESS

### Recommendation 13

We recommend that the campus consider session time-outs to mitigate the risks of attacks through an open network.

### Campus Response

We concur with the use of network session time-outs. We will implement mandatory time-outs for inactive wireless network connections campus-wide, and will implement a requirement that all computer users utilize appropriate timeouts in computer labs and on their desktops and laptops. In addition, the campus will perform a periodic campus-wide wireless audit to detect rogue access points and eliminate or remediate based on business needs and compensating controls. All of these actions will be completed by September 30, 2010.

## GRANTING OF ADMINISTRATIVE ACCESS

### Recommendation 14

We recommend that the campus:

- a. Establish a formal process for the granting and management of privileged system-level access to accounts within non-CMS systems.
- b. Develop a method to track, review, and periodically audit this type of access.

### Campus Response

We concur. As of November 2009, the campus implemented a process for formal campus-wide review, monitoring, and compliance with segregation of duties and access controls over the granting of privileged access to system level CMS accounts. The campus is in the process of implementing the use of a similar process for non-CMS system access campus-wide, as addressed in our response to Recommendation #9. Control over privileged system access will be implemented as part of the comprehensive server registration and management process detailed under Recommendation #4. All of these actions will be completed by September 30, 2010

## FIREWALLS AND ROUTING AND SWITCHING DEVICES

### Recommendation 15

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

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 network environment to identify potential or known vulnerabilities.

### **Campus Response**

We concur and will repair all identified network infrastructure device vulnerabilities, by September 30, 2010. We further concur with the other recommendations. As previously noted, management and control of all campus-wide network devices will be migrated to central IT. Additionally, the following actions will be taken.

- a. Develop a campus-wide policy defining a security baseline standard for all network infrastructure devices and a process for reviewing all new devices for security vulnerabilities prior to deployment.
- b. As part of the comprehensive patch management process detailed under Recommendations #4 and #7, we will develop a mandated, centrally administered patch management process for all network infrastructure devices.

All of the above actions will be completed by September 30, 2010.

## **NETWORK ARCHITECTURE**

### **Recommendation 16**

We recommend that the campus review its current network topology and determine the most logical way to separate Internet-accessible devices from other devices within the internal network.

### **Campus Response**

The campus concurs and will conduct a comprehensive campus-wide review of network topology and adopt the architecture that ensures the maximum segregation of Internet-accessible devices from other devices. This review will be done as part of the analysis that will lead to the centralization of all network activity, as noted in Recommendations #1 and #15. In addition, the university will adopt a policy that requires campus-wide adherence to the required network topology. The review, policy, and required network topology will be completed by July 1, 2010.

## **OPERATING SYSTEMS VULNERABILITIES**

### **Recommendation 17**

We recommend that the campus repair all the technical vulnerabilities, especially clear text protocols, that were identified and presented to it in detail.

In addition, we recommend that the campus:

- a. Formalize a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment.

- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing code on a periodic basis or new code prior to deployment into the production environment to identify potential or known vulnerabilities.

### **Campus Response**

The campus concurs and will repair all technical vulnerabilities, especially clear text protocols, that were identified and presented during the audit. The campus will develop a formal campus-wide policy defining a security baseline standard for applications (17a). In addition, the campus will include campus-wide patch management of operating systems and applications as part of the comprehensive patch management process detailed under Recommendations #4 and #7 (17b). All of these actions will be completed by September 30, 2010.

## **REVIEW OF SECURITY EVENT LOGS**

### **Recommendation 18**

We recommend that the campus:

- a. Establish a formal process to regularly review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of campus systems. This process could include the use of tools and analytical methods and should define personnel responsibilities, reviewing frequency, and reporting/escalating processes.
- b. Consider the implementation of security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

### **Campus Response**

We concur. By September 30, 2010, we will specify in a new campus-wide policy the logs subject to these provisions, as well as the process to be used for analysis of logs and mitigation of problems found. Additionally, we will use the comprehensive server registration and compliance process detailed under Recommendation #4 to require implementation, monitoring, and review of security event logs, followed by mitigation of security problems encountered in those logs (18a).

We will also leverage existing centrally managed security event monitoring tools to monitor and notify central administrative staff of critical security events (18b), and this will be completed by September 30, 2010.

## **BASELINE SECURITY STANDARDS**

### **Recommendation 19**

We recommend that the campus:

- a. Identify all current IT assets (including hardware, software, and their associated operating system versions) on the campus network and implement a process to monitor these for adequate security.
- b. Develop baseline security standards for the decentralized administration of servers and desktop systems.

**Campus Response**

The campus concurs and will use the policy detailed under Recommendation #4 to define mandatory security standards for all campus servers, desktops and other computer/network devices. The management and security monitoring software, noted in our response to Recommendation #5, will be used to identify all current IT assets campus-wide (19a). As noted under previous recommendations, our primary approach to ensuring compliance of currently decentralized computer and network devices is to centralize management and control of such devices as quickly as possible. We will also develop a policy for baseline security standards and require compliance with that policy for all campus computer and network devices (19b). All of these actions will be completed by September 30, 2010.

**PROTECTED DATA****ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION****Recommendation 20**

We recommend that the campus conduct annual or ongoing university-wide assessments to identify sensitive data on all servers and workstations.

**Campus Response**

The campus concurs and will develop a policy, by September 30, 2010. This policy will: require proactive identification of all sensitive and confidential data stored on servers, desktops, and other devices; require that sensitive data be housed only on centrally managed servers and devices in the central data center; and require that all sensitive data found on decentralized systems be reported to the Information Security Officer.

**LOST/STOLEN COMPUTERS****Recommendation 21**

We recommend that the campus ensure that all lost/stolen computers are reported to the information security office for an appropriate review and investigation.

**Campus Response**

We concur with the importance of identifying all lost and stolen computer devices. By September 30, 2010, we will develop a campus-wide policy requiring reporting of the loss of any computer or network device, with special attention to those potentially containing sensitive data.

**DISPOSITION OF PROTECTED DATA****Recommendation 22**

We recommend that the campus develop a process for disposing of computers that ensures adequate hard drive wiping is performed and sufficiently documented.

### **Campus Response**

We concur and will develop a campus-wide policy requiring controlled disposal of all computer and network devices, with special attention to those containing sensitive information. The policy will include guidelines detailing the procedure required to certify proper disposal. The policy and procedures will be completed by September 30, 2010.

## **INCIDENT RESPONSE MANAGEMENT**

### **Recommendation 23**

We recommend that the campus:

- a. Establish a formal security incident response policy.
- b. Develop written guidelines for the handling of specific types of security incidents.
- c. Develop and document procedures to identify the types, volume, and costs of security incidents to ensure that the campus monitors trends and risks.
- d. Establish a documented process for the reporting of types, volumes, and costs of security incidents to executive management to ensure support for enhanced control.
- e. Develop formal incident reporting procedures to ensure complete campus coverage, including the decentralized environments.

### **Campus Response**

The campus concurs and will develop and implement a campus-wide security incident response policy and guidelines for handling specific types of security incidents. The guidelines will document procedures to identify the types, volume, and costs of security incidents to ensure the campus monitors trends and risks, as well as to implement a process to report incidents to central executive management to raise awareness and ensure support. These actions will be completed by September 30, 2010.

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

BAKERSFIELD

March 29, 2010

CHANNEL ISLANDS

CHICO

**MEMORANDUM**

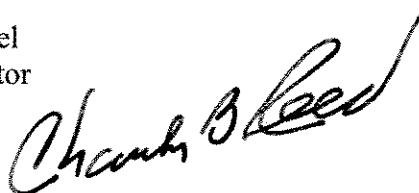
DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FROM: Charles B. Reed  
Chancellor



FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 09-36 on *Information Security*,  
California State University, Sacramento

LONG BEACH

LOS ANGELES

In response to your memorandum of March 29, 2010, I accept the response as submitted with the draft final report on *Information Security*, California State University, Sacramento.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS