

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

**Audit Report 09-38**  
**February 18, 2010**

---

**Members, Committee on Audit**

Henry Mendoza, Chair  
Raymond W. Holdsworth, Vice Chair  
Nicole M. Anderson Margaret Fortune  
George G. Gowgani Melinda Guzman  
William Hauck

---

**Staff**

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

---

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

---

# CONTENTS

Executive Summary ..... 1

Introduction..... 3

    Background ..... 3

    Purpose..... 4

    Scope and Methodology ..... 6

---

# OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

Security Governance..... 8

    Policy Issuance and Approval..... 8

    Record Retention ..... 8

    Employee Separation ..... 9

    Information Security Plan ..... 10

System Development and Change Management ..... 11

    Web Application Development and Maintenance..... 11

    Web Application Vulnerabilities ..... 13

Systems Security and Monitoring..... 14

    Control Over User Access ..... 14

    Firewalls and Routing and Switching Devices ..... 15

    Technical Vulnerabilities..... 17

    Password Standards ..... 18

    Vulnerability Management ..... 18

    Granting of Administrative Access..... 19

    Configuration Changes ..... 20

    Audit and Security Event Logs Management ..... 21

Protected Data..... 22

    Assessment and Inventory of Protected Information..... 22

    Lost/Stolen Computers ..... 22

    System Backup Encryption..... 23

    Disposition of Protected Data..... 24

    Incident Response Management ..... 25

## **APPENDICES**

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

---

## **ABBREVIATIONS**

ACL	Access Control List
CMS	Common Management Systems
CO	Office of the Chancellor
CSU	California State University
EO	Executive Order
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISRM	Information Security Risk Management
IT	Information Technology
ITRP	Infrastructure Terminal Resources Project
SQL	Structured Query Language

---

## EXECUTIVE SUMMARY

As a result of a system-wide 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 Office of the Chancellor (CO) and West Ed. data center from June 29, 2009 through July 31, 2009, and audited the procedures in effect at that time.

Our study and evaluation identified issues that, if left unattended, could impact the overall control environment. We identified a series of problems that were listed individually in this report; however, the underlying cause of many of the problems identified was the overall organization of the information security program. We also noted that the information security program did not sufficiently ensure that identified security issues were addressed in a timely manner.

In our opinion, the operational and administrative controls of information security in effect as of July 31, 2009, taken as a whole, were not sufficient to meet many of the objectives for a secured computing environment. While much of the CO's Information Technology department's control environment was satisfactory and provided appropriate safeguards over the critical financial and management systems, the practices of the information security office required improvement and greater 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 current information security policy was not comprehensive and did not adequately address information security topics. The CO did not address the annual review requirement of Executive Order 1031. Employees were not reminded of their ongoing legal responsibility for maintaining the security of protected data at the time of their separation. The CO's information security plan did not include projected timelines for addressing information security issues.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [10]**

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

## **SYSTEMS SECURITY AND MONITORING [14]**

The administration and management of user access profiles for systems other than the Common Management Systems required improvement. Firewalls and routing and switching devices were not always properly configured or adequately secured. Selected operating systems had technical vulnerabilities. The CO password policy had not been enforced on network devices and non-Windows production servers. The management of vulnerabilities required improvement. The CO lacked a formal process for granting privileged access. It also lacked policies and procedures defining a formal, periodic review of configuration changes for systems and network devices. Log management guidelines had not been formalized for managing, securing, and reviewing audit and security event logs of operating systems, servers, and applications.

## **PROTECTED DATA [22]**

The CO had not completed an overall security assessment of computers with sensitive information. The process to report lost/stolen equipment to the information security office to ensure the disposition of sensitive equipment was insufficient. Data backup tape copies, stored off-site, were not encrypted. Procedures to ensure that all sensitive information on computers was properly deleted prior to disposition required improvement. The asset management system did not track the disposition of desktop computers. The CO incident response process and procedures 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 and the Office of the Chancellor (CO) 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 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 CO. 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 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 system-wide distribution in late 2008. This timeline has now been extended an additional six months. Due to the pending status of this project during the time frame of the information security audits, these policies and standards were not used for evaluation of the campuses information security posture.

At the CO, the office of information technology services has overall responsibility for the management of computing systems and networks.

## **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, CO directives, and campus procedures.

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

- ▶ Certain essential administrative and managerial internal controls are in place, including delegations of authority and responsibility, formation of oversight committees, executive-level reporting, and documented policies and procedures.
- ▶ A management framework is established to initiate and control the implementation of information security within the organization; and management direction and support for information security is communicated in accordance with business requirements and relevant laws and regulations.
- ▶ All assets are accounted for and have a nominated owner/custodian who is granted responsibility for maintenance and control to achieve and maintain appropriate protection of organizational assets; and information is appropriately classified to indicate the need, priorities, and expected degree of protection when handling the information.

- ▶ Security responsibilities are addressed prior to employment so that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work; and procedures are in place to ensure that users' separation from the organization is managed and that the return of all equipment and the removal of all access rights are completed.
- ▶ Responsibilities and procedures for the management of information processing and service delivery are defined; and technical security controls are integrated within systems and networks.
- ▶ Access rights to networks, systems, applications, business processes, and data are controlled based on business and security requirements by means of user identification and authentication.
- ▶ Formal event reporting and escalation procedures are in place for information security events and weaknesses; and communication is accomplished in a consistent and effective manner, allowing timely corrective action to be taken.
- ▶ The design, operation, use, and management of information systems are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.
- ▶ Web application development and change management processes and procedures are adequate to ensure that application security and accessibility is considered during the design phase, that testing includes protection against known vulnerabilities, and that 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 reviewing the systems and managerial/technical measures for ongoing evaluation of data/information collected; identifying confidential, private, or sensitive information; authorizing access; securing information; detecting security breaches; and evaluating security incident reporting and response. Information security includes the activities/measures undertaken to protect the confidentiality, integrity, and access/availability of information, including measures to limit collection of information, control access to data and 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 contracted with technical specialists 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 Chancellor's Office assets. The assessment contained an internal component (within the network) and an external component (via the Internet) while encompassing a review of the security standards and processes that govern the CO. 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 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 MANAGEMENT RESPONSES**

## **SECURITY GOVERNANCE**

### **POLICY ISSUANCE AND APPROVAL**

The current information security policy was not comprehensive and did not adequately address information security topics.

The interim senior director of information security management stated that the Office of the Chancellor (CO) had updated its current information security policies. However, to ensure that the CO policy was fully compliant with the systemwide information security policy, formal approval had been deferred pending formal approval of the California State University (CSU) systemwide information security policy.

Failure to maintain a comprehensive information security policy increases the risk of inconsistent organizational practices governing information security and non-compliance with statutory information security requirements. Such inaction also affects the ability of the CO to measure the overall effectiveness of existing security provisions.

#### **Recommendation 1**

We recommend that the CO approve and communicate the comprehensive draft information security policy.

#### **Management Response**

We concur. The CO will adopt the systemwide information security policy and communicate the policy.

Remedial action will be completed by June 30, 2010.

### **RECORD RETENTION**

The CO had not completed an assessment of its compliance with Executive Order (EO) 1031.

During our review of record retention practices, we noted that:

- ▶ Three of three departments reviewed did not complete the annual review of records.
- ▶ Record retention schedules were not developed for the retention of e-mail systems. We noted that e-mail was retained for an indefinite period of time.
- ▶ Management had not assigned designated staff to provide necessary oversight in order ensure full compliance with EO 1031.

The interim senior director of information security management stated that the CO had not assigned responsibility for reviewing and assessing enterprise-wide compliance with EO 1031 to one person, but instead, the record retention responsibility was distributed among various department heads. She further stated that the development of an e-mail retention policy by the CO was undergoing consideration and discussion by management at the time of this audit.

Failure to meet compliance with EO 1031 increases the risk of inappropriate and untimely disposal of records and information.

### **Recommendation 2**

We recommend that the CO assign responsibility to an individual to ensure record retention action plans are completed and to ensure appropriate and timely disposal of records and information in accordance with CSU record retention and disposition schedules.

### **Management Response**

We concur. The CO's information security officer is now responsible for ensuring that departmental record retention action plans are complete, comply with EO 1031, and include procedures on the appropriate and timely disposal of records and information in accordance with CSU record retention and disposition schedules.

Remedial action will be completed by July 31, 2010.

## **EMPLOYEE SEPARATION**

The CO did not remind separating employees of their ongoing legal responsibility for maintaining the security of protected data.

The interim senior director of information security management stated that the CO believed the confidentiality agreement informed employees of their legal responsibility to maintain the security and privacy of protected information. She further stated that the CO was not aware that a reminder needed to be included in the employee separation process.

Failure to notify separating employees of their ongoing legal responsibility to maintain the security of protected data increases the risk that they will not comply with statutory information security requirements for any remaining access to, or unauthorized custody of, protected data.

### **Recommendation 3**

We recommend that the CO include in its personnel exit process a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data.

### **Management Response**

We concur. The CO will modify its personnel exit process to include a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data.

Remedial action will be completed by July 31, 2010.

### **INFORMATION SECURITY PLAN**

The CO lacked a process to identify and prioritize information security risks and an action plan to adequately address any identified risks within an established time frame.

The interim information security officer stated that although the CO had performed an informal risk assessment, it had not incorporated the results of the assessment into an information security action plan.

The lack of a formal action plan for identifying and prioritizing information security risks and for addressing the risks within an established timeline increases the potential for misunderstandings regarding campus information security direction. This also impacts the campus' ability to evaluate the overall effectiveness of existing security provisions related to protected data.

### **Recommendation 4**

We recommend that the CO establish a documented process to identify and prioritize information security risks, and create an action plan to adequately address any identified risks within an established time frame.

### **Management Response**

We concur. The information security officer will modify and document the CO information security risk management (ISRM) process. The revised CO ISRM process will include areas outside of information technology services, and will identify and prioritize information security risks. Future versions of the CO information security action plan will identify and address enterprise-wide risks and show target start, deployment, and completion dates.

Remedial action will be completed by July 31, 2010.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

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

Change management practices for web application development required improvement.

Specifically, we noted that:

- ▶ Developers had unlimited access to the source code in production environments and moved their own program changes to production.
- ▶ The production environment was not reviewed to ensure that only approved changes were migrated.
- ▶ Programming code testing was not consistently documented.
- ▶ Web security reviews were not performed to identify potential web application code vulnerabilities before moving code to production.
- ▶ End-user acceptance testing of program changes was not consistently documented.
- ▶ There was no source code version control process to ensure the integrity of source code.
- ▶ Some departments did not follow formal web application development change control procedures.
- ▶ One department did not have a test environment and made changes directly to production.

The interim senior director of information security management stated that although the CO had informal procedures in place that governed web development, software development practices had not been documented.

The lack of a formal web application development process and process control procedures increases the risk that web application changes may be unauthorized, may be inconsistent with user and management expectations, and may contain vulnerabilities.

#### **Recommendation 5**

We recommend that the CO:

- a. Develop procedures to correct segregation of duties conflicts for application development in these categories: exception monitoring, mitigating procedures, and review of developer-migrated changes, conducted by a reviewer outside the application development group.

- b. Develop formal documentation criteria for testing procedures used by all application development departments.
- c. Develop a security standard requiring that applications be reviewed for security vulnerabilities prior to deployment.
- d. Develop formal user-acceptance testing procedures for all departments.
- e. Implement version control to track changes and ensure the integrity of source code for all departments.
- f. Ensure all departments follow formal change control procedures.
- g. Create a development and test environment for all departments to ensure adequate testing before changes are moved to production.

**Management Response**

- a. We concur. The CO will develop procedures to address segregation of duties conflicts for application development. The procedures will include instructions on exception monitoring, mitigating procedures, and reviewing developer-migrated changes by an appropriate reviewer outside the application development group.

Remedial action will be completed by September 30, 2010.

- b. We concur. The CO will develop formal documentation criteria for testing procedures for application development projects.

Remedial action will be completed by September 30, 2010.

- c. We concur. The CO's application development standards will include a provision that requires applications be reviewed for security vulnerabilities prior to deployment.

Remedial action will be completed by September 30, 2010.

- d. We concur. The CO will develop formal user-acceptance procedures for application development projects.

Remedial action will be completed by September 30, 2010.

- e. We concur. The CO will implement version control to track changes and ensure the integrity of source code for application development projects.

Remedial action will be completed by September 30, 2010.

- f. We concur. The CO development teams will follow formal change control procedures.

Remedial action will be completed by July 31, 2010.

- g. We concur. The CO Information Technology Division will provide development and test environment for developers that need to test applications prior to deployment to a production environment.

Remedial action will be completed by September 30, 2010.

## **WEB APPLICATION VULNERABILITIES**

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

We found that the web application was subject to a structured query language (SQL) injection attack that increases the risk that protected information could be compromised.

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

### **Recommendation 6**

We recommend that the CO:

- a. Repair all of the web application vulnerabilities that were identified and presented in detail.
- b. Implement a comprehensive patch management process for all application development departments. This process would include a formalized documented review of existing web application code on a periodic basis or new code prior to deployment into the production environment, to identify potential or known vulnerabilities.

### **Management Response**

- a. We concur. The CO will repair all web application vulnerabilities that were identified in the audit.

Remedial action will be completed by September 30, 2010.

- b. We concur. The CO will develop a comprehensive patch management process for web applications. The process will include procedures to review (new or existing) web application code on a periodic basis, identify potential vulnerabilities, and remediate known risks.

Remedial action will be completed by September 30, 2010.

## **SYSTEMS SECURITY AND MONITORING**

### **CONTROL OVER USER ACCESS**

The administration and management of user access profiles for systems other than the Common Management Systems (CMS) required improvement.

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

- ▶ Data custodians had not performed periodic user access reviews for validating system access and/or permissions.
- ▶ Formal approval for new users who were given access to sensitive information was not obtained consistently.
- ▶ Confidentiality agreements for users had not been obtained consistently.
- ▶ Access to protected data of a transferred employee had not been removed within a timely manner.
- ▶ Access for one separated employee had not been removed within a timely manner.
- ▶ A separated employee's UNIX account was still active on the production server.

The interim senior director of information security management stated that competing priorities had diverted staff time from completing user access reviews of all non-CMS systems. She further stated that responsibility to manage user accounts was distributed to several individuals. She added that account management standards had not been rolled out to all non-CMS systems, as staff time had been focused on applying account management standards to the CMS systems.

Failure to periodically review user access and to properly administer provisioning of user accounts increases the risk of inappropriate access.

#### **Recommendation 7**

We recommend that the CO:

- a. Conduct and document periodic reviews of user access to systems containing protected data at least annually.
- b. Formalize a process for approving and removing user accounts.
- c. Ensure that user confidentiality agreements are completed and retained for those users with access to protected data.

### **Management Response**

- a. We concur. The CO will develop a process for conducting reviews of user access to systems containing protected data. The process will require the CO to conduct the reviews at least annually.

Remedial action will be completed by September 30, 2010.

- b. We concur. The CO will develop a formal process for approving and removing user accounts.

Remedial action will be completed by September 30, 2010.

- c. We concur. The CO's provisioning process will include a procedure to ensure that user confidentiality agreements are completed and retained.

Remedial action will be completed by September 30, 2010.

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

Firewalls and routing and switching devices were not always properly configured or adequately secured.

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

- ▶ Two network devices had users configured with dictionary-based passwords.
- ▶ One network device had no Access Control List (ACL) configured to restrict administrator access.
- ▶ Three devices and the border firewall were configured with clear-text Simple Network Management Protocol, which was unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ Two network devices were configured with weak passwords.
- ▶ One network device connection time-out setting had been configured for an excess amount of time.

The interim senior director of information security management stated that these vulnerabilities were due to a delay in configuration updates from the Infrastructure Terminal Resources Project (ITRP).

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 8**

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

In addition, we recommend that the CO:

- a. Ensure that all non-compliant systems and network devices adopt CO password standards.
- b. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- c. Implement a comprehensive, patch management process. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the live network environment, to identify potential or known vulnerabilities.

### **Management Response**

We concur. The CO will repair all network device vulnerabilities that were identified in the audit.

Remedial action will be completed by September 30, 2010.

- a. We concur. Where technically feasible, the CO will ensure that all systems and network devices adopt the CO password standards. The CO will document devices that cannot adopt the CO password standard due to technical constraints.

Remedial action will be completed by September 30, 2010.

- b. We concur. The CO's security standard for network devices will include a provision that requires network devices be reviewed for security vulnerabilities prior to deployment.

Remedial action will be completed by September 30, 2010.

- c. We concur. The CO will develop a comprehensive patch management process for network devices. The process will include procedures to review (new or existing) network devices on a periodic basis, identify potential vulnerabilities, and remediate known risks.

Remedial action will be completed by September 30, 2010.

## **TECHNICAL VULNERABILITIES**

Technical vulnerabilities existed on selected operating systems.

Our testing of selected servers disclosed the various vulnerabilities for which specific details were provided to the CO. Two remote desktop servers were running versions susceptible to a “man in the middle” attack. One domain controller was missing critical Windows security updates. One domain controller had an excess number of accounts with non-expiring passwords. One server lacked four critical Windows security updates.

The interim senior director of information security management stated that management’s lack of oversight and direction had permitted the majority of these vulnerabilities to propagate in the computing environments.

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

### **Recommendation 9**

We recommend that the CO repair all the technical vulnerabilities that were identified and presented in detail. In addition, we recommend that the CO:

- a. Formalize a security baseline standard and require the review of servers and computers for security vulnerabilities prior to deployment.
- b. Implement comprehensive patch management processes and procedures.

### **Management Response**

We concur. The CO will repair all technical vulnerabilities that were identified in the audit.

Remedial action will be completed by September 30, 2010.

- a. We concur. The CO’s security standard for servers and computers will include a provision that requires servers and computers be reviewed for security vulnerabilities prior to deployment.

Remedial action will be completed by September 30, 2010.

- b. We concur. The CO will develop a comprehensive patch management process for operating systems.

Remedial action will be completed by September 30, 2010.

## **PASSWORD STANDARDS**

The CO password policy had not been enforced and extended on all non-Windows production servers and network devices (i.e., routers and switches).

The interim senior director of information security management stated that CO password standards were being rolled out; however, some systems and network devices had not yet implemented the password standards.

The lack of a standard enforced password policy for critical applications increases the risk of easily guessed passwords and possible unauthorized access to network resources and confidential information.

### **Recommendation 10**

We recommend that the CO enforce existing password standards on all servers and network devices connected to the network.

### **Management Response**

We concur. Where technically feasible, the CO will ensure that all servers and network devices adopt the CO password standards. The CO will document servers and devices that cannot adopt the CO password standard due to technical constraints.

Remedial action will be completed by July 31, 2010.

## **VULNERABILITY MANAGEMENT**

The management of CO vulnerabilities required improvement.

During our review of the CO's vulnerability management practices, we found that:

- ▶ Formalized patch management procedures had not been developed for the Windows information technology server environment.
- ▶ Vulnerability remediation verification through network and host vulnerability scanning was not documented.
- ▶ Formal vulnerability assessments had not been conducted on level-one confidential data systems/applications.

The interim senior director of information security management stated that the CO used informal practices to patch Windows servers. She added that resource constraints limited the amount of time personnel could spend documenting remediation of vulnerabilities and manually reviewing intrusion

detection logs. She also stated that other priorities had made it difficult to focus staff time to develop formal requirements for vulnerability assessments.

Failure to address identified vulnerabilities may compromise network resources and lead to the loss of protected confidential information.

### **Recommendation 11**

We recommend that the CO:

- a. Formalize the patch management process and develop procedures for the Windows information technology server environment.
- b. Develop a method to document the remediation of vulnerabilities.
- c. Conduct vulnerability assessments on level-one confidential data systems/applications.

### **Management Response**

- a. We concur. The CO will formalize its patch management procedures for Windows servers.

Remedial action will be completed by September 30, 2010.

- b. We concur. The CO will update its vulnerability management procedures to ensure that remediation of vulnerabilities are documented.

Remedial action will be completed by September 30, 2010.

- c. We concur. The CO will conduct vulnerability assessments on application/systems that contain level 1 data.

Remedial action will be completed by September 30, 2010.

### **GRANTING OF ADMINISTRATIVE ACCESS**

The CO lacked a formal process for the granting and management of privileged system-level access to accounts.

The interim senior director of information security management stated that the lack of a formal process for granting privileged access caused the limited control documentation (i.e., logging and tracking).

The lack of a standard process for granting privileges may lead to inadequate segregation of duties or the granting of accounts not based on the principle of least privilege.

### **Recommendation 12**

We recommend that the CO establish a formal process for the granting of privileged system-level administrator access to accounts and that it develop a method to track, review, and periodically audit this type of access.

### **Management Response**

We concur. The CO will formalize its process for granting privileged system-level administrator access and develop a method to track, review, and periodically audit this type of access.

Remedial action will be completed by September 30, 2010.

## **CONFIGURATION CHANGES**

The CO lacked policies and procedures that defined a formal, periodic review of configuration changes for the firewalls, switches, routers and operating systems.

Informal periodic reviews of these systems and devices were performed at regular intervals as part of network operational responsibilities. However, this informal process was not adequate to ensure that network devices adhered to the latest configuration standards and updates.

The interim senior director of information security management stated that the lack of resources prevented a formal, periodic review process.

The lack of formal, documented periodic reviews of system and device configurations increases the risk of inconsistent and deprecated standards, which may permit malicious activity to go undetected.

### **Recommendation 13**

We recommend that the CO:

- 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 formal change management policies and procedures a formal sign-off process by appropriate CO personnel to ensure compliance with configuration reviews.

### **Management Response**

- a. We concur. The CO will modify its configuration management procedures to include a formal review of configuration standards.

Remedial action will be completed by September 30, 2010.

- b. We concur. The CO's change management procedures will be modified to include a formal sign-off process by appropriate CO personnel.

Remedial action will be completed by July 31, 2010.

## **AUDIT AND SECURITY EVENT LOGS MANAGEMENT**

Log management guidelines for managing, securing, and reviewing audit and security event logs of operating systems, servers, and applications were not formalized and required improvement.

We found that there were ongoing informal and undocumented practices for monitoring security logs and reviewing logs periodically for the intrusion detection system, network devices, border firewall, domain controllers, and production servers.

The interim senior director of information security management stated that the CO information technology (IT) staff reviewed audit logs when events were reported during the course of an investigation or when staff detected problems. She added that resource constraints limited the amount of time personnel could spend manually reviewing security event logs.

Inadequate management, security, and review of audit and security event logs increases the risk that malicious activity could go undetected or viruses or other malicious code could be embedded within the network and its resources, which could allow confidential information to be breached and not reported.

### **Recommendation 14**

We recommend that the CO:

- a. Establish a formal process to regularly review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of CO 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.

### **Management Response**

- a. We concur. The CO will develop a formal process to regularly review and analyze event logs to identify potential network vulnerabilities and breaches of CO systems.

Remedial action will be completed by September 30, 2010.

- b. We concur. The CO will examine the feasibility of acquiring tools to automate the review process.

Remedial action will be completed by September 30, 2010.

## **PROTECTED DATA**

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

The CO had not completed a formal security assessment to identify level-one protected data nor assigned data classifications to all information assets.

The interim senior director of information security management stated that the inventory of protected data was underway and the discovery phase was complete. She further stated that the CO was in the process of evaluating departmental controls used to safeguard level-one protected information assets.

Inadequate accountability of assets increases the risk of loss and inappropriate use of state resources, and increases the organization's exposure to information security breaches.

#### **Recommendation 15**

We recommend that the CO complete the assessment of the current inventory and the security of protected information, and also complete the assignment of data classifications to information assets.

#### **Management Response**

We concur. The CO will complete its inventory of level 1 and level 2 data.

Remedial action will be completed by September 30, 2010.

## **LOST/STOLEN COMPUTERS**

The CO process to report lost or stolen computers required improvement.

We noted several instances where lost/stolen computers had not been reported to the information security officer.

The interim senior director of information security management stated that the current process included an agreement between the information security officer and the IT service center to notify the information security officer whenever a computer was reported lost or stolen; however, the agreement was not formally documented.

Inadequate procedures for reporting and investigating lost or stolen equipment increases the risk that information security breaches could go unreported, resulting in significant financial penalty and damage to the organization's reputation.

**Recommendation 16**

We recommend that the CO develop a procedure to ensure that lost/stolen computers are consistently reported to the information security officer and that protected data was not compromised.

**Management Response**

We concur. The CO procedures have been modified to include instructions to notify the information security officer in the event of a lost/stolen laptop.

Remedial action will be completed by July 31, 2010.

**SYSTEM BACKUP ENCRYPTION**

Daily backup copies of systems with protected data stored off-site were not encrypted.

The interim senior director of information security management stated that the CO had not conducted a risk assessment to evaluate encryption as a safeguard for data backups. She further stated that the CO relied on other compensating controls (including administrative procedures and physical security) and the long-standing reputation of its tape storage vendor to provide a sufficient level of protection for backup tapes.

Inadequate security related to daily backups increases the likelihood of inappropriate access to protected data.

**Recommendation 17**

We recommend that the CO encrypt any system backups that contain protected data stored at off-site locations.

**Management Response**

We concur. The CO will encrypt backups that contain protected data that are stored off-site.

Remedial action will be completed by September 30, 2010.

## **DISPOSITION OF PROTECTED DATA**

The CO's process for ensuring that all sensitive information on computers and laptops was properly deleted prior to the computers' redeployment to other CSU campuses required improvement. Also, the asset management system did not track all IT resources valued below \$5,000 that could have contained sensitive information and should have been subject to the wiping process.

The interim senior director of information security management stated that although the CO had procedures in place to wipe and/or dispose of hard drives, they had not been formally documented.

The information security officer stated that property procedures required tracking concealable sensitive equipment that had a purchase price between \$500 and \$5,000. She further stated that the CO did not consider desktop computers to be concealable.

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

### **Recommendation 18**

We recommend that the CO:

- a. Update its process to ensure that hard-drive wiping is performed and sufficiently documented.
- b. Update property procedures to include the tracking of all sensitive equipment, especially those items that could contain sensitive information.

### **Management Response**

- a. We concur. The CO will update its procedures to ensure that hard-drive wiping is performed and documented.

Remedial action will be completed by July 31, 2010.

- b. We concur. The CO will update its property procedures to include tracking of all equipment classified as sensitive (e.g., equipment that contains protected data).

Remedial action will be completed by September 30, 2010.

## **INCIDENT RESPONSE MANAGEMENT**

The CO's incident response process required improvement.

We found that:

- ▶ No formalized comprehensive reporting process had been established to review and report on security incident metrics such as incident types, lessons learned, and costs incurred.
- ▶ The existing documented service desk procedures did not instruct service center personnel on how to reclassify a service ticket as a security incident or how to notify the information security officer in the event of a security incident.

The interim senior director of information security management stated that CO incident reports typically included information about an incident and recommendations. She further stated that the reports did not track other metrics such as incident costs. She added that the CO's incident response procedures did not assign responsibility for reclassifying service tickets in the event of a security incident/breach to service desk personnel.

Lack of a formalized monitoring and reporting process for security incidents increases the risk of loss and inappropriate use of state resources, and increases CO's exposure to information security breaches.

### **Recommendation 19**

We recommend that the CO:

- a. Develop a process to identify the types, lessons learned, frequency, and costs of security incidents so that it can monitor trends and risks.
- b. Develop a formal process to report security incidents to executive management.
- c. Update service desk procedures to reclassify a service ticket to a security incident, and direct service center personnel to notify the information security officer in the event of a security incident.

### **Management Response**

- a. We concur. The CO will modify its incident management procedures to track the types, lessons learned, frequency, and cost of information security incidents.

Remedial action will be completed by June 30, 2010.

- b. We concur. The CO will modify its incident management procedures to include a periodic reporting to executive management.

Remedial action will be completed by June 30, 2010.

- c. We concur. The CO will update the incident management procedures used by the service desk to include instructions to notify the information security officer in the event of an information security incident and help staff classify incident-related tickets.

Remedial action will be completed by June 30, 2010.

---

## APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Benjamin F. Quillian	Executive Vice Chancellor and Chief Financial Officer
George Ashkar	Assistant Vice Chancellor/Controller, Financial Services
Devon Arsenault	Senior System Administrator
David Avery	Personal Computer Site Administrator
Ron Basich	Director, Corporate Information Systems
Sue Bell	Assistant Director of Administration
Sheila Bickham	Director, Operations Support Services
Jaquelyn Bjazevich	Office Manager, General Counsel
Robert Boyhan	Director of Administration
Ben Cheng	Senior Financial Reporting Manager
Kelly Cox	Senior Accounting Manager
Mark Crase	Senior Director, Technology Infrastructure
Patricia Cuocco	Senior Director, Policy Planning and Advice
Michel Davidoff	Director, Cyberinfrastructure Services
Mike Deriso	Systems Administrator
Cuc Du	Information Security Officer
Richard Fletcher	Associate Director, Corporate Information Systems
Pat Garrabrandt	Office Manager, General Counsel (At time of review)
Gary Geidel	Director, User Support Services
Zachary Gifford	Assistant Systemwide Risk Manager Liability and Property
Jean Gill	Interim Assistant Controller
Ellyce Gordon	Property Clerk
Gerard Greenidge	Web Services Manager
Laura Guillory	Director, User Services
Gerry Hanley	Senior Director, Academic Technology
Alexander Harwood	Security Analyst
Kristy Hawman	Associate Director, Human Resources Services
Kim Hayes	Information Technology Service Center Operations Manager
Glen Hunter	Manager, Systems Support
Sedong John	Director, Systemwide Financial Standards and Reporting
Melody Kojima	Assistant Director, Purchasing
Cheryl Kwiatkowski	Senior Director, Enterprise Information Management
Jessie Lum	Interim Senior Director, Common Management Systems and Enterprise Systems
Michael McBride	Interim Director, Software Operations and Support Services
Michael McLean	Interim Chief Information Officer and Assistant Vice Chancellor Information Technology Services (At time of review)
Lisa Moske	Director, Systemwide Electronic Information Resources
Colleen Nickles	Assistant Vice Chancellor, Financial Services (At time of review)
Marvin Pollard	Unified Information Access System Project Manager
Michael Redmond	Interim Chief of Staff, Information Technology Services (At time of review)
Tom Roberts	Director, Contracts and Procurement

---

APPENDIX A: PERSONNEL CONTACTED

<b><u>Name</u></b>	<b><u>Title</u></b>
Stephen Schultz	Project Director, Security
Rebecca Skidmore	Risk Management Administrative Analyst
Jason Solis	Associate Director, Network and Telecommunications
Barbra Sperling	Manager of System Development
Berhanu Tadesse	Director, Data Center Services
Michael Trullinger	Associate Director, Identity Management
Cheryl Washington	Interim Senior Director, Information Security Management
Susan Westover	Team Leader, Litigation
Alice Yip	Lead Financial Reporting Analyst



**Business and Finance**  
401 Golden Shore, 5th Floor  
Long Beach, CA 90802-4210

[www.calstate.edu](http://www.calstate.edu)

**Benjamin F. Quillian**  
Executive Vice Chancellor and  
Chief Financial Officer

562-951-4600  
Fax 562-951-4971  
bquillian@calstate.edu

May 27, 2010

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

RECEIVED  
UNIVERSITY AUDITOR  
MAY 28 2010  
THE CALIFORNIA STATE  
UNIVERSITY

Subject: Campus Responses to Recommendations -  
Audit Report Number 09-38 Information Security  
at the Office of the Chancellor

Dear Mr. Mandel,

Enclosed is our response to the recommendations described in Audit Report 09-38, Information Security, at the Office of the Chancellor. Upon acceptance of our response, we will follow up with your office in providing supporting documentation for each recommendation by the anticipated completion dates.

Please let us know if you have any questions or need additional information.

Sincerely,

Benjamin F. Quillian  
Executive Vice Chancellor and  
Chief Financial Officer

Enclosure

c: Amir Dabirian, Assistant Vice Chancellor / CIO, Information Technology  
Cheryl Washington, Interim Senior Director, Systemwide Information Security Mgmt.

---

<b>CSU Campuses</b>	Fresno	Monterey Bay	San Francisco
Bakersfield	Fullerton	Northridge	San José
Channel Islands	Humboldt	Pomona	San Luis Obispo
Chico	Long Beach	Sacramento	San Marcos
Dominguez Hills	Los Angeles	San Bernardino	Sonoma
East Bay	Maritime Academy	San Diego	Stanislaus

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

**Audit Report 09-38**

**SECURITY GOVERNANCE**

**POLICY ISSUANCE AND APPROVAL**

**Recommendation 1**

We recommend that the CO approve and communicate the comprehensive draft information security policy.

**Management Response**

We concur. The CO will adopt the system-wide information security policy and communicate the policy.

Remedial action will be completed by June 30, 2010

**RECORD RETENTION**

**Recommendation 2**

We recommend that the CO assign responsibility to an individual to ensure record retention action plans are completed and to ensure appropriate and timely disposal of records and information in accordance with CSU record retention and disposition schedules.

**Management Response**

We concur. The CO's Information Security Officer is now responsible for ensuring that departmental record retention action plans are complete, comply with EO 1031, and include procedures on the appropriate and timely disposal of records and information in accordance with CSU record retention and disposition schedules.

Remedial action will be completed by July 31, 2010

## **EMPLOYEE SEPARATION**

### **Recommendation 3**

We recommend that the CO include in its personnel exit process a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data.

### **Management Response**

We concur. The CO will modify its personnel exit process to include a reminder to separating employees of their ongoing legal responsibility to maintain the security of protected data.

Remedial action will be completed by July 31, 2010

## **INFORMATION SECURITY PLAN**

### **Recommendation 4**

We recommend that the CO establish a documented process to identify and prioritize information security risks, and create an action plan to adequately address any identified risks within an established time frame.

### **Management Response**

We concur. The information security officer will modify and document the CO information security risk management (ISRM) process. The revised CO ISRM process will include areas outside of Information Technology Services, and identify and prioritize information security risks. Future versions of the CO information security action plan will identify and address enterprise-wide risks and show target start, deployment and completion dates.

Remedial action will be completed by July 31, 2010

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

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

#### **Recommendation 5**

We recommend that the CO:

- a. Develop procedures to correct segregation of duties conflicts for application development in these categories: exception monitoring, mitigating procedures, and review of developer-migrated changes, conducted by a reviewer outside the application development group.
- b. Develop formal documentation criteria for testing procedures used by all application development departments.

- c. Develop a security standard requiring that applications be reviewed for security vulnerabilities prior to deployment.
- d. Develop formal user-acceptance testing procedures for all departments.
- e. Implement version control to track changes and ensure the integrity of source code for all departments.
- f. Ensure all departments follow formal change control procedures.
- g. Create a development and test environment for all departments to ensure adequate testing before changes are moved to production.

**Management Response**

- a. We concur. The CO will develop procedures to address segregation of duties conflicts for application development. The procedures will include instructions on exception monitoring, mitigating procedures, and reviewing developer-migrated changes by an appropriate reviewer outside the application development group.

Remedial action will be completed by September 30, 2010

- b. We concur. The CO will develop formal documentation criteria for testing procedures for application development projects.

Remedial action will be completed by September 30, 2010

- c. We concur. The CO's application development standards will include a provision that requires applications be reviewed for security vulnerabilities prior to deployment.

Remedial action will be completed by September 30, 2010

- d. We concur. The CO will develop formal user-acceptance procedures for application development projects.

Remedial action will be completed by September 30, 2010

- e. We concur. The CO will implement version control to track changes and ensure the integrity of source code for application development projects

Remedial action will be completed by September 30, 2010

- f. We concur. The CO development teams will follow formal change control procedures.

Remedial action will be completed by July 31, 2010

- g. We concur. The CO Information Technology Division will provide development and test environment for developers that need to test applications prior to deployment to a production environment.

Remedial action will be completed by September 30, 2010

## **WEB APPLICATION VULNERABILITIES**

### **Recommendation 6**

We recommend that the CO:

- a. Repair all of the web application vulnerabilities that were identified and presented in detail.
- b. Implement a comprehensive patch management process for all application development departments. This process would include a formalized documented review of existing web application code on a periodic basis or new code prior to deployment into the production environment, to identify potential or known vulnerabilities.

### **Management Response**

- a. We concur. The CO will repair all web application vulnerabilities that were identified in the audit.

Remedial action will be completed by September 30, 2010

- b. We concur. The CO will develop a comprehensive patch management process for web applications. The process will include procedures to review (new or existing) web application code on a periodic basis, identify potential vulnerabilities, and remediate known risks.

Remedial action will be completed by September 30, 2010

## **SYSTEMS SECURITY AND MONITORING**

### **CONTROL OVER USER ACCESS**

#### **Recommendation 7**

We recommend that the CO:

- a. Conduct and document periodic reviews of user access to systems containing protected data at least annually.
- b. Formalize a process for approving and removing user accounts.
- c. Ensure that user confidentiality agreements are completed and retained for those users with access to protected data.

**Management Response**

- a. We concur. The CO will develop a process for conducting reviews of user access to systems containing protected data. The process will require the CO to conduct the reviews at least annually.

Remedial action will be completed by September 30, 2010

- b. We concur. The CO will develop a formal process for approving and removing user accounts.

Remedial action will be completed by September 30, 2010

- c. We concur. The CO's provisioning process will include a procedure to ensure that user confidentiality agreements are completed and retained.

Remedial action will be completed by September 30, 2010

**FIREWALLS AND ROUTING AND SWITCHING DEVICES**

**Recommendation 8**

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

In addition, we recommend that the CO:

- a. Ensure that all non-compliant systems and network devices adopt CO password standards.
- b. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- c. Implement a comprehensive, patch management process. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the live network environment, to identify potential or known vulnerabilities.

**Management Response**

We concur. The CO will repair all network device vulnerabilities that were identified in the audit.

Remedial action will be completed by September 30, 2010

- a. We concur. Where technically feasible, the CO will ensure that all systems and network devices adopt the CO password standards. The CO will document devices that cannot adopt the CO password standard due to technical constraints.

Remedial action will be completed by September 30, 2010

- b. We concur. The CO's security standard for network devices will include a provision that requires network devices be reviewed for security vulnerabilities prior to deployment.

Remedial action will be completed by September 30, 2010

- c. We concur. The CO will develop a comprehensive patch management process for network devices. The process will include procedures to review (new or existing) network devices on a periodic basis, identify potential vulnerabilities, and remediate known risks

Remedial action will be completed by September 30, 2010

## **TECHNICAL VULNERABILITIES**

### **Recommendation 9**

We recommend that the CO repair all the technical vulnerabilities that were identified and presented in detail.

In addition, we recommend that the CO:

- a. Formalize a security baseline standard and require the review of servers and computers for security vulnerabilities prior to deployment.
- b. Implement comprehensive patch management processes and procedures.

### **Management Response**

We concur. The CO will repair all technical vulnerabilities that were identified in the audit.

Remedial action will be completed by September 30, 2010

- a. We concur. The CO's security standard for servers and computers will include a provision that requires servers and computers be reviewed for security vulnerabilities prior to deployment.

Remedial action will be completed by September 30, 2010

- b. We concur. The CO will develop a comprehensive patch management process for operating systems.

Remedial action will be completed by September 30, 2010

## PASSWORD STANDARDS

### Recommendation 10

We recommend that the CO enforce existing password standards on all servers and network devices connected to the network.

### Management Response

We concur. Where technically feasible, the CO will ensure that all servers and network devices adopt the CO password standards. The CO will document servers and devices that cannot adopt the CO password standard due to technical constraints.

Remedial action will be completed by July 31, 2010

## VULNERABILITY MANAGEMENT

### Recommendation 11

We recommend that the CO:

- a. Formalize the patch management process and develop procedures for the Windows information technology server environment.
- b. Develop a method to document the remediation of vulnerabilities.
- c. Conduct vulnerability assessments on level-one confidential data systems/applications.

### Management Response

- a. We concur. The CO will formalize its patch management procedures for Windows servers.

Remedial action will be completed by September 30, 2010

- b. We concur. The CO will update its vulnerability management procedures to ensure that remediation of vulnerabilities are documented.

Remedial action will be completed by September 30, 2010

- c. We concur. The CO will conduct vulnerability assessments on application/systems that contain level 1 data.

Remedial action will be completed by September 30, 2010

## GRANTING OF ADMINISTRATIVE ACCESS

### Recommendation 12

We recommend that the CO establish a formal process for the granting of privileged system-level administrator access to accounts and that it develop a method to track, review, and periodically audit this type of access.

### Management Response

We concur. The CO will formalize its process for granting privileged system-level administrator access and develop a method to track, review, and periodically audit this type of access.

Remedial action will be completed by September 30, 2010

## CONFIGURATION CHANGES

### Recommendation 13

We recommend that the CO:

- 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 formal change management policies and procedures a formal sign-off process by appropriate CO personnel to ensure compliance with configuration reviews.

### Management Response

- a. We concur. The CO will modify its configuration management procedures to include a formal review of configuration standards.

Remedial action will be completed by September 30, 2010

- b. We concur. The CO's change management procedures will be modified to include a formal sign-off process by appropriate CO personnel.

Remedial action will be completed by July 31, 2010

## AUDIT AND SECURITY EVENT LOGS MANAGEMENT

### Recommendation 14

We recommend that the CO:

- a. Establish a formal process to regularly review and analyze the security event logs in order to identify potential network vulnerabilities and breaches of CO 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.

**Management Response**

- a. We concur. The CO will develop a formal process to regularly review and analyze event logs to identify potential network vulnerabilities and breaches of CO systems.

Remedial action will be completed by September 30, 2010

- b. We concur. The CO will examine the feasibility of acquiring tools to automate the review process.

Remedial action will be completed by September 30, 2010

**PROTECTED DATA**

**ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION**

**Recommendation 15**

We recommend that the CO complete the assessment of the current inventory and the security of protected information, and also complete the assignment of data classifications to information assets.

**Management Response**

We concur. The CO will complete its inventory of level 1 and level 2 data.

Remedial action will be completed by September 30, 2010

**LOST/STOLEN COMPUTERS**

**Recommendation 16**

We recommend that the CO develop a procedure to ensure that lost/stolen computers are consistently reported to the information security officer and that protected data was not compromised.

**Management Response**

We concur. The CO procedures have been modified to include instructions to notify the information security officer in the event of a lost/stolen laptop.

Remedial action will be completed by July 31, 2010

## SYSTEM BACKUP ENCRYPTION

### Recommendation 17

We recommend that the CO encrypt any system backups that contain protected data stored at off-site locations.

### Management Response

We concur. The CO will encrypt backups that contain protected data that are stored off-site.

Remedial action will be completed by September 30, 2010

## DISPOSITION OF PROTECTED DATA

### Recommendation 18

We recommend that the CO:

- a. Update its process to ensure that hard-drive wiping is performed and sufficiently documented.
- b. Update property procedures to include the tracking of all sensitive equipment, especially those items that could contain sensitive information.

### Management Response

- a. We concur. The CO will update its procedures to ensure that hard-drive wiping is performed and documented.

Remedial action will be completed by July 31, 2010

- b. We concur. The CO will update its property procedures to include tracking of all equipment classified as sensitive (e.g., equipment that contains protected data).

Remedial action will be completed by September 30, 2010

## INCIDENT RESPONSE MANAGEMENT

### Recommendation 19

We recommend that the CO:

- a. Develop a process to identify the types, lessons learned, frequency, and costs of security incidents so that it can monitor trends and risks.
- b. Develop a formal process to report security incidents to executive management.

- c. Update service desk procedures to reclassify a service ticket to a security incident, and direct service center personnel to notify the information security officer in the event of a security incident.

**Management Response**

- a. We concur. The CO will modify its incident management procedures to track the types, lessons learned, frequency, and cost of information security incidents.

Remedial action will be completed by June 30, 2010

- b. We concur. The CO will modify its incident management procedures to include a periodic reporting to executive management.

Remedial action will be completed by June 30, 2010

- c. We concur. The CO will update the incident management procedures used by the service desk to include instructions to notify the ISO in the event of an information security incident and help staff classify incident related tickets.

Remedial action will be completed by June 30, 2010

THE CALIFORNIA STATE UNIVERSITY  
OFFICE OF THE CHANCELLOR



BAKERSFIELD

CHANNEL ISLANDS

July 2, 2010

CHICO

DOMINGUEZ HILLS

**MEMORANDUM**

EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FULLERTON

FROM: Charles B. Reed  
Chancellor

HUMBOLDT

SUBJECT: Draft Final Report 09-38 on *Information Security*,  
Office of the Chancellor

LONG BEACH

LOS ANGELES

MARITIME ACADEMY

In response to your memorandum of July 2, 2010, I accept the response as submitted with the draft final report on *Information Security*, Office of the Chancellor.

MONTEREY BAY

NORTHRIDGE

POMONA

CBR/amd

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS