

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**DOMINGUEZ HILLS**

**Audit Report 08-23**  
**May 22, 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 Authority and Responsibility .....	8
Payment Card Industry Data Security Standards .....	8
Information Security Awareness Training .....	9
Employee Separation.....	10
Information Security Plan .....	10
Decentralized Computing.....	11
Confidential Information .....	11
Technical Vulnerabilities .....	11
System Development and Change Management.....	13
Web Application Development and Maintenance.....	13
Web Application Vulnerabilities.....	14
Systems Security and Monitoring .....	15
Configuration Changes.....	15
Control of User Access.....	16
Vulnerability Management.....	17
Network Monitoring.....	18
Granting of Administrative Access .....	19
Firewalls and Routing and Switching Devices.....	19
Network Architecture .....	20
Review of Security Event Logs.....	21
Protected Data .....	22
System Backup Encryption .....	22
Incident Response Management.....	22

## **APPENDICES**

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

---

## **ABBREVIATIONS**

CIO	Chief Information Officer
CMS	Common Management System
CSU	California State University
DMZ	Demilitarized Zone
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITRP	Infrastructure Terminal Resource Project
PCI DSS	Payment Card Industry Data Security

---

## 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, Dominguez Hills campus from October 27 2008, through December 5, 2008, and audited the procedures in effect at that time.

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

In our opinion, the operational and administrative controls of information security in effect as of December 5, 2008, taken as a whole, were sufficient to meet the objectives stated below.

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 did not have a full-time, dedicated information security officer; and security responsibilities for individuals assuming the roles of the information security officer function had not been clearly defined and documented. Further, the campus and auxiliaries had not completed a Payment Card Industry Data Security Standards compliance summary plan to define its applicable vendor level and respective contractual requirements. In addition, information security awareness training had not been completed by all employees with access to critical systems or protected data, and the campus did not remind employees of their ongoing legal responsibility for maintaining the security of protected data at the time of their separation. The campus also lacked a process to identify and prioritize information security risks and create an action plan to adequately address any identified risks within an established timeline.

## **DECENTRALIZED COMPUTING [11]**

The campus process to identify, approve, and review access to confidential information was not applied to systems owned and managed by its decentralized sites. In addition, technical vulnerabilities existed on a variety of decentralized systems throughout the campus, which were not maintained by the central information technology team, and were not held to the same programming standard, code review, or security configuration standards.

## **SYSTEMS DEVELOPMENT AND CHANGE MANAGEMENT [13]**

Change management procedures for web application development did not ensure adequate documentation of approval, testing, user acceptance and deployment; appropriately limit developer abilities; and require encryption for authentication to certain web applications. Further, web application vulnerabilities existed on the website selected for testing.

## **SYSTEMS SECURITY AND MONITORING [15]**

Policies and procedures had not been developed to address the periodic review and approval of configuration changes for systems and devices. Further, administration of user access to certain systems and applications containing protected data was inadequate, and periodic assessments to detect vulnerabilities or exploits related to security of servers and desktops connected to the campus network were not performed. In addition, administration of IT assets on the campus network was inadequate, policies and procedures had not been developed to address the granting and management of privileged access to accounts, and firewalls and routing and switching devices were not always properly configured or adequately secured. Also, internet-accessible devices were located within the same segments as internal resources, and periodic reviews of security event logs were not regularly performed and documented.

## **PROTECTED DATA [22]**

Daily backup copies for all campus administrative systems containing protected data were not encrypted when stored off-site. In addition, campus procedures for handling security incidents did not ensure appropriate handling and adequate monitoring and reporting.

---

## 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 decentralized 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; IT security; configuration management and change control; access control; asset management; management of information systems; information security incident management; physical security; business continuity and disaster recovery; and legal and regulatory compliance. The Information Technology Advisory Committee, composed of the chief information officers from each campus, and the Information Security Advisory Committee, composed of the information security officers from each campus, was integrally involved in this policy development process in order to ensure that the final product was an appropriate fit for the CSU. This project began in September 2007 with the expectation that these policies and standards were to be completed by August 2008 for subsequent adoption and official systemwide distribution in late 2008. This timeline has now been extended an additional six months. Due to the pending status of this project during the time frame of the information security audits, these policies and standards were not used for evaluation of the campuses information security posture.

At California State University, Dominguez Hills, 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 decentralized 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, are equipped to support organizational security policy in the course of their normal work, and responsibilities are in place to ensure user's exit 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 exist 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.

## **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 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 KPMG to perform a technical security assessment that included running diagnostic software designed to identify improper configuration of selected systems, servers, and network devices. The purpose of the technical security assessment was to determine the effectiveness of technology and security controls governing the confidentiality, integrity, and availability of selected campus assets. The assessment contained an internal component (within the campus network) and an external component (via the Internet) while encompassing a review of the security standards and processes that govern the California State University, Dominguez Hills 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 AUTHORITY AND RESPONSIBILITY**

The campus did not have a full-time, dedicated information security officer; and security responsibilities for individuals assuming the roles of the information security officer function had not been clearly defined and documented.

The chief information officer (CIO) stated that the position of information security officer had been vacant for some time; and due to budget constraints, he and the director of instructional computing and network services currently share the information security responsibilities.

The lack of a full-time, dedicated information security officer and clearly defined security responsibilities increases the risk of misunderstandings regarding information security responsibilities, and limits the campus' ability to direct a comprehensive system of information security management throughout the campus community, consistently apply security governance, and prioritize information security prerogatives.

#### **Recommendation 1**

We recommend that the campus appoint a full-time information security officer dedicated to fulfilling information security responsibilities and clearly define and document security responsibilities for this individual or other individuals assuming the roles of the information security officer function.

#### **Campus Response**

We concur. The campus will review workload capabilities in light of budgetary constraints and consider appointing a full-time information security officer or an individual to assume the role dedicated to fulfilling information security responsibilities, and clearly define and document security responsibilities for this individual.

Expected completion date: November 2009

#### **PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS**

The campus and auxiliaries had not completed a Payment Card Industry (PCI) Data Security Standards (DSS) compliance summary plan to define its applicable vendor level and respective contractual requirements.

We found that:

- ▶ An annual risk assessment was not performed to determine comprehensive compliance obligations for credit card data maintained on servers and transmitted throughout the campus network as required by PCI DSS.

- ▶ Responsibility for assessing campus and auxiliary PCI DSS compliance was not defined.

The CIO stated that although the campus had implemented measures to provide a PCI DSS compliant gateway for credit card transactions through TouchNet, an assessment of other credit card processors on campus had not been completed.

Failure to comply with PCI DSS requirements exposes the campus to potential financial penalties and credit card usage restrictions, which could include termination of the campus' ability to accept credit cards.

### **Recommendation 2**

We recommend that the campus:

- a. Complete a PCI DSS compliance summary plan to define its applicable vendor level and respective PCI DSS requirements.
- b. Define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

### **Campus Response**

We concur. The campus will:

- a. Complete a PCI DSS compliance summary plan to define the applicable vendor level and respective PCI DSS requirements.
- b. Define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

Expected completion date: November 2009

## **INFORMATION SECURITY AWARENESS TRAINING**

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

The CIO stated that although security awareness training had been conducted regularly, it had not been a mandatory requirement of employment, which made it difficult to enforce for all employees.

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

### **Recommendation 3**

We recommend that the campus ensure that information security awareness training is completed by all employees with access to critical systems or protected data.

### **Campus Response**

We concur. The campus is currently monitoring the CSU-developed security awareness training deployed on campus by Workplace Answers to ensure that all employees with access to critical systems or protected data are trained.

Expected completion date: November 2009

### **EMPLOYEE SEPARATION**

Employees were not reminded of their ongoing legal responsibility for maintaining the security of protected data at the time of their separation.

The CIO stated that this requirement was discussed in human resources confidentiality training, but had not yet been formalized in separation documentation.

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

### **Recommendation 4**

We recommend that the campus modify its personnel exit process to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data.

### **Campus Response**

We concur. The campus has completed the modification of the personnel exit process to inform separating employees of their ongoing legal responsibility for maintaining security of protected data.

Corrective action has been completed.

### **INFORMATION SECURITY PLAN**

The campus lacked a process to identify and prioritize information security risks and create an action plan to adequately address any identified risks within an established timeline.

The CIO stated that although an informal risk assessment had been performed, it had not been incorporated into an information security action plan.

The lack of a process to identify and prioritize information security risks and create an action plan to adequately address any identified risks within an established timeline increases the risk of misunderstandings regarding campus information security risks and impacts the campus' ability to opine on the overall effectiveness of existing security provisions related to protected data.

### **Recommendation 5**

We recommend that the campus 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 timeline.

### **Campus Response**

We concur. The individual assuming the role of the information security officer will develop a documented process to identify and prioritize information security risks and create a plan to address any identified risks within an established timeframe.

Expected completion date: November 2009

## **DECENTRALIZED COMPUTING**

### **CONFIDENTIAL INFORMATION**

The campus process to identify, approve, and review access to confidential information was not applied to systems owned and managed by its decentralized sites.

The CIO stated that the decentralized sites were following separate policies for securing their systems, which did not completely align with campus-wide policy for controlling confidential information.

Inadequate control over access to confidential information increases the risk that the data may be compromised without detection.

### **Recommendation 6**

We recommend that the campus follow their documented process to identify, approve, and review access to confidential information owned and managed by its decentralized sites.

### **Campus Response**

We concur. The campus will follow the documented process to identify, approve, and review access to confidential information owned and managed by the ancillary sites.

Expected completion date: November 2009

### **TECHNICAL VULNERABILITIES**

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

Our external testing of selected servers disclosed 55 vulnerabilities on a variety of servers for which specific details were provided to the campus.

Additionally, deployment of servers in the decentralized computing environment was inadequately managed and lacked professional standards and guidance. The decentralized servers were not consistently patched, there was no baseline security standard for server security or application security, and professional application development standards and methodologies were absent or inadequate.

The CIO stated that misinterpretation of the policy by the decentralized administrators created a gap in the security of these systems.

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

#### **Recommendation 7**

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Develop and implement a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This process would 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 or known vulnerabilities.
- c. Develop and implement a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the decentralized IT units with a security baseline standard for securing servers prior to allowing them to become Internet facing.

#### **Campus Response**

We concur. The campus will repair the technical vulnerabilities detected by the KPMG scan.

In addition, we will:

- a. Document and implement a campus-wide patch management process.

- b. Develop and implement a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. The process will include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment.
- c. Develop a campus-wide Internet-facing web application development standard to which all developers must comply prior to deploying any web application and submit the web application for official campus approval.
- d. Enforce the security baseline standard for securing servers to all ancillary sites prior to allowing them to become Internet facing.

Expected completion date: November 2009

## **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 web application development:

- ▶ Written approval was not required for projects put into production.
- ▶ Testing criteria for the security of web applications were not documented.
- ▶ User acceptance and deployment were not documented.
- ▶ Developers had unlimited access to source code.
- ▶ Developers had the ability to move applications into production.
- ▶ Encryption had not been utilized for authentication to certain web applications.

The CIO stated that limited staffing contributed to the noted deficiencies in the change management procedures.

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

#### **Recommendation 8**

We recommend that the campus:

- a. Require documented approval of all web application projects put into production.
- b. Establish and document testing criteria for the security of web applications, including but not limited to, input and output validation tests.

- c. Establish a documented process for user acceptance and deployment 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.
- f. Ensure that encryption is utilized for authentication to all web applications.
- g. 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. The campus will:

- a. Require documented approval of all web projects prior to deployment.
- b. Establish and document a comprehensive testing criteria plan for security of web applications.
- c. Establish and document a process for user acceptance and deployment of web applications.
- d. Restrict access to web application source code to only those employees who need it as part of their job responsibilities.
- e. Define work flow to limit developers ability to place web applications into development.
- f. Ensure that encryption is utilized for authentication to all web applications.
- g. Create a process to formally review and centrally approve all web applications prior to user acceptance through baseline security standards for web applications that are being developed by the campus.

Expected completion date: November 2009

### **WEB APPLICATION VULNERABILITIES**

Web application vulnerabilities existed on the website selected for testing.

The web application reviewed allowed TRACE and TRACK methods, cross-site scripting, secured page browser cache, and Structured Query Language injection.

The CIO stated that these vulnerabilities were the result of various causes including delays in patching servers and/or applications by areas not within central IT control.

Web application vulnerabilities increase the risk that a remote attacker may be able to exploit vulnerabilities that could lead to loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

#### **Recommendation 9**

We recommend that the campus:

- a. Repair the web application vulnerabilities that were identified and presented in detail to the campus.
- b. Develop and implement 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 or known vulnerabilities.

#### **Campus Response**

We concur. The campus will:

- a. Repair the web application vulnerabilities that were identified and detected.
- b. Develop and implement a campus-wide Internet-facing web application development standard to which all developers must comply prior to deploying any web application and submit the web application for official campus approval.

Expected completion date: November 2009

## **SYSTEMS SECURITY AND MONITORING**

### **CONFIGURATION CHANGES**

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

Specifically, policies and procedures should address the following:

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

We noted that the periodic reviews of these systems and devices were informally occurring 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 CIO stated that the campus had not documented these processes due to the limited staff that are working on these systems and their familiarity with the campus network.

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

### **Recommendation 10**

We recommend that the campus develop and document policies and procedures for the periodic review and approval of system configuration changes that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.

### **Campus Response**

We concur. The campus has purchased scanning software that will assist in the process of identifying misconfigured network devices and will update policies and procedures for the periodic review and approval of system configuration changes.

Expected completion date: November 2009

## **CONTROL OF USER ACCESS**

Administration of user access to certain decentralized systems and applications containing protected data was inadequate.

We found that:

- ▶ The process for adding and removing user access was not consistently documented.
- ▶ Periodic management review for validating system access and/or permissions was not consistently performed.

The CIO stated that some of the systems reviewed were not part of the centralized Common Management Systems (CMS) user access requirements. He added that these systems were not subject to the same access review process as CMS, and policies on user access had not been created in these areas.

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

**Recommendation 11**

We recommend that the campus:

- a. Establish a documented process for adding and removing user accounts to decentralized systems.
- b. Perform and document periodic management reviews of user access to all systems and applications containing protected data.

**Campus Response**

We concur. The campus will:

- a. Create and document a process for managing user accounts for all ancillary systems.
- b. Perform and document a process that will include periodic management reviews of user access to all systems and applications containing protected data.

Expected completion date: November 2009

**VULNERABILITY MANAGEMENT**

Periodic assessments to detect vulnerabilities or exploits related to security of servers and desktops connected to the campus network were not performed.

We noted that while assessments may be performed on an as-needed basis, there was no established process for periodic monitoring, detecting, and remediating campus-wide vulnerabilities and exploits to ensure compliance with campus-wide policies.

The CIO stated that periodic vulnerability assessments were not completed due to the staffing levels needed to perform such scans.

Failure to perform periodic assessments to detect vulnerabilities and exploits may lead to compromise in network resources and loss of protected confidential information.

**Recommendation 12**

We recommend that the campus establish a documented process to perform periodic assessments to detect vulnerabilities and exploits on all servers and desktops connected to the campus network.

**Campus Response**

We concur. The campus will create and document processes for periodic assessments to detect vulnerabilities and exploits on all servers and desktops connected to the campus network.

Expected completion date: November 2009

## **NETWORK MONITORING**

Administration of IT assets on the campus network was inadequate.

We found that:

- ▶ All IT assets on the campus network, whether owned and managed by central IT or decentralized IT sites, were not identified or monitored.
- ▶ Web servers were not scanned prior to deployment to ensure that minimum system operating standards are met.

The CIO stated that system administrators are directed by campus policy to adhere to baseline server hardening, and that central IT has only recently established a policy to ensure that hardening is occurring on new systems when they are assigned an IP address. He also stated that servers that were put in service prior to this policy have not yet been scanned.

Inadequate administration of network IT assets increases the risk that the campus could become vulnerable to both internal and external attacks which could slow or shutdown the network; and increases the risk that an attacker could inject malicious code or viruses into the network or compromise confidential information.

### **Recommendation 13**

We recommend that the campus establish documented processes to:

- a. Identify and monitor all IT assets (including hardware, software, operating system versions, etc.) on the campus network.
- b. Scan web servers prior to deployment to ensure minimum system operating standards are met.

### **Campus Response**

We concur. The campus will:

- a. Identify and monitor all IT assets on the campus network and place them into appropriate firewall zones as part of the data center redesign project.
- b. Enforce the security baseline standard for securing web servers prior to deployment.

Expected completion date: November 2009

## **GRANTING OF ADMINISTRATIVE ACCESS**

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

The CIO stated that the current process had generally been informal due to the limited number of individuals who had privileged access.

The lack of policies and procedures for the granting and management of privileged access 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 develop and document policies and procedures to address the granting and management of privileged access to accounts, taking into consideration the criteria for individuals who should have access, roles, and responsibilities for these resources; and develop a method to track, review, and periodically audit this type of access.

### **Campus Response**

We concur. The campus will develop a standard for the management of privileged access to accounts. The director in each IT department that controls administrative and service accounts will ensure that a formal process for tracking, reviewing, and auditing access to these types of accounts exists.

Expected completion date: November 2009

## **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 selected routing and switching devices disclosed that:

- ▶ Three devices were configured with Simple Network Management Protocol, which was unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ One device was enabled with Telecommunication Network, which could allow a remote attacker to obtain confidential authentication tokens to permit remote access to the devices since the user logins, passwords, and commands are transferred across the network in clear text.
- ▶ One device was not configured with Access Control List to restrict administrative access.

- ▶ One device was running an older version of OpenSSH, which could allow an attacker to gain root shell access.

The CIO stated that at the time of the audit, the firewalls and switches were scheduled for replacement through the Infrastructure Terminal Resource Project (ITRP) process and that vulnerabilities would be addressed during the completion of this project.

These configuration and security exposures increase the risk that a remote attacker may be able to gain access to network resources and exploit vulnerabilities that could lead to the loss of protected confidential information and the execution of malicious programs on the server that could potentially disable additional network resources.

### **Recommendation 15**

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

In addition, we recommend that the campus:

- a. Develop and implement a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment. 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.
- b. Implement a comprehensive, campus-wide patch management process.

### **Campus Response**

We concur. The campus will repair all network device vulnerabilities as identified. Additionally the campus will:

- a. Develop and implement a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment. The process will 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.
- b. Create and implement a comprehensive campus-wide patch management process.

Expected completion date: November 2009

## **NETWORK ARCHITECTURE**

Internet-accessible devices were located within the same segments as internal resources.

Normally, Internet-accessible devices are segmented into a demilitarized zone (DMZ) such that, if the devices are compromised, there is separation among other internal network resources.

The CIO stated that the campus had not deployed a DMZ in anticipation of the ITRP process that would include a DMZ.

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 if a layered security model is not used.

**Recommendation 16**

We recommend that the campus review its current network topology and determine how to best logically segment Internet-accessible devices from devices residing within the internal network.

**Campus Response**

We concur. The topology is being reviewed through the ITRP process for data center redesign. The campus has determined a method to segment Internet-accessible devices from those residing in the internal network using a logical DMZ that is part of the redesign.

Expected completion date: November 2009

**REVIEW OF SECURITY EVENT LOGS**

Periodic reviews of security event logs were not regularly performed and documented.

The CIO stated that security event logs were massive when produced and required a log management tool, which had been discussed but not yet purchased and implemented.

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, which could lead to confidential information being breached and not reported.

**Recommendation 17**

We recommend that the campus:

- a. Perform and document periodic reviews of security event logs to assist in identifying potential network vulnerabilities and breaches on campus systems, taking into consideration the use of tools and analytical methods, defining personnel responsibilities, reviewing frequency, and reporting/escalating processes.
- b. Consider the implementation of centralized security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

### **Campus Response**

We concur. The campus will:

- a. Perform and document periodic reviews of security event logs to assist in identifying potential network vulnerabilities and breaches on campus systems; and take into consideration the use of tools and analytical methods, defining personnel responsibilities, reviewing frequency and reporting/escalating processes.
- b. Consider the implementation of centralized security information/event monitoring tools that will centralize security monitoring and provide trend analysis, logging and automated notification.

Expected completion date: November 2009

## **PROTECTED DATA**

### **SYSTEM BACKUP ENCRYPTION**

Daily backup copies for all campus administrative systems containing protected data were not encrypted when stored off-site.

The CIO stated his belief that the off-site services provided by the outside party were sufficient.

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

### **Recommendation 18**

We recommend that the campus encrypt daily system backups containing protected data when stored at off-site locations.

### **Campus Response**

We concur. The campus now encrypts daily system backups containing protected data when stored at off-site locations.

Corrective action has been completed.

## **INCIDENT RESPONSE MANAGEMENT**

Campus procedures for handling security incidents required improvement.

Specifically, we noted that:

- ▶ Written guidelines for the handling of specific types of security incidents had not been developed.

- ▶ Types, volumes, and costs of information security incidents were not identified to assist in the monitoring of trends and risks.
- ▶ There was no formal process to periodically report the types, volumes and costs of security incidents to executive management to ensure support for enhanced control.

The CIO stated that security incidents were informally discussed in monthly staff meetings but had not been part of a formal, periodic, management process.

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

### **Recommendation 19**

We recommend that the campus:

- a. Develop written guidelines for the handling of specific types of security incidents.
- b. Develop and document procedures to identify the types, volumes, and costs of security incidents to ensure the monitoring of trends and risks on campus.
- c. Establish a documented process for the reporting of types, volumes, and costs of security incidents to executive management to ensure support for enhanced control.

### **Campus Response**

We concur. The campus will:

- a. Incorporate current practices in written guidelines for handling of specific types of security incidents.
- b. Create documentation on the use of our HEAT tracking system that tracks the type, volume, and costs of security incidents, which will assist in the monitoring of trends and risks on campus.
- c. Create a documented process in conjunction with the tracking of incidents for the reporting to executive management to ensure they are supporting the control of incidents on campus.

Expected completion date: November 2009

---

## APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Mildred Garcia	President
Mahabub Alam	Network Backbone Coordinator
Lynn Anderson	Director, Instructional Computing and Network Services
Tonya Belcher	Administrative Analyst
Ron Bergmann	Chief Information Officer
Jim Bersig	Director, Common Management Systems
Tim Farris	Director, Administrative Information Systems
Khiem Ha	Network Analyst
Edgar Lazarian	UNIX Administrator
Tina Lee	Assistant Director, Human Resources
Janie MacHarg	Director, Student Health and Psychology
Farhad Mansouri	IT Consultant
Mary Ann Rodriguez	Vice President, Administration and Finance
Mark Seigle	Assistant Vice President, Human Resources
Susan Sloan	Chief of Police
Karen Wall	Associate Vice President, Administration and Finance
Sabrina Warrington	Manager, Help Desk
Emmit Williams	Director, Procurement and Contracts



California State University  
**Dominguez Hills**

---

Office of the Vice President for Administration and Finance  
1000 E. Victoria Street – WH B470 Carson, CA 90747 (310) 243-3750 FAX (310) 234-3869

June 18, 2009

RECEIVED  
UNIVERSITY AUDITOR

JUN 22 2009

THE CALIFORNIA STATE  
UNIVERSITY

Mr. Larry Mandel  
University Auditor  
The California State University  
401 Golden Shore, 4<sup>th</sup> Floor  
Long Beach, CA 90802-4210

Dear Mr. Mandel:

Enclosed, please find California State University, Dominguez Hills' responses to the Information Security Audit 08-23, dated May 22, 2009. The campus is committed to addressing and resolving the issues identified in the audit report.

If you have any questions or would like additional information, please contact me.

Sincerely,

A handwritten signature in black ink, appearing to read 'MARodriguez'.

Mary Ann Rodriguez  
Vice President, Administration and Finance

c: Mildred García, President  
Ronald Bergmann, Associate Vice President/Chief Information Officer  
Karen Wall, Associate Vice President, Administration and Finance

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**DOMINGUEZ HILLS**

**Audit Report 08-23**

**SECURITY GOVERNANCE**

**SECURITY AUTHORITY AND RESPONSIBILITY**

**Recommendation 1**

We recommend that the campus appoint a full-time information security officer dedicated to fulfilling information security responsibilities and clearly define and document security responsibilities for this individual or other individuals assuming the roles of the information security officer function.

**Campus Response**

We concur. The campus will review workload capabilities in light of budgetary constraints and consider appointing a full-time information security officer or an individual to assume the role dedicated to fulfilling information security responsibilities, and clearly define and document security responsibilities for this individual.

Expected completion date: November 2009

**PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS**

**Recommendation 2**

We recommend that the campus:

- a. Complete a PCI DSS compliance summary plan to define its applicable vendor level and respective PCI DSS requirements.
- b. Define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

**Campus Response:**

We concur. The campus will:

- a. Complete a PCI DSS compliance summary plan to define the applicable vendor level and respective PCI DSS requirements.
- b. Define and document responsibility for assessing campus and auxiliary PCI DSS compliance.

Expected competition date: November 2009

## **INFORMATION SECURITY AWARENESS TRAINING**

### **Recommendation 3**

We recommend that the campus ensure that information security awareness training is completed by all employees with access to critical systems or protected data.

### **Campus Response**

We concur. The campus is currently monitoring the CSU developed security awareness training deployed on campus by Workplace Answers to ensure that all employees with access to critical systems or protected data are trained.

Expected completion date: November 2009

## **EMPLOYEE SEPARATION**

### **Recommendation 4**

We recommend that the campus modify its personnel exit process to include a reminder to separating employees of their ongoing legal responsibility for maintaining the security of protected data.

### **Campus Response**

We concur. The campus has completed the modification of the personnel exit process to inform separating employees of their ongoing legal responsibility for maintaining security of protected data.

Corrective action has been completed.

## **INFORMATION SECURITY PLAN**

### **Recommendation 5**

We recommend that the campus 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 timeline.

### **Campus Response**

We concur. The individual assuming the role of the information security officer will develop a documented process to identify and prioritize information security risks and create a plan to address any identified risks within an established timeframe.

Expected completion date: November 2009

## DECENTRALIZED COMPUTING

### CONFIDENTIAL INFORMATION

#### Recommendation 6

We recommend that the campus follow their documented process to identify, approve, and review access to confidential information owned and managed by its decentralized sites.

#### Campus Response

We concur. The campus will follow the documented process to identify, approve and review access to confidential information owned and managed by the ancillary sites.

Expected completion date: November 2009

### TECHNICAL VULNERABILITIES

#### Recommendation 7

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Develop and implement a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. This process would 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 or known vulnerabilities.
- c. Develop and implement a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing application.
- d. Provide all the decentralized IT units with a security baseline standard for securing servers prior to allowing them to become Internet facing.

#### Campus Response

We concur. The campus will repair the technical vulnerabilities detected by the KPMG scan.

In addition, we will:

- a. Document and implement a campus-wide patch management process.
- b. Develop and implement a security baseline standard that requires the review of applications for security vulnerabilities prior to deployment. The process will include the review of existing web application code on a periodic basis or new code prior to deployment into the production environment.

- c. Develop a campus-wide Internet-facing web application development standard to which all developers must comply prior to deploying any web application and submit the web application for official campus approval.
- d. Enforce the security baseline standard for securing servers to all ancillary sites prior to allowing them to become Internet facing.

Expected completion date: November 2009

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

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

#### **Recommendation 8**

We recommend that the campus:

- a. Require documented approval of all web application projects put into production.
- b. Establish and document testing criteria for the security of web applications, including but not limited to, input and output validation tests.
- c. Establish a documented process for user acceptance and deployment 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.
- f. Ensure that encryption is utilized for authentication to all web applications.
- g. 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. The campus will:

- a. Require documented approval of all web projects prior to deployment.
- b. Establish and document a comprehensive testing criteria plan for security of web applications.
- c. Establish and document a process for user acceptance and deployment of web applications.
- d. Restrict access to web application source code to only those employees who need it as part of their job responsibilities.
- e. Define work flow to limit developers ability to place web applications into development.

- f. Ensure that encryption is utilized for authentication to all web applications.
- g. Create a process to formally review and centrally approve all web applications prior to user acceptance through baseline security standards for web applications that are being developed by the campus.

Expected completion date: November 2009

## **WEB APPLICATION VULNERABILITIES**

### **Recommendation 9**

We recommend that the campus:

- a. Repair the web application vulnerabilities that were identified and presented in detail to the campus.
- b. Develop and implement 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 or known vulnerabilities.

### **Campus Response**

We concur. The campus will:

- a. Repair the web application vulnerabilities that were identified and detected.
- b. Develop and implement a campus-wide Internet-facing web application development standard to which all developers must comply prior to deploying any web application and submit the web application for official campus approval.

Expected completion date for: November 2009

## **SYSTEMS SECURITY AND MONITORING**

### **CONFIGURATION CHANGES**

#### **Recommendation 10**

We recommend that the campus develop and document policies and procedures for the periodic review and approval of system configuration changes that will assist management with assigning accountability and responsibility for identifying potentially misconfigured network devices.

#### **Campus Response**

We concur. The campus has purchased scanning software that will assist in the process of identifying misconfigured network devices and will update policies and procedures for the periodic review and approval of system configuration changes.

Expected completion date: November 2009

## **CONTROL OF USER ACCESS**

### **Recommendation 11**

We recommend that the campus:

- a. Establish a documented process for adding and removing user accounts to decentralized systems.
- b. Perform and document periodic management reviews of user access to all systems and applications containing protected data.

### **Campus Response**

We concur. The campus will:

- a. Create and document a process for managing user accounts for all ancillary systems.
- b. Perform and document a process that will include periodic management reviews of user access to all systems and applications containing protected data.

Expected completion date: November 2009

## **VULNERABILITY MANAGEMENT**

### **Recommendation 12**

We recommend that the campus establish a documented process to perform periodic assessments to detect vulnerabilities and exploits on all servers and desktops connected to the campus network.

### **Campus Response**

We concur. The campus will create and document processes for periodic assessments to detect vulnerabilities and exploits on all servers and desktops connected to the campus network.

Expected completion date: November 2009

## **NETWORK MONITORING**

### **Recommendation 13**

We recommend that the campus establish documented processes to:

- a. Identify and monitor all IT assets (including hardware, software, operating system versions, etc.) on the campus network.
- b. Scan web servers prior to deployment to ensure minimum system operating standards are met.

### **Campus Response**

We concur. The campus will:

- a. Identify and monitor all IT assets on the campus network and place them into appropriate firewall zones as part of the datacenter redesign project.
- b. Enforce the security baseline standard for securing web servers prior to deployment.

Expected completion date: November 2009

## **GRANTING OF ADMINISTRATIVE ACCESS**

### **Recommendation 14**

We recommend that the campus develop and document policies and procedures to address the granting and management of privileged access to accounts, taking into consideration the criteria for individuals who should have access, roles, and responsibilities for these resources; and develop a method to track, review, and periodically audit this type of access.

### **Campus Response**

We concur. The campus will develop a standard for the management of privileged access to accounts. The director in each IT department that controls administrative and service accounts will ensure that a formal process for tracking, reviewing, and auditing access to these types of accounts exists.

Expected completion date: November 2009

## **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 in detail to the campus.

In addition, we recommend that the campus:

- a. Develop and implement a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment. 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.
- b. Implement a comprehensive, campus-wide patch management process.

### **Campus Response**

We concur. The campus will repair all network device vulnerabilities as identified. Additionally the campus will:

- a. Develop and implement a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment. The process will 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.
- b. Create and implement a comprehensive campus-wide patch management process.

Expected completion date: November 2009

## **NETWORK ARCHITECTURE**

### **Recommendation 16**

We recommend that the campus review its current network topology and determine how to best logically segment Internet-accessible devices from devices residing within the internal network.

### **Campus Response**

We concur. The topology is being reviewed through the ITRP process for datacenter redesign. The campus has determined a method to segment Internet accessible devices from those residing in the internal network using a logical DMZ that is part of the redesign.

Expected completion date: November 2009

## **REVIEW OF SECURITY EVENT LOGS**

### **Recommendation 17**

We recommend that the campus:

- a. Perform and document periodic reviews of security event logs to assist in identifying potential network vulnerabilities and breaches on campus systems, taking into consideration the use of tools and analytical methods, defining personnel responsibilities, reviewing frequency, and reporting/escalating processes.
- b. Consider the implementation of centralized security information/event monitoring tools that would centralize all security monitoring and provide trend analysis, logging, and automated notification.

### **Campus Response**

We concur. The campus will:

- a. Perform and document periodic reviews of security event logs to assist in indentifying potential network vulnerabilities and breaches on campus systems; and take into consideration the use of

tools and analytical methods, defining personnel responsibilities, reviewing frequency and reporting/escalating processes.

- b. Consider the implementation of centralized security information/event monitoring tools that will centralize security monitoring and provide trend analysis, logging and automated notification.

Expected completion date: November 2009

## PROTECTED DATA

### SYSTEM BACKUP ENCRYPTION

#### Recommendation 18

We recommend that the campus encrypt daily system backups containing protected data when stored at off-site locations.

#### Campus Response

We concur. The campus now encrypts daily system backups containing protected data when stored and off-site locations.

Corrective action has been completed.

### INCIDENT RESPONSE MANAGEMENT

#### Recommendation 19

We recommend that the campus:

- a. Develop written guidelines for the handling of specific types of security incidents.
- b. Develop and document procedures to identify the types, volumes, and costs of security incidents to ensure the monitoring of trends and risks on campus.
- c. Establish a documented process for the reporting of types, volumes, and costs of security incidents to executive management to ensure support for enhanced control.

#### Campus Response

We concur. The campus will:

- a. Incorporate current practices in written guidelines for handling of specific types of security incidents.
- b. Create documentation on the use of our HEAT tracking system that tracks the type, volume and costs of security incidents, which will assist in the monitoring of trends and risks on campus.

- c. Create a documented process in conjunction with the tracking of incidents for the reporting to executive management to ensure they are supporting the control of incidents on campus.

Expected completion date: November 2009



THE CALIFORNIA STATE UNIVERSITY  
OFFICE OF THE CHANCELLOR

BAKERSFIELD

August 4, 2009

CHANNEL ISLANDS

CHICO

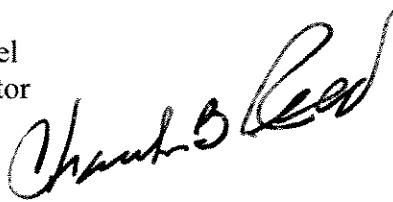
**MEMORANDUM**

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FROM: Charles B. Reed  
Chancellor


FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 08-23 on *Information Security*,  
California State University, Dominguez Hills

LONG BEACH

LOS ANGELES

In response to your memorandum of August 4, 2009, I accept the response as submitted with the draft final report on *Information Security*, California State University, Dominguez Hills.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/ms

POMONA

Enclosure

SACRAMENTO

c: Dr. Mildred Garcia, President

SAN BERNARDINO

Ms. Karen J. Wall, Associate Vice President, Administration and Finance

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS