

INFORMATION SECURITY

**CALIFORNIA STATE UNIVERSITY,
MONTEREY BAY**

**Audit Report 09-39
February 12, 2010**

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
Policy Issuance and Approval.....	8
Security Authority and Responsibility.....	9
Mobile Devices	9
Payment Card Industry Data Security Standards.....	10
Information Security Awareness Training.....	10
Record Retention	11
Employee Separation	11
System Development and Change Management	12
Web Application Development and Maintenance.....	12
Web Application Vulnerabilities	13
Systems Security and Monitoring.....	14
Technical Vulnerabilities.....	14
Configuration Changes	15
Vulnerability Management	15
Password Standards	16
Network Access	17
Granting of Administrative Access.....	17
Firewalls and Routing and Switching Devices	18
Network Architecture	19
Operating Systems Vulnerabilities	20
Review of Security Event Logs	21
Protected Data.....	22
Assessment and Inventory of Protected Information.....	22
Lost/Stolen Computers	22
Incident Response Management	23

APPENDICES

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

ABBREVIATIONS

CIO	Chief Information Officer
CSU	California State University
CSUMB	California State University, Monterey Bay
DMZ	Demilitarized Zone
EO	Executive Order
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
PCI DSS	Payment Card Industry Data Security Standards
PDA	Personal Data Assistant
RDP	Remote Desktop Protocol
SAQ	Self-Assessment Questionnaire
SNMP	Simple Network Management Protocol
SSH	Secure Shell
Telnet	Telecommunication Network

EXECUTIVE SUMMARY

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

We visited the California State University, Monterey campus from August 24, 2009, through October 16, 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 are 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 October 16, 2009, taken as a whole, were not sufficient to meet many of the objectives for a secured computing environment. While much of the campus information technology department control environment was satisfactory and provided appropriate safeguards over the critical financial and student systems, the information security office required significant improvement and management oversight.

As a result of changing conditions and the degree of compliance with procedures, the effectiveness of controls changes over time. Specific limitations that may hinder the effectiveness of an otherwise adequate system of controls include, but are not limited to, resource constraints, faulty judgments, unintentional errors, circumvention by collusion, and management overrides. Establishing controls that would prevent all these limitations would not be cost-effective; moreover, an audit may not always detect these limitations.

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

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

SECURITY GOVERNANCE [8]

The campus had not finalized and communicated information security policies. Security responsibilities were not clearly defined and documented for individuals performing the functions of the information security officer role. The campus did not have guidelines for mobile devices to access campus resources on campus. 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. All campus personnel with computer access had not completed security awareness training. The campus had not completed an assessment of its compliance with Executive Order 1031

pertaining to a record retention policy. The campus did not remind separating employees of their ongoing legal responsibility to maintain the security of protected data.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [12]

Change management procedures for in-house development of web applications required improvement. Web application vulnerabilities existed on the web application selected for testing.

SYSTEMS SECURITY AND MONITORING [14]

Technical vulnerabilities existed on a variety of campus systems. The campus lacked policies and procedures that defined a formal, periodic review of configuration changes for firewalls, switches, routers, and operating systems. The campus had no consistent process for detecting vulnerabilities related to the security of servers and desktops connected to the campus network. The campus did not have a password policy and did not adhere to password best practices. Campus administration of wireless networks required improvement. The campus lacked a formal process for granting and managing accounts with privileged system-level access. Firewalls and routing and switching devices were not always properly configured or adequately secured. The campus had not appropriately segregated the campus network. Technical vulnerabilities existed on selected operating systems. The campus lacked a formal process for the review of security event logs.

PROTECTED DATA [22]

The campus had not recently completed a university-wide assessment to identify sensitive data on all servers and workstations. The campus lacked a formal process to ensure that lost/stolen computers were consistently reported to the information security office. The campus' security incident handling procedures for compromised electronic resources required improvement.

INTRODUCTION

BACKGROUND

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

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

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

It further states that campuses must have security policies and procedures that, at a minimum, implement information security, confidentiality practices consistent with these policies, and end-user responsibilities for the physical security of the equipment and the appropriate use of hardware, software, and network facilities. The policy applies to all data systems and equipment on campus that contain data deemed private or confidential and/or which contain mission critical data, including departmental, divisional, and other ancillary systems and equipment.

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

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

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

At California State University, Monterey Bay (CSUMB), the office of information technology services has overall responsibility for the management of campus 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, Office of the Chancellor directives, and campus procedures.

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

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

- ▶ Security responsibilities are addressed prior to employment so that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work; and procedures are in place to ensure that users' separation from the organization is managed and that the return of all equipment and the removal of all access rights are completed.
- ▶ Responsibilities and procedures for the management of information processing and service delivery are defined; and technical security controls are integrated within systems and networks.
- ▶ Access rights to networks, systems, applications, business processes, and data are controlled based on business and security requirements by means of user identification and authentication.
- ▶ Formal event reporting and escalation procedures are in place for information security events and weaknesses; and communication is accomplished in a consistent and effective manner, allowing timely corrective action to be taken.
- ▶ The design, operation, use, and management of information systems are in conformance with statutory, regulatory, and contractual security requirements and are regularly reviewed for compliance.
- ▶ Web application development and change management processes and procedures are adequate to ensure that application security and accessibility is considered during the design phase, 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 retained contractors to perform a technical security assessment that included running diagnostic software designed to identify improper configuration of selected systems, servers, and network devices. The purpose of the technical security assessment was to determine the effectiveness of technology and security controls governing the confidentiality, integrity, and availability of selected campus assets. The assessment contained an internal component (within the campus network) and an external component (via the Internet) while encompassing a review of the security standards and processes that govern the CSUMB 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

POLICY ISSUANCE AND APPROVAL

The campus had not finalized and communicated information security policies.

We found that campus information security policies were not always complete, few were finalized, and many were pending formal approval by the campus' academic senate board. The lack of finalization and board action had prevented the official distribution of such policies throughout the campus and restricted compliance enforcement. The following policies/procedures were only available in draft form:

- ▶ Information Security Policy
- ▶ Wireless Communication Policy
- ▶ Extranet Policy
- ▶ Information Sensitivity Policy
- ▶ Internal Lab Security Policy
- ▶ Internet Demilitarized Zone (DMZ) Policy
- ▶ DMZ Lab Security Policy
- ▶ Risk Assessment Policy

The chief information officer (CIO) stated that the campus had not finalized the policies because the campus was waiting for the chancellor's office to issue systemwide information security policies.

Failure to finalize and communicate campus-wide policies increases the risk of unauthorized exceptions and could compromise compliance with statutory information security requirements. Such inaction also impacts the ability of the campus to evaluate the overall effectiveness of existing security provisions related to protected data.

Recommendation 1

We recommend that the campus finalize and communicate information security policies.

Campus Response

The campus concurs. The campus is drafting its Information Security and Privacy Plan and associated procedures. The campus will complete this work by June 27, 2010.

SECURITY AUTHORITY AND RESPONSIBILITY

Security responsibilities for individuals assuming the functions of the information security officer role had not been clearly defined and documented.

The provost and vice president of academic affairs stated that the campus had not had the time to formally define the security manager responsibilities.

The lack of 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 2

We recommend that the campus clearly define and document security responsibilities for individuals assuming the functions of the information security officer role.

Campus Response

The campus concurs. The campus is drafting its Information Security Roles and Responsibilities documentation with specific information security responsibilities assigned to appropriate individuals. The campus will complete this work by June 27, 2010.

MOBILE DEVICES

The campus did not have guidelines for the use of mobile technologies such as phones and Personal Data Assistants (PDAs) accessing campus resources on campus.

The CIO stated that the campus had begun discussions surrounding mobile devices but no formal guidelines had been developed or adopted.

The lack of guidelines for mobile devices increases the risk that sensitive information could be inadequately protected, and increases campus exposure to security breaches.

Recommendation 3

We recommend that the campus create a guideline addressing the use of mobile devices to access campus resources.

Campus Response

The campus concurs. The campus has drafted mobile device usage guidelines. They are under final management review. The campus will complete this work by April 27, 2010.

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 obligations.

We found that:

- ▶ The campus had not performed an annual risk assessment to determine comprehensive compliance obligations for credit card data maintained on servers and transmitted throughout the campus network, as required by PCI DSS.
- ▶ The campus had not assigned responsibility for assessing campus and auxiliary PCI DSS compliance.

The CIO stated that the campus was in the process of evaluating and remediating PCI compliance.

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 4

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

The campus concurs. The campus has completed its PCI-DSS-SAQ, determined its PCI vendor level, and has completed two quarterly external scans. Documentation for PCI compliance responsibilities has been drafted and is under final management review. The campus will complete this work by April 27, 2010.

INFORMATION SECURITY AWARENESS TRAINING

All campus personnel with computer access had not completed security awareness training.

The CIO stated that although staff personnel had completed training, collective bargaining agreements limit the campus' ability to mandate training for faculty.

Failure to provide employees with information security awareness training increases the risk that protected data could be mismanaged, which, in turn, increases the campus' exposure to security breaches and could compromise its compliance with statutory information security requirements.

Recommendation 5

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

Campus Response

The campus concurs. The campus has adopted the Workplace Answers SAT via the chancellor's office. The campus will complete program development by April 27, 2010.

RECORD RETENTION

The campus had not completed an assessment of its compliance with Executive Order (EO) 1031 pertaining to a record retention policy.

The CIO stated that campus division heads had reviewed the EO and each division was responsible for compliance with the EO but that the campus had not conducted a formal campus-wide assessment.

Failure to complete a record retention plan increases the risk of inappropriate and untimely disposal of records and information.

Recommendation 6

We recommend that the campus complete a record retention action plan and corresponding procedures that ensure its appropriate and timely disposal of records and information.

Campus Response

The campus concurs. The CIO (in coordination with senior leadership) is reviewing EO 1031 and is developing guidelines and procedures for the campus. The campus will complete this work by April 27, 2010.

EMPLOYEE SEPARATION

The campus did not remind separating employees of their ongoing legal responsibility to maintain the security of protected data.

The director of human resources operations stated that the campus had not considered including this practice in its termination process.

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

Recommendation 7

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

Campus Response

Subsequent to this finding, the Office of University Auditor has advised the campus of changes in underlying considerations that lead to the recommendation above. The campus will review its current procedures and advise if any changes are warranted. The campus will complete this work by June 27, 2010.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

WEB APPLICATION DEVELOPMENT AND MAINTENANCE

Change management procedures for in-house development of web applications required improvement.

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

- ▶ The campus did not require written approval to move projects into production.
- ▶ The campus had not defined web applications security testing criteria.
- ▶ The campus did not document user acceptance testing.
- ▶ Developers were able to move applications into production without management approval.

The CIO stated that the web services lead, working together with the department manager, provides a sufficient organizational structure to oversee the web services unit. He further stated that documenting project approval would introduce unnecessary delays in the web development cycle and that the campus believed that the current level of management oversight of web development was sufficient.

The lack of formal change management procedures increases the risk that in-house developed 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 prior to placement into production.
- b. Establish and document testing criteria for web applications, including but not limited to, input and output validation tests, and tests of vulnerabilities that are commonly exploited.
- c. Establish a documented process for user acceptance testing of web applications.
- d. Limit developers' ability to move web applications into production, or create procedures so that management monitors changes to production.

Campus Response

The campus concurs. The campus is implementing version control (Subversion), application testing systems (Selenium), and vulnerability scanning (NeXpose) that will address each of the items in this recommendation. The campus will complete this work by June 27, 2010.

WEB APPLICATION VULNERABILITIES

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

The web application reviewed enabled an AUTOCOMPLETE function that allowed passwords to be stored in browsers and retrieved.

The CIO stated that programming oversight caused these vulnerabilities.

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

Recommendation 9

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

In addition, we recommend that the campus:

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

deployment into the production environment to minimize the potential deployment of code susceptible to known vulnerabilities.

Campus Response

The campus concurs. All identified issues have been resolved. The campus is implementing version control, application testing, and vulnerability scanning systems (see recommendation 8) that will address this recommendation. The campus will complete this work by June 27, 2010.

SYSTEMS SECURITY AND MONITORING

TECHNICAL VULNERABILITIES

Technical vulnerabilities existed on a variety of campus systems.

Our external testing disclosed 31 vulnerabilities on a variety of servers. We provided specific details of these vulnerabilities to the campus.

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

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

Recommendation 10

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Formalize a security baseline standard that requires servers be reviewed for security vulnerabilities prior to deployment.

Campus Response

The campus concurs. All identified issues have been resolved. Patch management procedures and baseline server standards have been documented and are under final management review. The campus will complete this work by April 27, 2010.

CONFIGURATION CHANGES

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

We found that periodic reviews of these systems and devices were occurring informally as part of the 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 due to the low attrition rate of employees, he had not considered it necessary to formalize policies and procedures to review configuration changes.

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

Recommendation 11

We recommend that the campus:

- a. Develop policies and procedures that establish a formal review of system configurations to help management determine accountability for potentially incorrectly configured network devices and assign responsibility for identifying and remediating configuration problems.
- b. Incorporate into these change management policies and procedures a formal process for appropriate campus personnel sign-off to ensure compliance of configuration reviews.

Campus Response

The campus concurs. Configuration management procedures and baseline configuration standards for firewalls, routers, and switches have been documented and are under final management review. Change management procedures have been documented and are under final management review. The campus will complete this work by April 27, 2010.

VULNERABILITY MANAGEMENT

The campus had no consistent process for monitoring, detecting, and remediating security vulnerabilities on servers connected to the campus network.

The CIO stated that resource constraints prevented full implementation of a vulnerability management program.

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

Recommendation 12

We recommend that the campus develop a consistent process to detect vulnerabilities on all servers and desktops connected to the campus network.

Campus Response

The campus concurs. The campus acquired and is finalizing implementation of vulnerability scanning software. The campus has documented vulnerability scanning procedures, and they are under final review by management. The campus will complete this work by June 27, 2010.

PASSWORD STANDARDS

The campus did not have a password policy and did not adhere to password best practices.

We noted that:

- ▶ The campus did not have a password policy that it extended to, and enforced for, some departments and/or applications on campus.
- ▶ The minimum interval before a password can be changed was set to zero, allowing individuals to immediately reset their passwords and circumvent reuse.
- ▶ Administrative level passwords for certain devices had not been changed from default, and passwords had not been set to expire periodically.

The CIO stated that password policies were enforced through the campus Active Directory system. However, there were some stand-alone systems that had not yet been subjected to these password policies.

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

Recommendation 13

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

Campus Response

The campus concurs. The campus has documented its password policy, and it is under final management review. The campus will complete this work by April 27, 2010.

NETWORK ACCESS

Campus administration of wireless networks required improvement.

Specifically, we noted that:

- ▶ The wireless network had not been segregated from the internal campus network.
- ▶ Encryption had not been used to secure wireless traffic.
- ▶ The wireless network allowed anonymous user access without limiting the session duration.

The CIO stated that the tools to implement wireless encryption and session duration were available but some university-owned assets were not capable of supporting encrypted wireless, which prevented full implementation.

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

Recommendation 14

We recommend that the campus:

- a. Segregate the wireless network from the internal campus network.
- b. Use encryption to secure wireless traffic that connects to the internal campus network.
- c. Limit wireless session duration to limit the risk of misuse of campus resources.

Campus Response

The campus concurs. The campus acquired, installed, and is finalizing migration to a new network topology and wireless access control incorporating all elements of this recommendation. The campus will complete this work by April 27, 2010.

GRANTING OF ADMINISTRATIVE ACCESS

The campus lacked a formal process for granting and managing accounts with privileged system-level access.

The CIO stated his belief that the system did not require a more formal process because few people had system-level access privileges.

The lack of a formal process for granting and managing privileged access could lead to inadequate segregation of duties, the granting of accounts not based on the principle of least privilege, and/or unauthorized access.

Recommendation 15

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

Campus Response

The campus concurs. The campus has documented its privileged account access process, and it is under final management review. The campus will complete this work by April 27, 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 selected routing and switching devices disclosed that:

- ▶ Two devices were configured with no control to restrict access to administrative accounts.
- ▶ Four devices were configured with Simple Network Management Protocol (SNMP), which transmits in clear text and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ One device was enabled with Telecommunication Network (Telnet), which transfers user logins, passwords, and commands across the network in clear text. Telnet could allow a remote attacker to obtain confidential authentication credentials enabling remote access to the devices.
- ▶ One device had an older version of the Secure Shell (SSH) protocol enabled, which an attacker could exploit to execute system commands.
- ▶ One device had not been configured in accordance with firewall best practices. For example, we noted that the firewall was not configured to deny all traffic and only allow exceptions.

The CIO stated that these vulnerabilities were due to staff oversight or the lack of resources to implement the required technology. He also stated that the firewall rule sets had been part of the legacy implementation which had not been reviewed and updated and would be replaced with new firewall architecture.

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 disable other network resources.

Recommendation 16

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

In addition, we recommend that the campus:

- a. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the periodic review of existing device configurations to identify potential vulnerabilities.
- c. Review current firewall architecture to ensure configurations adhere to best practices by denying all traffic and only allow on an exception basis.

Campus Response

The campus concurs. All identified vulnerabilities have been resolved. The campus has documented baseline security configurations (firewalls, routers, and switches), patch management, and configuration review procedures, and they are under final management review. The campus has reviewed current firewall configurations and is implementing new standard configurations across the campus network. The campus will complete this work by June 27, 2010.

NETWORK ARCHITECTURE

The campus had not appropriately segregated the campus network.

Specifically, we noted that a DMZ was available but no servers had been placed within this network segment.

The CIO stated that the campus had been in the process of rebuilding the campus' network topology and had received final approval from the chancellor's office and equipment had been ordered to implement the new plan.

Inadequate separation of publicly accessible servers from internal network resources increases the risk that compromised devices could be used to attack other network servers.

Recommendation 17

We recommend that the campus appropriately segregate its network by placing Internet servers in the DMZ.

Campus Response

The campus concurs. The campus acquired, installed, and is finalizing migration to a new network topology incorporating this recommendation. The campus will complete this work by April 27, 2010.

OPERATING SYSTEMS VULNERABILITIES

Technical vulnerabilities existed on selected operating systems.

Our testing of three servers disclosed various vulnerabilities, and we provided details of these vulnerabilities to the campus:

- ▶ One server was running an old version of the operating system with multiple security vulnerabilities.
- ▶ One server had an excessive maximum password age, and one did not have a password set to a powerful system utility.
- ▶ One had a number of files that allowed anybody to modify them.
- ▶ One server was missing security updates.
- ▶ Two servers had user accounts with non-expiring passwords.
- ▶ One server did not enable auditing of login failures.
- ▶ Two servers were running a vulnerable version of remote desk protocol (RDP).
- ▶ Two servers were running a vulnerable web-based management interface.
- ▶ Two servers enabled the TRACE and TRACK methods.

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

The extent of vulnerabilities on these critical servers demonstrates a lack of attention and oversight to sever security and management, and increases the risk of a remote attack that could result in a loss of protected confidential information and the execution of malicious programs on the server that could disable additional network resources.

Recommendation 18

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

In addition, we recommend that the campus:

- a. Immediately perform an assessment of all critical campus servers to ensure that all servers are appropriately secured.
- b. Formalize a security baseline standard that requires applications be reviewed for security vulnerabilities prior to deployment.

- c. Implement a comprehensive, campus-wide patch management process. This process would include the periodic review of existing code to identify potential or known vulnerabilities.

Campus Response

The campus concurs. All identified vulnerabilities have been resolved. The campus has documented vulnerability scanning procedures, server security baselines, and patch management procedures, and they are under final management review. The campus will complete this work by June 27, 2010.

REVIEW OF SECURITY EVENT LOGS

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

The CIO stated that network activity was monitored continuously and that logs were reviewed informally as needed.

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

Recommendation 19

We recommend that the campus:

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

Campus Response

The campus concurs. The campus is developing event log management and review procedures and is evaluating additional tools for implementation. The campus will complete this work by June 27, 2010.

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

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

The CIO stated that an assessment had not been performed because of competing information technology priorities.

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

Recommendation 20

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

Campus Response

The campus concurs. The campus is evaluating assessment procedures to identify sensitive data stored on campus assets. Process implementation planning is under management review. The campus will complete this work by June 27, 2010.

LOST/STOLEN COMPUTERS

The campus lacked a formal process to ensure that lost/stolen computers were consistently reported to the information security office. Accordingly, the campus could not determine whether these computers contained any sensitive information or whether public disclosure was required.

The CIO stated that the campus had an informal process and the campus is now formalizing its procedures to ensure that all lost/stolen computers are reported to the information security office.

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

Recommendation 21

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

Campus Response

The campus concurs. The campus has documented procedures for information security office notification of lost/stolen assets. This procedure is under final management review. The campus will complete this work by April 27, 2010.

INCIDENT RESPONSE MANAGEMENT

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

We noted that:

- ▶ The campus had no formal security incident response policy.
- ▶ The campus had no formal process to monitor types, frequency, and costs of information security incidents.
- ▶ Security incidents were not formally reported to executive management.

The CIO stated that the campus had an informal process for non-noticeable events and it had not considered the necessity to formalize the process due to the low number of incidents on campus. He further stated that although the campus directives require periodic reporting, this process had not been documented.

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

Recommendation 22

We recommend that the campus:

- a. Establish a formal security incident response policy.
- b. Develop and document procedures to identify the types, volume, and costs of security incidents to ensure that the campus monitors trends and risks.
- c. Establish a documented process for reporting security incidents to executive management.

Campus Response

The campus concurs. The campus is developing its CSIRT policy and executive management notification procedures. The campus will complete this work by June 27, 2010.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Dianne F. Harrison	President
Kathryn Cruz-Uribe	Provost and Vice President for Academic Affairs
Isaac Davis-King	Web Programming Specialist
John Fitzgibbon	Associate Vice President for Finance
Gretchen Fuentes	Director, Human Resources Operations
Monica Galligan	Human Resources Systems Manager
George Lenno	Chief Information Officer
James E. Main	Vice President for Administration and Finance
Steven Mann	Senior Operations Analyst
Mary Mauro	Manager, Campus Data Warehouse
Susan McFarlane	Director, Administrative Systems Management
Kevin Miller	Web Programming Specialist
Brian Peralsky	Network Engineering Analyst
Greg Pool	Web Publishing Coordinator
Brian Shaw	Software and Desktop Management Coordinator
Eric Simoni	Associate Director, Information Systems
Henry Simpson	Director, Technology Support Services
Chris Taylor	Director of Network Services



CALIFORNIA STATE UNIVERSITY
Monterey Bay

OFFICE OF THE VICE PRESIDENT
FOR ADMINISTRATION AND FINANCE

100 CAMPUS CENTER, BUILDING 84D
SEASIDE, CA 93955-8001
831-582-3398
FAX 831-582-3339
WWW.CSUMB.EDU

March 19, 2010

RECEIVED
UNIVERSITY AUDITOR

MAR 19 2010

THE CALIFORNIA STATE
UNIVERSITY

Mr. Larry Mandel
University Auditor
Office of the University Auditor
California State University
401 Golden Shore, 4th Floor
Long Beach, CA 90802

Subject: Information Security Audit #09-39

Dear Larry:

Attached is the hard copy of CSU Monterey Bay's responses to the recommendations regarding the subject audit. Electronic copy has been transmitted to your attention.

Please contact AVP John Fitzgibbon if you have any questions or comments.

Sincerely,

James E. Main
VP for Administration and Finance

Attachment

cc: Senior Director Schlack
Provost Cruz-Uribe
CIO Chip Lenno
Associate VP Fitzgibbon

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
MONTEREY BAY

Audit Report 09-39

SECURITY GOVERNANCE

POLICY ISSUANCE AND APPROVAL

Recommendation 1

We recommend that the campus finalize and communicate information security policies.

Campus Response

The campus concurs. The campus is drafting its Information Security and Privacy Plan and associated procedures. The campus will complete this work by June 27th, 2010.

SECURITY AUTHORITY AND RESPONSIBILITY

Recommendation 2

We recommend that the campus clearly define and document security responsibilities for individuals assuming the functions of the information security officer role.

Campus Response

The campus concurs. The campus is drafting its Information Security Roles and Responsibilities documentation with specific Information Security responsibilities assigned to appropriate individuals. The campus will complete this work by June 27th, 2010.

MOBILE DEVICES

Recommendation 3

We recommend that the campus create a guideline addressing the use of mobile devices to access campus resources.

Campus Response

The campus concurs. The campus has drafted mobile device usage guidelines. They are under final management review. The campus will complete this work by April 27th, 2010.

PAYMENT CARD INDUSTRY DATA SECURITY STANDARDS

Recommendation 4

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

The campus concurs. The campus has completed its PCI-DSS-SAQ, determined its PCI vendor level, and has completed two quarterly external scans. Documentation for PCI compliance responsibilities has been drafted and is under final management review. The campus will complete this work by April 27th, 2010.

INFORMATION SECURITY AWARENESS TRAINING

Recommendation 5

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

Campus Response

The campus concurs. The campus has adopted the Workplace Answers SAT via the Chancellors Office. The campus will complete program development by April 27th, 2010.

RECORD RETENTION

Recommendation 6

We recommend that the campus complete a record retention action plan and corresponding procedures that ensure its appropriate and timely disposal of records and information.

Campus Response

The campus concurs. The CIO (in coordination with Senior Leadership) is reviewing EO 1031 and is developing guidelines and procedures for the campus. The campus will complete this work by April 27th, 2010.

EMPLOYEE SEPARATION

Recommendation 7

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

Campus Response

Subsequent to this finding, the Office of University Auditor has advised the campus of changes in underlying considerations that lead to the recommendation above. The campus will review its current procedures and advise if any changes are warranted.

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 prior to placement into production.
- b. Establish and document testing criteria for web applications, including but not limited to, input and output validation tests, and tests of vulnerabilities that are commonly exploited.
- c. Establish a documented process for user acceptance testing of web applications.
- d. Limit developers' ability to move web applications into production, or create procedures so that management monitors changes to production.

Campus Response

The campus concurs. The campus is implementing version control (Subversion), application testing systems (Selenium), and vulnerability scanning (NeXpose) that will address each of the items in this recommendation. The campus will complete this work by June 27th, 2010.

WEB APPLICATION VULNERABILITIES

Recommendation 9

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

In addition, we recommend that the campus:

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

Campus Response

The campus concurs. All identified issues have been resolved. The campus is implementing version control, application testing, and vulnerability scanning systems (see recommendation 8) that will address this recommendation. The campus will complete this work by June 27th, 2010.

SYSTEMS SECURITY AND MONITORING

TECHNICAL VULNERABILITIES

Recommendation 10

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

In addition, we recommend that the campus:

- a. Implement a comprehensive, campus-wide patch management process.
- b. Formalize a security baseline standard that requires servers be reviewed for security vulnerabilities prior to deployment.

Campus Response

The campus concurs. All identified issues have been resolved. Patch management procedures and baseline server standards have been documented and are under final management review. The campus will complete this work by April 27th, 2010.

CONFIGURATION CHANGES

Recommendation 11

We recommend that the campus:

- a. Develop policies and procedures that establish a formal review of system configurations to help management determine accountability for potentially incorrectly configured network devices and assign responsibility for identifying and remediating configuration problems.
- b. Incorporate into these change management policies and procedures a formal process for appropriate campus personnel sign-off to ensure compliance of configuration reviews.

Campus Response

The campus concurs. Configuration management procedures and baseline configuration standards for firewalls, routers, and switches have been documented and are under final management review. Change management procedures have been documented and are under final management review. The campus will complete this work by April 27th, 2010.

VULNERABILITY MANAGEMENT

Recommendation 12

We recommend that the campus develop a consistent process to detect vulnerabilities on all servers and desktops connected to the campus network.

Campus Response

The campus concurs. The campus acquired and is finalizing implementation of vulnerability scanning software. The campus has documented vulnerability scanning procedures and they are under final review by management. The campus will complete this work by June 27th, 2010.

PASSWORD STANDARDS

Recommendation 13

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

Campus Response

The campus concurs. The campus has documented its password policy and it is under final management review. The campus will complete this work by April 27th, 2010.

NETWORK ACCESS

Recommendation 14

We recommend that the campus:

- a. Segregate the wireless network from the internal campus network.
- b. Use encryption to secure wireless traffic that connects to the internal campus network.
- c. Limit wireless session duration to limit the risk of misuse of campus resources.

Campus Response

The campus concurs. The campus acquired, installed and is finalizing migration to a new network topology and wireless access control incorporating all elements of this recommendation. The campus will complete this work by April 27th, 2010.

GRANTING OF ADMINISTRATIVE ACCESS

Recommendation 15

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

Campus Response

The campus concurs. The campus has documented its privileged account access process and it is under final management review. The campus will complete this work by April 27th, 2010.

FIREWALLS AND ROUTING AND SWITCHING DEVICES

Recommendation 16

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

In addition, we recommend that the campus:

- a. Formalize a security baseline standard that requires the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the periodic review of existing device configurations to identify potential vulnerabilities.
- c. Review current firewall architecture to ensure configurations adhere to best practices by denying all traffic and only allow on an exception basis.

Campus Response

The campus concurs. All identified vulnerabilities have been resolved. The campus has documented baseline security configurations (firewalls, routers, and switches), patch management, and configuration review procedures and they are under final management review. The campus has reviewed current firewall configurations and is implementing new standard configurations across the campus network. The campus will complete this work by June 27th, 2010.

NETWORK ARCHITECTURE**Recommendation 17**

We recommend that the campus appropriately segregate its network by placing Internet servers in the DMZ.

Campus Response

The campus concurs. The campus acquired, installed and is finalizing migration to a new network topology incorporating this recommendation. The campus will complete this work by April 27th, 2010.

OPERATING SYSTEMS VULNERABILITIES**Recommendation 18**

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

In addition, we recommend that the campus:

- a. Immediately perform an assessment of all critical campus servers to ensure that all servers are appropriately secured.
- b. Formalize a security baseline standard that requires applications be reviewed for security vulnerabilities prior to deployment.
- c. Implement a comprehensive, campus-wide patch management process. This process would include the periodic review of existing code to identify potential or known vulnerabilities.

Campus Response

The campus concurs. All identified vulnerabilities have been resolved. The campus has documented vulnerability scanning procedures, server security baselines, and patch management procedures and they are under final management review. The campus will complete this work by June 27th, 2010.

REVIEW OF SECURITY EVENT LOGS

Recommendation 19

We recommend that the campus:

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

Campus Response

The campus concurs. The campus is developing event log management and review procedures and is evaluating additional tools for implementation. The campus will complete this work by June 27th, 2010.

PROTECTED DATA

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

Recommendation 20

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

Campus Response

The campus concurs. The campus is evaluating assessment procedures to identify sensitive data stored on campus assets. Process implementation planning is under management review. The campus will complete this work by June 27th, 2010.

LOST/STOLEN COMPUTERS

Recommendation 21

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

Campus Response

The campus concurs. The campus has documented procedures for ISO notification of lost/stolen assets. This procedure is under final management review. The campus will complete this work by April 27th, 2010.

INCIDENT RESPONSE MANAGEMENT

Recommendation 22

We recommend that the campus:

- a. Establish a formal security incident response policy.
- b. Develop and document procedures to identify the types, volume, and costs of security incidents to ensure that the campus monitors trends and risks.
- c. Establish a documented process for reporting security incidents to executive management.

Campus Response

The campus concurs. The campus is developing its CSIRT policy and executive management notification procedures. The campus will complete this work by June 27th, 2010.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR

BAKERSFIELD

April 30, 2010

CHANNEL ISLANDS

CHICO

MEMORANDUM

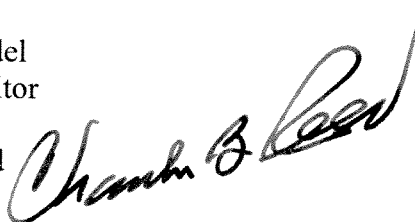
DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed
Chancellor



FULLERTON

SUBJECT: Draft Final Report 09-39 on *Information Security*,
California State University, Monterey Bay

HUMBOLDT

LONG BEACH

LOS ANGELES

In response to your memorandum of April 30, 2010, I accept the response as submitted with the draft final report on *Information Security*, California State University, Monterey Bay.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS