

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**LONG BEACH**

**Audit Report 09-35**  
**November 9, 2009**

---

**Members, Committee on Audit**

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

---

**Staff**

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

---

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

---

# CONTENTS

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

---

## OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance.....	8
Security Organization .....	8
Information Security Policy .....	9
Remote Computing .....	9
Employee-Owned Computers .....	10
Information Security Awareness Training.....	10
Employee Separation .....	11
Background Checks .....	11
Information Security Plan.....	12
Record Retention .....	12
Decentralized Computing .....	13
Non-ITS Computing Environments .....	13
Technical Vulnerabilities.....	15
System Development and Change Management .....	16
Systems Security and Monitoring.....	16
Vulnerability Management .....	16
Network Monitoring .....	17
Granting of Administrative Access.....	18
Firewalls and Routing and Switching Devices .....	18
Network Architecture .....	19
Review of Security Event Logs .....	20
Protected Data.....	21
Assessment and Inventory of Protected Information.....	21
Lost/Stolen Computers .....	22
Disposition of Protected Data.....	22

## **APPENDICES**

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

---

## **ABBREVIATIONS**

CSU	California State University
CSULB	California State University, Long Beach
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITS	Information Technology Services
SNMP	Simple Network Management Protocol
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, Long Beach campus from March 16, 2009, through April 24, 2009, and audited the procedures in effect at that time.

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

In our opinion, the operational and administrative controls of information security in effect as of April 24, 2009, taken as a whole, were not sufficient to meet many of the objectives for a secured computing environment. While much of the campus IT department control environment was satisfactory and provided appropriate safeguards over the critical financial and student systems, the decentralized computing environments that were not under the purview of campus IT require significant improvement and management oversight.

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

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

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

### **SECURITY GOVERNANCE [8]**

The campus had not defined the position and authority of the divisional information security officers and lacked a process to monitor and enforce campus-wide policies and procedures. The campus' information security policy had not been updated to address current business practices. The campus lacked a policy to address the authorization, management, and monitoring of mobile computing and the associated remote access to campus resources.

The campus lacked a policy to address the use of employee-owned computers with access to campus resources. Security awareness training had not been completed by all campus personnel with computer access. The campus did not perform criminal background checks of information technology professionals with access to campus systems nor remind separating employees of their ongoing legal responsibility for maintaining the security of protected data. The campus had not developed a formal action plan to identify and prioritize information security risks and had not established a timeline for addressing these risks. The campus record retention action plan required improvement.

### **DECENTRALIZED COMPUTING [13]**

Administration of non-information technology services (ITS) college technology environments required improvement. Technical vulnerabilities existed on a variety of systems throughout the campus.

### **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [16]**

The campus lacked written procedures to test for vulnerabilities in web applications prior to their deployment into the production environment, and professional application development standards and methodologies were absent or inadequate.

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

The campus' process for detecting vulnerabilities related to the security of servers and desktops connected to the campus network required improvement. The campus lacked a formal process to identify and monitor all IT resources on the campus network, which included servers, workstations, and laptops that were owned and managed by non-ITS college technology environments or the other colleges and divisions. The campus lacked a formal process for the granting and management of privileged system-level access to accounts on all servers. Firewalls and routing and switching devices were not always properly configured or adequately secured. Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources. The campus lacked a formal process for the review of security event logs.

### **PROTECTED DATA [21]**

The campus had not completed a campus-wide assessment to identify sensitive data on all on servers, workstations, and laptops, and it did not have a formal process to identify, approve, or review access to confidential information owned and managed by campus decentralized sites. Lost or stolen equipment that might contain protected data was not consistently reported to the information security office. Procedures to ensure that all sensitive information on computers is properly deleted prior to disposition 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 man-made 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; information technology (IT) security; configuration management and change control; access control; asset management; management of information systems; information security incident management; physical security; business continuity and disaster recovery; and legal and regulatory compliance. The Information Technology Advisory Committee, composed of the chief information officers from each campus, and the Information Security Advisory Committee, composed of the information security officers from each campus, was integrally involved in this policy development process in order to ensure that the final product was an appropriate fit for the CSU. This project began in September 2007 with the expectation that these policies and standards were to be completed by August 2008 for subsequent adoption and official systemwide distribution in late 2008. This timeline has now been extended an additional six months. Due to the pending status of this project during the time frame of the information security audits, these policies and standards were not used for evaluation of the campuses information security posture.

At California State University, Long Beach (CSULB), the office of information technology services has overall responsibility for the management of campus networks, telecommunications and administrative systems, and some campus systems. 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 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 the production servers are adequately protected.
- ▶ E-mail systems are properly configured and managed so that vulnerabilities are not allowed into the network, incidents are properly escalated, campus usage and retention guidelines are followed, and e-mail addresses are maintained in a central location to facilitate campus-wide communications.
- ▶ The operational security of selected operating systems is adequate to prevent the exploitation of vulnerabilities on the internal network by individuals who gain access to it from dial-in connections, the Internet, and hosts on the internal network.
- ▶ The Internet firewall system is sufficient to identify and thwart attacks from the external Internet and filter unwanted network traffic.
- ▶ Selected routing and switching devices are properly managed and configured to effectively provide the designated network security or traffic controls.
- ▶ Systems connected to the Internet make publicly available any information that may provide enticement to penetrate the Internet gateway.
- ▶ Web application vulnerabilities that provide the potential for an unauthorized party to subvert controls and gain access to critical and proprietary information, use resources inappropriately, interrupt business, or commit fraud are identified and addressed.

## **SCOPE AND METHODOLOGY**

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

In addition to the interviews and inquiry procedures affecting the operation and support of the network devices reviewed by the Office of the University Auditor, we also contracted with 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 CSULB 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 were designed to provide a managerial level review of key information security practices, which included detailed testing of a limited number of network and computing devices. Our review did not examine all aspects of information security, selected emerging technologies were excluded from the scope of the review, and our testing approach was designed to provide a view of the security technologies used to protect only key computing resources.

---

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

## **SECURITY GOVERNANCE**

### **SECURITY ORGANIZATION**

The campus had not defined the position and authority of the divisional information security officers and lacked a process to monitor and enforce campus-wide policies and procedures.

We noted that:

- ▶ The campus had not formally defined and communicated divisional information security officers' roles, responsibilities, and authority.
- ▶ The campus lacked a process to track and report on the various divisions' ongoing compliance with campus information security policies and procedures. We noted that the information security office issued security policies and procedures, but relevant users either did not consistently follow these practices, did not know of these practices, or believed that these practices were not applicable to their areas.

The information security officer stated that the organizational structure of the campus environment did not allow for the direct oversight necessary to ensure that information security best practices were followed.

Failure to define the information security function and the lack of a process to monitor and enforce campus-wide policies and procedures limits the campus' ability to direct a comprehensive information security program. Such limitations increase the campus' exposure to security breaches and the risk of inappropriate use.

### **Recommendation 1**

We recommend that the campus:

- a. Formally define and communicate divisional information security officers' roles, responsibilities, and authority.
- b. Develop a process to track and report on the various divisions' ongoing compliance with campus information security policies and procedures.

### **Campus Response**

We concur. The campus will:

- a. Formally define and communicate divisional information security officers' roles, responsibilities, and authority by formal delegation of authority letters.

- b. Develop a process to monitor divisions' ongoing compliance with campus information security policies and procedures.

Estimated date of completion is May 31, 2010.

## **INFORMATION SECURITY POLICY**

The campus' information security policy had not been updated to address current business practices.

Specifically, we noted that the Campus Information Technology Committee had been disbanded, and the campus had not enforced periodic reporting of information security compliance as stated in the information security policy.

The information security officer stated that updating the information security policy had not been a priority in comparison to other campus-wide issues.

Failure to properly update information security policies limits the effectiveness of information security governance and increases the risk of misunderstandings regarding user responsibilities.

### **Recommendation 2**

We recommend that the campus update its information security policy to reflect current business practices.

### **Campus Response**

We concur. We updated the campus' information security policy to reflect current business practices. Corrective action on this issue is complete.

## **REMOTE COMPUTING**

The campus lacked a policy to address the authorization, management, and monitoring of mobile computing and the associated remote access to campus resources.

The associate vice president of information technology services (ITS) stated that although this issue had been discussed, a formal policy or standard had not been developed.

The lack of policy for remote users 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 policy addressing the authorization, management, and monitoring of mobile computing and the associated remote access to campus resources.

**Campus Response**

We concur. A draft policy has been developed and is in the process of review and approval. Estimated date of completion is May 31, 2010.

**EMPLOYEE-OWNED COMPUTERS**

The campus lacked a policy to address the use of employee-owned computers with access to campus resources.

The associate vice president of ITS stated that although this issue had been discussed, a formal policy had not been developed.

The lack of a policy for the use of employee-owned computers with access to campus resources increases the risk that computers may not be implemented with appropriate security.

**Recommendation 4**

We recommend that the campus develop a policy to address the use of employee-owned computers with access to campus resources.

**Campus Response**

We concur. A draft policy has been developed and is in the process of campus review and approval. Estimated date of completion is May 31, 2010.

**INFORMATION SECURITY AWARENESS TRAINING**

Security awareness training had not been completed by all campus personnel with computer access.

The information security officer stated that the campus' ability to mandate training for its faculty was limited by its collective bargaining agreement.

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 the campus' compliance with statutory information security requirements.

**Recommendation 5**

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

### **Campus Response**

We concur. The information security awareness training will now be offered to California State University, Long Beach faculty. Estimated date of completion is May 31, 2010.

### **EMPLOYEE SEPARATION**

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

The director of staff human resources stated that he had not considered including this practice as part of the 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 6**

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**

We concur. The campus modified its personnel exit process form to include a reminder of ongoing legal responsibility to maintain the security of protected data. Corrective action on this issue is complete.

### **BACKGROUND CHECKS**

The campus had not performed criminal background checks of information technology professionals with access to privileged campus systems.

The director of staff human resources stated that background checks for information technology professionals had not been considered in its background check policy.

Failure to perform criminal background checks increases the risk of employee malfeasance.

### **Recommendation 7**

We recommend that the campus revise procedures to implement background checks for information technology professionals with access to privileged campus systems.

### **Campus Response**

We concur. The campus will revise its procedures to implement background checks for information technology professionals with privileged access to campus systems. Corrective action on this issue is complete.

### **INFORMATION SECURITY PLAN**

The campus had not developed a formal action plan to identify and prioritize information security risks and had not established a timeline for addressing these risks.

The information security officer indicated that the campus did not have a chance to address this requirement.

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

### **Recommendation 8**

We recommend that the campus create a formal action plan to identify and prioritize information security risks and establish a specified timeline to address identified risks.

### **Campus Response**

We concur. The campus will create a formal action plan. Estimated date of completion is May 31, 2010.

### **RECORD RETENTION**

The campus record retention action plan required improvement.

Specifically, we noted that the campus did not have written documentation formally designating its custodians of records.

Executive Order 1031, *Systemwide Records/Information Retention and Disposition Schedules Implementation*, dated February 27, 2008, states that each campus must establish and publish procedures for the modification of retention and disposition schedules as needed to incorporate records unique to each campus; and that it must annually review its records/information as listed on the schedules to determine if they should be destroyed or maintained.

The information security officer stated that although the campus had identified custodians of records for certain areas, it was still in the process of identifying the custodians for others.

Failure to formally designate custodians of records increases the risk of inappropriate and untimely disposal of records/information.

**Recommendation 9**

We recommend that the campus revise its record retention action plan to formally designate its custodians of records.

**Campus Response**

We concur. The campus will revise its record retention action plan to formally designate its custodians of records. Estimated date of completion is May 31, 2010.

**DECENTRALIZED COMPUTING**

**NON-ITS COMPUTING ENVIRONMENTS**

Administration of non-ITS college technology environments required improvement.

On a sample basis, we reviewed some non-ITS supported computing operations on campus. Our review of four colleges disclosed that:

- ▶ Colleges had not completed an evaluation to determine which users should have administrative access to their computers.
- ▶ Encryption had not been used for the storage of Level 1 data on desktops and laptops.
- ▶ Backups were stored in local servers rather than being sent off-site.
- ▶ Passwords did not meet minimum campus standards.
- ▶ Backup personnel had not been designated for a departmental system administrator with privileged access to department systems.
- ▶ Designated college information technology professionals did not have adequate authority and oversight over all information security best practices within the college environment.

The associate vice president of academic technology stated that the decentralized nature of the campus resulted in these deficiencies.

Failure to properly administer decentralized servers increases the risk that servers may be compromised, resulting in loss of confidential data in the event of a security breach.

### **Recommendation 10**

We recommend that the campus:

- a. Eliminate administrative access to computers unless specifically approved.
- b. Encrypt desktops and/or laptops that store Level 1 data on desktops and laptops.
- c. Ensure that backups are stored off-site.
- d. Ensure all passwords meet minimum campus standards.
- e. Ensure that departmental system administrators have a designated backup.
- f. Ensure that college information technology professionals have appropriate authority and oversight to implement information security best practices within the college environments as defined by university policies and procedures.

### **Campus Response**

We concur. The campus will:

- a. Eliminate administrative access to computers and create an approval process for exceptions. Exceptions required to carry out business or academic efforts will be documented, tracked, and managed in a standard manner.
- b. Encrypt desktops/laptops storing Level 1 data.
- c. Ensure that backups are stored off-site.
- d. Ensure all passwords meet minimum campus standards.
- e. Ensure that departmental system administrators have designated backups.
- f. Ensure that the college information technology professionals follow established university policies and procedures to implement information security best practices within the college environments and with appropriate authority and oversight within each college.

Estimated date of completion is May 31, 2010.

## **TECHNICAL VULNERABILITIES**

Technical vulnerabilities existed on a variety of systems throughout the campus.

Our external testing of selected servers disclosed 215 vulnerabilities on a variety of servers. We provided the specific details of these vulnerabilities to the campus.

Additionally, ITS did not coordinate the deployment of servers in the decentralized computing environment, nor did it provide professional standards and guidance related to such deployments. The decentralized servers were not routinely patched, and there was no baseline standard for server or application security.

The director of network services stated that the lack of centralized information technology (IT) oversight and direction had permitted the majority of these vulnerabilities to propagate in the decentralized computing environments.

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

### **Recommendation 11**

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

In addition, we recommend that the campus:

- a. Implement a patch management process that ensures servers and other computers are applied with security updates on a routine and consistent basis.
- b. Formalize a consistent process that requires the review of web applications for security vulnerabilities on a periodic basis.
- c. Provide all the decentralized non-ITS units with a security baseline standard for securing servers.

### **Campus Response**

We concur. The campus will address all identified and presented technical vulnerabilities by June 2010. In addition, the campus will do the following:

- a. Develop a patch management process to ensure that servers and other computers receive and apply security updates on a routine and consistent basis by June 2010.
- b. Develop and formalize a consistent process that requires the review of web applications for security vulnerabilities on a periodic basis by June 2010.

- c. Distribute to non-ITS units a security baseline standard for securing servers by May 2010.

## **SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

The campus lacked written procedures to test for vulnerabilities in web applications prior to their deployment into the production environment, and professional application development standards and methodologies were absent or inadequate.

The academic technology support specialist stated that their department had always relied on the developers to review their own applications for vulnerabilities.

The lack of proper web application development testing procedures increases the risk that web application projects may contain vulnerabilities.

### **Recommendation 12**

We recommend that the campus:

- a. Formalize a baseline standard and require the review of applications for security vulnerabilities prior to deployment into the production environment.
- b. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing applications.

### **Campus Response**

We concur. The campus will develop and formalize standards for reviewing applications for security vulnerabilities prior to production deployment and create standards for developers to follow and comply with prior to deployment of Internet-facing applications by April 2010.

## **SYSTEMS SECURITY AND MONITORING**

### **VULNERABILITY MANAGEMENT**

The campus' process for detecting vulnerabilities related to the security of servers and desktops connected to the campus network required improvement.

Although ITS performed periodic vulnerability scans for servers within its control, the campus did not have a consistent process for monitoring, detecting, and remediating vulnerabilities on other decentralized servers.

The associate vice president of ITS stated that since both ITS and office of academic technology servers in the data centers are monitored on a regular basis, she felt comfortable that vulnerabilities on those servers were remediated effectively.

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

### **Recommendation 13**

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

### **Campus Response**

We concur. The campus will develop a consistent process to scan servers and desktops that are connected to the campus network for vulnerabilities by July 2010.

## **NETWORK MONITORING**

The campus lacked a formal process to identify and monitor all IT resources on the campus network, which included servers, workstations, and laptops that were owned and managed by non-ITS college technology environments or the other colleges and divisions.

We noted that any user on the network had the ability to place a server on the campus network without receiving authorization from ITS.

The associate vice president of ITS stated that the decentralized nature of the campus environment made it difficult to identify and track all IT resources placed on the network.

The inability to identify and monitor all campus IT resources (servers, workstations, and laptops) can leave the campus vulnerable to both internal and external attacks that could slow or disrupt the network. This also increases the risk that an attacker could inject malicious code or viruses into the network or compromise confidential information.

### **Recommendation 14**

We recommend that the campus:

- a. Identify all current campus-owned IT assets (including hardware, software, operating system versions, etc.) on the campus network and implement a process to monitor these assets for adequate security.
- b. Implement a formal process for campus users that requires them to receive ITS' authorization prior to adding a server to the network.

### **Campus Response**

We concur. The campus will:

- a. Develop a process to identify all campus-owned IT assets on the campus network and monitor them for adequate security by July 2010.
- b. Implement a process that requires campus users to receive ITS' authorization prior to adding a server to the network by July 2010.

### **GRANTING OF ADMINISTRATIVE ACCESS**

The campus lacked a formal process for the granting and management of privileged system-level access to accounts on all servers.

The director of network services stated his belief that a more formalized process was not required due to the limited number of people allowed privileged system-level access.

The lack of a formal process for granting and managing 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 15**

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

### **Campus Response**

We concur. The campus will develop a formal process for managing and granting privileged system-level access to accounts on all servers and develop a method to track, review, and periodically audit access by May 31, 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 Simple Network Management Protocol (SNMP). SNMP is unencrypted and could allow an attacker to capture device configuration settings, including authentication details.
- ▶ One device was enabled with Telecommunication Network (Telnet). Because Telnet transfers user logins, passwords, and commands across the network in clear text, this could allow a remote attacker to obtain confidential authentication tokens, which could enable remote access to the devices.

The associate vice president of ITS stated that the campus is compliant with the chancellor's office guidance regarding these devices.

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

### **Recommendation 16**

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

In addition, we recommend that the campus:

- a. Formalize a security baseline and require the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the network environment to identify potential vulnerabilities.

### **Campus Response**

We concur. The campus will address all identified and presented network device vulnerabilities by July 2010. In addition, the campus will formalize its process to review network devices to the CSU's security baseline for vulnerabilities prior to deployment by July 2010. This process will include the review of existing or new devices prior to deployment onto the campus network for potential vulnerabilities and patch management.

## **NETWORK ARCHITECTURE**

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

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

The associate vice president of ITS stated that the network had not been segregated due to other priorities on campus.

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

### **Recommendation 17**

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

### **Campus Response**

We concur. ITS has reviewed the network topology and acquired and installed an additional data center firewall in front of the campus' web servers and other Internet-accessible servers. Corrective action on this issue is complete.

## **REVIEW OF SECURITY EVENT LOGS**

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

We noted that reviews of security event logs were performed informally and were not documented.

The associate vice president of ITS stated that network activity was monitored on a continual basis and that security event logs were reviewed on an as-needed basis.

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

### **Recommendation 18**

We recommend that the campus:

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

### **Campus Response**

We concur. The campus will formally document by August 2010 its network monitoring process which identifies potential network vulnerabilities and breaches and regularly reviews and analyzes security event logs on the campus network. In addition, the campus will consider implementing security tools that will centralize security event monitoring for trend analysis, logging, and automated notification by August 2010.

## **PROTECTED DATA**

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

The campus had not completed a campus-wide assessment to identify sensitive data on all servers, workstations, and laptops, and it did not have a formal process to identify, approve, or review access to confidential information owned and managed by campus decentralized sites.

The associate vice president of ITS stated that the campus did not have the tools to properly assess sensitive data on all servers, workstations, and laptops.

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

### **Recommendation 19**

We recommend that the campus:

- a. Complete a campus-wide assessment to identify sensitive data on all servers and workstations.
- b. Develop a formal process to identify, approve, or review access to confidential information owned and managed by decentralized colleges and divisions.

### **Campus Response**

We concur. The campus will develop a process and research tools to perform a campus-wide assessment by September 2010 to identify sensitive data on all servers and workstations. In addition, the campus will develop a formal process by July 2010 to identify, approve, or review access to confidential information owned and managed by decentralized colleges and divisions.

## **LOST/STOLEN COMPUTERS**

Lost or stolen equipment that might contain protected data was not consistently reported to the information security office.

The information security officer stated that although it had communicated this process to all the departments, the departments might not have complied with it.

Inadequate procedures for the reporting of lost or stolen equipment, which might 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 20**

We recommend that the campus ensure that all lost/stolen laptops are reported to the information security office.

#### **Campus Response**

We concur. The campus police will ensure that all lost/stolen laptops are reported to the information security office. Corrective action on this issue is complete.

## **DISPOSITION OF PROTECTED DATA**

Procedures to ensure that all sensitive information on computers is properly deleted prior to disposition required improvement.

We noted that:

- ▶ Certain departments did not consistently use approved methods to wipe hard drives.
- ▶ The campus lacked a formal process to ensure and document hard-drive wiping.

The information security officer stated that departments are responsible for wiping their own drives prior to disposition but that they may not have followed best practices in doing so.

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

### **Recommendation 21**

We recommend that the campus update its procedures to ensure that hard-drive wiping is performed using approved methods and sufficiently documented, including retention of documentation.

**Campus Response**

We concur. The campus will update its procedures for equipment re-deployment and surveying, including communications to the university regarding the hard-drive wiping procedures and where to find them. Estimated date of completion is May 31, 2010.

---

## APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
F. King Alexander	President
Tom Angel	Director, Staff Human Resources
Scott Apel	Associate Vice President, Human Resources Management
Martin Brenner	Director of Technology, College of the Arts
Kathleen Clark	Coordinator, Decentralized Services and Electronic Medical Records
Janet Foster	Associate Vice President, Information Technology Services
Laurinda Fuller	Internal Auditor, Internal Auditing Services (At time of review)
Don Gardner	Associate Vice President of Academic Technology
Dixie Grimmet	Dean, College of Health and Human Services
Bill Grissom	Manager of Technical Support, College of Liberal Arts
Jill Horn	Technology Support Specialist, Office of Academic Technology
Craig Kleen	Assistant Director of Network Services
Steve La	Director of Network Services
Brian Lawver	Director of Advancement Services
Robert Loeschen	Director of Instructional and Research Facilities
Michael Markoski	Director of Administrative Computing Services
Danny Nguyen	Information Technology Coordinator, College of Natural Sciences and Math
Mike Nosow	Director of Technology, College of Health and Human Services
Donald J. Para	Dean, College of the Arts
Gerie Riposa	Dean, College of Liberal Arts
Jon Rosene	Lead Dispatcher, Police Services
Maryann Rozanski	Information Security Officer
Beth Ryan	Director, Human Resources Group
Aysu Spruill	Director, Internal Auditing Services
Mary Stephens	Vice President of Administration and Finance
Eugene Wohlgezogen	Assistant Information Security Officer



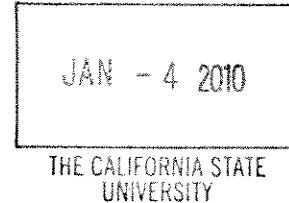
CALIFORNIA STATE UNIVERSITY, LONG BEACH

DIVISION OF ADMINISTRATION AND FINANCE

December 24, 2009

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

RECEIVED  
UNIVERSITY AUDITOR



Re: Response to Information Security Audit #09-35

Dear Larry:

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

Please let me know if we can provide you with any additional information.

Sincerely,

A handwritten signature in black ink, appearing to read "Mary Stephens".

Mary Stephens  
Vice President for Administration and Finance

Enclosure

IA-0230

c: F. King Alexander, President  
Janet Foster, Associate Vice President, Information Technology Services  
Don Gardner, Associate Vice President, Academic Technology  
Ted Kadowaki, Associate Vice President, Budget and University Services  
Aysu Spruill, Director, Internal Auditing Services

**INFORMATION SECURITY**  
**CALIFORNIA STATE UNIVERSITY,**  
**LONG BEACH**

**Audit Report 09-35**

**SECURITY GOVERNANCE**

**SECURITY ORGANIZATION**

**Recommendation 1**

We recommend that the campus:

- a. Formally define and communicate divisional information security officers' roles, responsibilities, and authority.
- b. Develop a process to track and report on the various divisions' ongoing compliance with campus information security policies and procedures.

**Campus Response**

We concur.

- a. The campus will formally define and communicate divisional information security officers' roles, responsibilities, and authority by formal delegation of authority letters.
- b. The campus will develop a process to monitor divisions' ongoing compliance with campus information security policies and procedures.

Estimated date of completion is May 31, 2010.

**INFORMATION SECURITY POLICY**

**Recommendation 2**

We recommend that the campus update its information security policy to reflect current business practices.

**Campus Response**

We concur. We updated the campus' information security policy to reflect current business practices. Corrective action on this issue is complete.

## **REMOTE COMPUTING**

### **Recommendation 3**

We recommend that the campus create a policy addressing the authorization, management, and monitoring of mobile computing and the associated remote access to campus resources.

### **Campus Response**

We concur. A draft policy has been developed and is in the process of review and approval. Estimated date of completion is May 31, 2010.

## **EMPLOYEE-OWNED COMPUTERS**

### **Recommendation 4**

We recommend that the campus develop a policy to address the use of employee-owned computers with access to campus resources.

### **Campus Response**

We concur. A draft policy has been developed and is in the process of campus review and approval. Estimated date of completion is May 31, 2010.

## **INFORMATION SECURITY AWARENESS TRAINING**

### **Recommendation 5**

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

### **Campus Response**

We concur. The information security awareness training will now be offered to CSULB Faculty. Estimated date of completion is May 31, 2010.

## **EMPLOYEE SEPARATION**

### **Recommendation 6**

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**

We concur. The campus modified its personnel exit process form to include a reminder of ongoing legal responsibility to maintain the security of protected data. Corrective action on this issue is complete.

## **BACKGROUND CHECKS**

### **Recommendation 7**

We recommend that the campus revise procedures to implement background checks for information technology professionals with privileged access to campus systems.

### **Campus Response**

We concur. The campus will revise its procedures to implement background checks for information technology professionals with privileged access to campus systems. Corrective action on this issue is complete.

## **INFORMATION SECURITY PLAN**

### **Recommendation 8**

We recommend that the campus create a formal action plan to identify and prioritize information security risks and establish a specified timeline to address identified risks.

### **Campus Response**

We concur. The campus will create a formal action plan. Estimated date of completion is May 31, 2010.

## **RECORD RETENTION**

### **Recommendation 9**

We recommend that the campus revise its record retention action plan to formally designate its custodians of records.

### **Campus Response**

We concur. The campus will revise its record retention action plan to formally designate its custodians of records. Estimated date of completion is May 31, 2010.

## **DECENTRALIZED COMPUTING**

### **NON-ITS COMPUTING ENVIRONMENTS**

#### **Recommendation 10**

We recommend that the campus:

- a. Eliminate administrative access to computers unless specifically approved.

- b. Encrypt desktops and/or laptops that store Level 1 data on desktops and laptops.
- c. Ensure that backups are stored off-site.
- d. Ensure all passwords meet minimum campus standards.
- e. Ensure that departmental system administrators have a designated backup.
- f. Ensure that college information technology professionals have appropriate authority and oversight to implement information security best practices within the college environments as defined by university policies and procedures.

### **Campus Response**

We concur.

- a. We will eliminate administrative access to computers and create an approval process for exceptions. Exceptions required to carry out business or academic efforts will be documented, tracked and managed in a standard manner.
- b. We will encrypt desktops/laptops storing Level 1 data.
- c. We will ensure that backups are stored off-site.
- d. We will ensure all passwords meet minimum campus standards.
- e. We will ensure that departmental system administrators have designated backups.
- f. The campus will ensure the college information technology professionals follow established university policies and procedures to implement information security best practices within the college environments and with appropriate authority and oversight within each college.

Estimated date of completion is May 31, 2010.

### **TECHNICAL VULNERABILITIES**

#### **Recommendation 11**

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

In addition, we recommend that the campus:

- a. Implement a patch management process that ensures servers and other computers are applied with security updates on a routine and consistent basis.
- b. Formalize a consistent process that requires the review of web applications for security vulnerabilities on a periodic basis.

- c. Provide all the decentralized non-ITS units with a security baseline standard for securing servers.

**Campus Response**

We concur. The campus will address all identified and presented technical vulnerabilities by June 2010. In addition, the campus will do the following:

- a. The campus will develop a patch management process to ensure that servers and other computers receive and apply security updates on a routine and consistent basis by June 2010.
- b. The campus will develop and formalize a consistent process that requires the review of web applications for security vulnerabilities on a periodic basis by June 2010.
- c. The campus will distribute to non-ITS units a security baseline standard for securing servers by May 2010.

**SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT**

**Recommendation 12**

We recommend that the campus:

- a. Formalize a baseline standard and require the review of applications for security vulnerabilities prior to deployment into the production environment.
- b. Develop a campus-wide application development standard to which all developers must comply prior to deploying any Internet-facing applications.

**Campus Response**

We concur. The campus will develop and formalize standards for reviewing applications for security vulnerabilities prior to production deployment and create standards for developers to follow and comply with prior to deployment of internet facing applications by April 2010.

**SYSTEMS SECURITY AND MONITORING**

**VULNERABILITY MANAGEMENT**

**Recommendation 13**

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

**Campus Response**

We concur. The campus will develop a consistent process to scan servers and desktops that are connected to the campus network for vulnerabilities by July 2010.

**NETWORK MONITORING**

**Recommendation 14**

We recommend that the campus:

- a. Identify all current campus-owned IT assets (including hardware, software, operating system versions, etc.) on the campus network and implement a process to monitor these assets for adequate security.
- b. Implement a formal process for campus users that requires them to receive ITS' authorization prior to adding a server to the network.

**Campus Response**

We concur.

- a. The campus will develop a process to identify all campus-owned IT assets on the campus network and monitor them for adequate security by July 2010.
- b. The campus will implement a process that requires campus users to receive ITS' authorization prior to adding a server to the network by July 2010.

**GRANTING OF ADMINISTRATIVE ACCESS**

**Recommendation 15**

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

**Campus Response**

We concur. The campus will develop a formal process for managing and granting privileged system-level access to accounts on all servers and develop a method to track, review and periodically audit access by May 31, 2010.

**FIREWALLS AND ROUTING AND SWITCHING DEVICES**

**Recommendation 16**

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

In addition, we recommend that the campus:

- a. Formalize a security baseline and require the review of network devices for security vulnerabilities prior to deployment.
- b. Implement a comprehensive, campus-wide patch management process. This process would include the review of existing device configurations on a periodic basis or new configurations prior to deployment into the network environment to identify potential vulnerabilities.

**Campus Response**

We concur. The campus will address all identified and presented network device vulnerabilities by July 2010. In addition, the campus will formalize its process to review network devices to the CSU's security baseline for vulnerabilities prior to deployment by July 2010. This process will include the review of existing or new devices prior to deployment onto the campus network for potential vulnerabilities and patch management.

**NETWORK ARCHITECTURE**

**Recommendation 17**

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

**Campus Response**

We concur. ITS has reviewed the network topology and acquired and installed an additional data center firewall in front the campus' web servers and other internet-accessible servers. Corrective action on this issue is complete.

**REVIEW OF SECURITY EVENT LOGS**

**Recommendation 18**

We recommend that the campus:

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

### **Campus Response**

We concur. The campus will formally document by August 2010 its network monitoring process which identifies potential network vulnerabilities and breaches and regularly reviews and analyzes security event logs on the campus network. In addition, the campus will consider implementing security tools that will centralize security event monitoring for trend analysis, logging, and automated notification by August 2010.

## **PROTECTED DATA**

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

#### **Recommendation 19**

We recommend that the campus:

- a. Complete a campus-wide assessment to identify sensitive data on all servers and workstations.
- b. Develop a formal process to identify, approve, or review access to confidential information owned and managed by decentralized colleges and divisions.

#### **Campus Response**

We concur. The campus will develop a process and research tools to perform a campus wide assessment by September 2010 to identify sensitive data on all servers and workstations. In addition, the campus will develop a formal process by July 2010 to identify, approve or review access to confidential information owned and managed by decentralized colleges and divisions.

## **LOST/STOLEN COMPUTERS**

#### **Recommendation 20**

We recommend that the campus ensure that all lost/stolen laptops are reported to the information security office.

#### **Campus Response**

We concur. The campus police will ensure that all lost/stolen laptops are reported to the information security office. Corrective action on this issue is complete.

## **DISPOSITION OF PROTECTED DATA**

#### **Recommendation 21**

We recommend that the campus update its procedures to ensure that hard-drive wiping is performed using approved methods and sufficiently documented, including retention of documentation.

**Campus Response**

We concur. Updates to the procedures for equipment re-deployment and surveying, including communications to the university regarding the hard drive wiping procedures and where to find them. Estimated date of completion is May 31, 2010.

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

BAKERSFIELD

January 22, 2010

CHANNEL ISLANDS

CHICO

**MEMORANDUM**

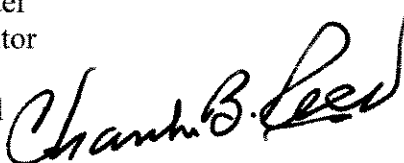
DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel  
University Auditor

FRESNO

FROM: Charles B. Reed  
Chancellor



FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 09-35 on *Information Security*,  
California State University, Long Beach

LONG BEACH

LOS ANGELES

In response to your memorandum of January 22, 2010, I accept the response as submitted with the draft final report on *Information Security*, California State University, Long Beach.

MARITIME ACADEMY

MONTEREY BAY

CBR/amd

NORTHRIDGE

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS