

INFORMATION SECURITY

SYSTEMWIDE

Audit Report 08-13

August 23, 2010

Members, Committee on Audit

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

Staff

University Auditor: Larry Mandel
Senior Director: Michelle Schlack
IT Audit Managers: Greg Dove, Gary Miller
Senior Auditors: Alec Lu and Dominick Owens
Internal Auditor: Sal Rodriguez

BOARD OF TRUSTEES

THE CALIFORNIA STATE UNIVERSITY

CONTENTS

Executive Summary	1
Introduction	4
Background	4
Purpose.....	5
Scope and Methodology.....	7

OBSERVATIONS, RECOMMENDATIONS, AND MANAGEMENT RESPONSES

Systemwide Information Security	9
Information Security Governance	9
Systemwide Information Security Program	11
Campus Information Security Oversight	13
Decentralized Computing.....	15
Campus Security Governance	15
Incident Response	17
System Development and Change Management.....	18
Web Application Development and Maintenance	18
Web Application Vulnerability Management	20
System Security and Monitoring.....	21
Protected Data	23

APPENDICES

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

ABBREVIATIONS

CIO	Chief Information Officer
CMS	Common Management Systems
CO	Office of the Chancellor
CSU	California State University
EH&S	Environmental Health & Safety
FMS	Facilities Management and Services
HR	Human Resources
IEC	International Electrotechnical Commission
ISMO	Information Security Management Office
ISMS	Information Security Management System
ISO	International Organization for Standardization
I&IT	Instructional and Information Technology
IT	Information Technology
OWASP	Open Web Application Security Project
PCI DSS	Payment Card Industry Data Security Standard

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 19 campuses and the Office of the Chancellor (CO) from March 9, 2008, through December 16, 2009, and audited the procedures in effect at that time. These audits will be collectively referred to as “the campuses” for purposes of this report unless specifically noted. The campus-specific findings and recommendations have been discussed and reported individually.

Our study and evaluation revealed certain conditions that, in our opinion, could result in continual risk exposures if not corrected. The audit of information security is different from other audit topics because it is an ongoing process, and security configuration changes are continuous. In addition, the management of information security must continue to evolve because threats are constantly changing, statutory regulations continue to change, the work force is becoming more mobile, and external malicious forces continue to evolve. In general, many of the individual campus audits identified a significant number of information security issues and concerns. We also noted that many of the individual campus issues identified were symptoms of much larger issues that would be more effectively addressed through systemwide guidance and collaboration.

Specifically, the California State University (CSU) had not formally defined and delegated authority to the CSU Information Security Management Office, and the organizational reporting structure represents a potential conflict of interest. In addition, many of the individual campus issues identified related to disparity in overall governance of information security that was exacerbated by organizational structures like the decentralized campus computing environments. Special attention should be given to the decentralized computing environment which, in its current form, does not provide for secure adaption of new mobile computing technologies, does not easily accommodate implementation of strategic initiatives like identity management, and creates redundant security concerns in superfluous equipment, trained personnel and physical security of facilities, all of which can have adverse effects on the management of information security. The details of these issues are addressed later in this report. In addition, some technical problems that were identified should be considered for systemwide solutions to leverage purchasing power, and technical expertise and labor.

In our opinion, the operational and administrative controls of information security in effect as of December 16, 2009, taken as a whole, were not sufficient to meet many of the objectives for a secured computing environment. While most of the campus information technology (IT) department control environments were satisfactory and provided appropriate safeguards over the critical financial and student systems, other campus systems and the decentralized computing environments that were not under the purview of central 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.

SYSTEMWIDE INFORMATION SECURITY [9]

The CSU did not have a fully established information security governance structure to guide the development and management of a comprehensive information security program that supports business objectives. The CSU Information Security Management Office did not have a comprehensive information security program to effectively address the information security needs of the system. The CSU had not defined a maturity model for the information security office or for the individual campuses, had not performed a gap analysis nor defined the steps needed to achieve program maturity. Guidance and oversight of campus information security programs was not sufficient to effectively organize, coordinate or address systemwide information security initiatives or ensure compliance with relevant laws, regulations, and CSU policies.

DECENTRALIZED COMPUTING [15]

The current implementation of the decentralized computing model, used at many campuses, did not lend itself to an efficient information security structure, which resulted in redundant data center physical security controls, underutilized computer equipment that had to be separately protected, inadequate systems administration training, network and security complexities and deficiencies, and increased difficulty in implementing new technology initiatives affecting security such as identity management. The incident response and resolution process was not performed with consistency and guaranteed reliability across the campuses, and relevant personnel had not been trained consistently in computer forensics.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [18]

Website development methodologies used at the various campuses were inconsistent, often lacked key process controls, did not always provide adequate vulnerability testing, lacked software tools for code management, and were often performed on each campus by multiple decentralized departments without campus guidance or oversight. Website development methodologies used at the various campuses did not always provide adequate vulnerability testing and lacked software tools for vulnerability assessment.

SYSTEM SECURITY AND MONITORING [21]

Many of the campuses lacked software tools that would enable them to proactively monitor system logs intrusion attempts and tools to identify vulnerable network servers and devices.

PROTECTED DATA [2322]

The CSU does not have an adequate process for ensuring that protected data remains secure and is not inadvertently exposed, and does not conduct an annual assessment of protected data.

INTRODUCTION

BACKGROUND

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

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

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

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

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

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

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

At many CSU campuses, an IT services department has overall responsibility for the management of campus systems and networks. However, a significant level of decentralization has shifted many critical IT responsibilities to individual colleges and ancillary departmental units throughout the campus.

PURPOSE

Our overall audit objective was to ascertain the effectiveness of existing policies and procedures related to the administration of information security and to determine the adequacy of controls over the related processes to evaluate adherence to an industry-accepted standard, ISO 17799/27002, *Code of Practice for Information Security Management*, and to ensure compliance with relevant governmental regulations, Trustee policy, Office of the Chancellor directives, and campus procedures.

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

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

- ▶ Security responsibilities are addressed prior to employment so that users are aware of information security threats and concerns and are equipped to support organizational security policy in the course of their normal work; and procedures are in place to ensure 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 CSU campuses. 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 MANAGEMENT RESPONSES

SYSTEMWIDE INFORMATION SECURITY

INFORMATION SECURITY GOVERNANCE

The California State University (CSU) did not have a fully established information security governance structure to guide the development and management of a comprehensive information security program that supports business objectives.

Such governance structure will generally consist of:

- ▶ A comprehensive security strategy intrinsically linked with business objectives.
- ▶ Governing security policies that address each aspect of strategy, controls, and regulations.
- ▶ A complete set of standards for each policy to ensure procedures and guidelines comply with policy.
- ▶ An effective security organization structure void of organizational conflicts of interest.
- ▶ Institutionalized monitoring process to ensure compliance and provide feedback on effectiveness.

We noted that:

- ▶ The CSU organizational structure did not provide sufficient independence for the Office of the Chancellor's Information Security Management Office (ISMO). This office reported directly to the chief information officer (CIO), who reported to the executive vice chancellor and chief financial officer.
- ▶ There was no defined charter for the ISMO, and the Board of Trustees and/or the Chancellor had not formally delegated overall authority and responsibility for systemwide monitoring and accountability.
- ▶ The systemwide Information Security Policy and Standards had not been issued despite a three-year effort.

The CIO stated that the Information Security Program had been expanding over the past several years, as the initial foundations were being formed. Furthermore, although organizational changes were proposed, progress was delayed during the employment search for a permanent information security officer.

The scope of information security initiatives encompasses all aspects of the CSU operations. Subordinate reporting to the finance department or other operating departments could create conflicting priorities, could lead to suppressed discoveries, and could result in inadequate or conflicting budgetary decisions for projects. Failure to create a departmental charter and receive

formal delegation of authority could result in a program mission that is not properly aligned with CSU goals. Failure to receive formal authority to implement information security initiatives on a systemwide basis could result in campus failure to implement timely changes that are needed to safeguard CSU systems and data. Lack of formal policies and procedures could lead to confusion regarding management's intent and could cause unintentional actions that are not aligned with that intent, or result in data not being adequately or properly protected.

Recommendation 1

We recommend that the Office of the Chancellor (CO):

- a. Improve independence of the CSU ISMO by either moving the function to a more direct reporting relationship to the Chancellor, or to a department that is independent of day-to-day business operations.
- b. Create a charter for the ISMO that outlines the operational framework for the department and states the overall goals and mission.
- c. Formally delegate authority to the ISMO to monitor systemwide information security responsibilities and consider establishing the campus information security officer as a dotted-line reporting relationship.
- d. Issue the systemwide information security policy and standards, communicate the policy and standards to the campuses, and develop a process to ensure that the policy and standards are implemented by the campuses and periodically reviewed and updated to reflect the current environment.

Management Response

We concur.

The CO will develop a charter for ISMO that defines the mission and objectives of the systemwide information security program, outlines operational framework for the department, delegates authority to the systemwide ISMO to review CSU information security programs, and directs the ISMO to advise and provide guidance to CSU campuses on security related issues. The CO will evaluate the reporting relationship of the ISMO to identify and mitigate potential conflicts of interest.

The CSU information security policy was approved and communicated to campuses in May 2010. Policies, standards, procedures, and guidelines are communicated to the campuses through several channels, including, but not limited to: the Integrated California State University Administrative Manual, the Information Security Advisory Committee (ISAC), and the ISAC listserv.

The CSU information security policy assigns responsibility to the ISMO to conduct an annual review of the systemwide information security policy and, in accordance with the CSU information security policy, "update as necessary to reflect changes in the CSU's academic, administrative, or technical environments, or applicable laws and regulations."

Target completion date: July 1, 2011

SYSTEMWIDE INFORMATION SECURITY PROGRAM

The CSU ISMO did not have a comprehensive information security program to effectively address the information security needs of the system. The CSU had not defined a maturity model for the information security office or for the individual campuses, had not performed a gap analysis, nor defined the steps needed to achieve program maturity.

A well-managed information security office should address the following concerns:

- ▶ The information security program should reflect the risks and complexity of the organization.
- ▶ The program should actively investigate and implement new ways of protecting the organization from harm based on threat trends.
- ▶ The program should include an active education and awareness effort, so that management and staff understand their individual roles and responsibilities.
- ▶ The security measures and controls should be regularly tested for operational effectiveness and ensure corrective actions are occurring.
- ▶ Performance should be measured and reported to executive management.
- ▶ The organization's security should be regularly compared with other well-run organizations that are similar to the CSU.

The ISMO had created an information security program and established some general guidance; however, the office had not made a broad, top-down, assessment of information security initiatives. We noted that many of the problems that were identified during the campus audits were attributed to the existing information security model not keeping pace with new technology and changing workforce demands.

Specifically, we noted that:

- ▶ The CSU had not defined what the mature information security program should entail. We noted that there was no information security maturation model; the CSU had not investigated the broader use of available resources that could be incorporated into a security program that collaborates between the faculty, students, and campus security personnel; nor had the CSU actively pursued federal grant money to develop and provide information security best practices. Already within the CSU, one campus had received Title 5 grant money to develop an information security awareness-training program, and another campus computer science department teaches cyber security and hosts an annual student competition in partnership with the United States Navy. The CSU could benefit from taking a systemwide approach to information security initiatives that incorporates all campuses, relevant faculty departments, and students.

- ▶ Information security programs were not effective on many campuses. Specifically, we noted that many campuses were understaffed and did not have full-time staff assigned to information security. We also noted that at certain campus, information security staff lacked professional certification, were not professionally trained in security, lacked necessary software assessment tools, and did not consistently solicit assistance from other technical groups in their campus communities. In addition, there was no consistent assistance provided by the ISMO to help these campuses in addressing their deficiencies.
- ▶ The CSU has not provided guidance or expectations to individual campus information security offices regarding their individual governance models, which vary widely, and have wide disparities in their scope, objectives, reporting and authority. Some campuses had not sufficiently defined the security roles or assigned delegation of authority. Others did not have adequate information security action plans, or had not performed comprehensive security risk assessments.
- ▶ The CSU had not established a uniform position or basic guidance for the campuses regarding implementation of new computing technologies that could adversely affect information security, such as unauthenticated wireless and wired network access, as well as other technologies. For example, we noted a wide disparity among campuses regarding whether authentication was enforced for public wireless access, and in some cases for wired connection to the campus network. In addition, many campuses had inadequate practices for monitoring, restricting, and securing access through network wall jacks.

Systemwide management stated that significant progress had been made in establishing the information security organization and structure, and in creating systemwide policies but that expansion of the program into a proactive posture had not yet been addressed.

Failure to implement a proactive posture for the information security office leaves the system in a reactive model and does not enable the CSU to identify new security trends and technologies, or to adopt them in a timely manner. Lack of guidance in campus security governance models, could lead to wide variance in how information security is addressed and result in differing levels of scope and authority, and could hamper the ability of the system to collect data on and monitor the overall security posture of the system. Further, not establishing consistent approaches to the implementation of technologies could result in installations that could put the system at risk or that do not comply with management expectations.

Recommendation 2

We recommend that the CO:

- a. Develop an information security model for the CSU system and also for the individual campuses, and define the steps necessary to achieve program maturation.
- b. Examine how the CSU could best incorporate the collective resources that are available within the system and develop a platform of cooperation in which all existing CSU information security resources work together in a collaborative effort to create a world-class information security organization.

- c. Create an information security governance model that can be implemented by the individual campuses to ensure that there is consistency in management oversight, in breadth and scope of information security operations, and in assessing risk, planning, and executive reporting.
- d. Develop and implement a common standard for new and existing technologies that establishes a consistent and reliable model that can effectively address information security risks and that establishes a compliance baseline.

Management Response

We concur.

The CO will develop information security models for the systemwide and individual campus programs. The models will describe steps to achieve program maturity and include strategies for governing campus information security programs.

The CSU Information Security Advisory Committee fosters collaboration among the CSU security professionals. The CO will identify other opportunities to increase collaboration among CSU information security resources.

The CO will develop a standard for new and existing technologies that effectively address information security risks.

Target completion date: July 1, 2011

CAMPUS INFORMATION SECURITY OVERSIGHT

Guidance and oversight of campus information security programs was not sufficient to effectively organize, coordinate or address systemwide information security initiatives or ensure compliance with relevant laws, regulations, and CSU policies.

We noted that existing processes and procedures did not provide for effective collection or reporting of the overall progress or direction of key security initiatives that should have a systemwide focus. Specifically, we noted that:

- ▶ There was no centralized monitoring or assessment of the individual campus information security programs, which did not allow for analysis of the risks facing multiple campuses or campus-specific projects that might best be addressed with a systemwide initiative.
- ▶ There was no consistent process to ensure compliance with relevant laws, regulations, and CSU policies related to information security. For example, half of the campuses audited were not in full compliance with the CSU's record retention and disposition policies. The existing model, in which the CO monitors changes in laws that could have broad ranging effect on CSU practices and technologies, often duplicates effort between the various campuses. The CSU seems to take a reactive approach to the issuance of new state and federal legislation, Payment Card Industry

and Data Security Standard (PCI DSS) and other industry compliance issues as related to CSU information security responsibility and applicability.

- ▶ The systemwide information security policy had not been issued despite a three-year effort. Accordingly, there were no guidelines for performing an information security risk assessment, and most campus security plans were incomplete, not based on a comprehensive risk assessment, not prioritized by risk and did not include target completions dates. We also noted there was no systemwide requirement or policy to submit the results of campus risk assessments to the ISMO for executive management reporting.

Systemwide management stated that the ISMO and overall CSU information security oversight responsibilities were relatively new. Hence, emphasis had been placed on overall organization and coordination of the individual campus offices, and not yet on consistent monitoring and reporting, or expanding the program to include more proactive practices to address the information security needs of the CSU.

Lack of overall monitoring and coordination of the campus information security initiatives could affect the CSU's ability to identify the campus security operations' needs broadly. Failure to create a centralized process to monitor changing laws and regulations could cause redundant effort among the campus information security offices, and could lead to inconsistent interpretation and compliance. Failure to perform a comprehensive information security risk assessment could lead to significant omissions from the security plan. Furthermore, inadequate risk-based security reporting to executive management could omit significant projects from executive oversight and acknowledgement.

Recommendation 3

We recommend that the CO:

- a. Develop and implement a monitoring process for the campus information security offices; track their significant initiatives and impediments to ascertain whether the CO could provide systemwide assistance; and provide a means for executive reporting of the systemwide information security posture.
- b. Develop and implement a centralized program to monitor legislative initiatives and disseminate the information to the campuses. Consider implementing a certification process for campus compliance with applicable laws and regulations.
- c. Ensure that the campuses have plans to comply with the systemwide information security policy; assist the campuses by creating a risk assessment and reporting model to ensure that all information security risks are being properly captured and campus executives are timely presented with risk-based priorities.

Management Response

We concur.

The CO will develop and implement a process to review campus information security programs and monitor campus efforts to comply with the systemwide information security policy. The ISMO will work collaboratively with campus information security officers to track significant campus initiatives and impediments and identify opportunities for the CO to provide systemwide assistance. The process will include executive-level reporting on the CSU's information security posture.

The CO will develop a systemwide program to monitor and distribute information regarding legislative initiatives. The CO will consider implementing a certification process in the systemwide compliance program.

The CO will work collaboratively with CSU security professionals to identify (or develop, if necessary) risk management and reporting tools to ensure that information security risks are properly documented and campus executives are made aware of risk-based priorities.

Target completion date: July 1, 2011

DECENTRALIZED COMPUTING

CAMPUS SECURITY GOVERNANCE

The current decentralized computing model, used at many campuses, did not lend itself to an efficient or effective information security structure. It resulted in redundant data center physical security controls; underutilized computer equipment that required separate protection; inadequate systems administration training; network and security complexities and deficiencies; and increased difficulty in implementing new technology initiatives affecting security such as identity management. We identified numerous information security compliance issues on campuses that had implemented a decentralized computing model.

We found that the campus decentralized computing model led to:

- ▶ Inadequate physical security of computing equipment. Many colleges and departments have constructed and maintained computer room facilities that are separate and, in most cases, redundant to the main campus data center. These college and department computer facilities did not have the necessary physical and environmental controls that are common in the main campus data center facilities. In order to protect the decentralized equipment and to comply with environmental controls, these decentralized facilities would require duplicate spending on fire suppression, air conditioning, door access controls, system backup, and emergency power. In some cases, servers were located under the desks of employees.
- ▶ Ineffective use of new technologies that could reduce information security maintenance. We found that the decentralized physical servers were not consistently patched, updated, tested, or

monitored. The campuses were not taking full advantage of recent changes in server technology, which allow the consolidation of physical servers that are now capable of emulating multiple virtual servers. By failing to utilize this new technology, the CSU could not optimize server capacity and reduce the number of physical servers, which would reduce the number of servers that must be secured.

- ▶ Inadequate security training of personnel. Operating multiple independent servers requires redundant personnel for system administration and increases the technical training requirements and training for information security practices. We found that most of the decentralized server environments were not adequately managed, resulting in extensive compliance deficiencies and numerous exploitable vulnerabilities.
- ▶ Inadequate logical security of server environments. Many decentralized computing environments operated separate and redundant active directory domains, which added detrimental complexity to the issuance and removal of network access, resulted in non-compliance with campus policies, and created additional detrimental security complexity to the systemwide efforts to implement identity management technologies.
- ▶ Inadequate monitoring and tracking of security incidents. Decentralized support for desktop services adversely affected the efforts of the information security office to track, monitor, and report on the various types of computer infections. The decentralized departments did not consistently track or report compromised computers to the information security office, which affected the capability to ensure that sensitive or protected data was not compromised and affected their capability to analyze the events to identify security issues that may have been systemic or which may have required additional training.

Recent changes in computer technology allow servers to be consolidated into one or more physical servers that operate as multiple virtual servers. Other changes allow those servers to continue to be administered in a decentralized manner by various departments, while reducing the need for highly skilled technical system administration personnel. Fewer physical devices reduce the effort required to ensure that these servers are adequately patched and secured.

Campus management stated that the current decentralized model used at some campuses originated from a need by the college to have local access and local support, but that recent changes in server technology, network capacity and routing, operating system software, and CSU initiatives have eliminated much of the need for a physically decentralized environment, and that similar services could be provided with logical decentralization.

Operating multiple redundant computer services departments adversely affects information security monitoring and compliance efforts, adds unnecessary cost and redundancy, increases risk, and adds unneeded complexity to future and existing CSU technology initiatives.

Recommendation 4

We recommend that the CO:

- a. Conduct a study to determine the most effective way to consolidate the physical computing environments to improve information security controls, reduce redundancy, and simplify the overall complexity of the facilities environments.
- b. Based on the results of the study, instruct the campuses to document plans to simplify information security.
- c. Ensure that the campus information security offices have the means and methodology to enable coordination of decentralized desktop support and provide consistent reporting of all desktop security incidents. One approach would be to use a common help desk reporting system for the entire campus that generates work tickets to the decentralized college and departmental support staff.

Management Response

We concur.

The CO will conduct a study of decentralized computing environments to identify strategies to improve information security controls, reduce redundancies, and simplify operations. Based on the results of the study, the campuses will be directed to document strategic plans to improve information security in their decentralized computing environments.

The CO will work collaboratively with campus information security officers to ensure that desktop support procedures comply with campus and CSU information security policies and standards and desktop security incidents are appropriate reported.

Target completion date: July 1, 2011

INCIDENT RESPONSE

The incident response and resolution process was not performed with consistency and guaranteed reliability across the campuses, and relevant personnel had not consistently been trained in computer forensics.

Campus management stated that incident response was a relatively new function and that the procedures were still being developed or were being refined. They also stated that forensic analysis tools were expensive and that not all relevant personnel had been trained in forensic analysis.

Lack of a comprehensive incident response process and trained personnel could lead to incorrect or inadequate actions that could corrupt forensic data needed for proper investigation and possible litigation.

Recommendation 5

We recommend that the CO ensure that reliable and consistent incident response procedures are developed and implemented at all campuses and investigate the best approach for providing forensic training. Consideration could be given to creating a central or virtual group of trained individuals that could be deployed to investigate incidents, or the CSU could initiate a systemwide contract with a reliable and respected tech company with expert consultants, to ensure that forensic data is adequately retained and that proper repairs are performed following security incidents.

Management Response

We concur. The CO will review campus incident response procedures to ensure compliance with the CSU incident response policy, investigate the feasibility of providing forensic training, and study the feasibility of developing a virtual CSU Computer Security Incident Response Team or contracting with a company to provide forensics support.

Target completion date: July 1, 2011

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

WEB APPLICATION DEVELOPMENT AND MAINTENANCE

Website development methodologies used at the various campuses were inconsistent, often lacked key process controls, did not always provide adequate vulnerability testing, lacked software tools for code management, and were performed on each campus by multiple decentralized departments without campus guidance or oversight.

In addition, systemwide resources to address information security risks related to web development were lacking. The web development process is not routinely examined, neither are specific applications that include system interfacing controls.

It is common practice to centralize the development and communication of guidelines for web development activities. Examples include the California Department of Education Web Application Development Standards, <http://www.cde.ca.gov/re/di/ws/appdevstandards.asp>, and Harvard University Web Development Standards http://oas.harvard.edu/dev_standards/.

We found that:

- ▶ There were no consistent policies, procedures or practices for web application development, and the practices examined frequently did not include all of the management approval, project tracking, and user acceptance practices that have been routine in traditional application development guidance for decades.
- ▶ Many of the practices examined did not include key process controls such as preventing programmers from updating production source code; providing adequate software version

control, including adequate back-out recovery planning; or providing adequate peer review of code changes.

- ▶ Many of the campus web development teams did not conduct sufficient vulnerability testing and did not actively monitor emerging vulnerabilities.
- ▶ A majority of the developers had not received specific security and coding training, or did not adhere to published security best practices, such as those provided by the Open Web Application Security Project (OWASP):
http://www.owasp.org/index.php/Main_Page.
- ▶ Training was not adequate for new and ongoing staff responsible for security of applications and technical changes to applications.
- ▶ Most of the campus web development teams did not have software tools available to automate and expedite vulnerability testing, and did not use version control software to monitor, track, and protect program code.
- ▶ There were no web content or development guidelines. Web application development was often decentralized among the campus departments, and development activities were not consistently monitored for compliance with campus guidance, disability requirements, consistency with campus design, or appropriate content including advertising and linked Internet sites.

Campus management cited various reasons for inadequate application development, including lack of monetary resources, lack of sufficient training, and insufficient personnel resources.

Failure to develop an adequately controlled application development process could lead to unauthorized changes, reduce effectiveness of the control environment, cause failure to properly prioritize change requests, and produce applications that are vulnerable to compromise, which could lead to compromise of sensitive data and increase the overall security risk to the CSU, our customers, and our students.

Recommendation 6

We recommend that the campuses develop formal management controls over development practices for all departments and colleges that create web applications, and that the CO monitor this activity to ensure that each campus reaches compliance.

Specifically, we recommend that the CO:

- a. Assist the campuses to implement project and process management controls to ensure that change requests are authorized, prioritized and tracked, including approval and testing by appropriate end-user management.
- b. Ensure that process controls prevent programmers from being able to modify production code without management approval, or if staffing limitations do not permit campuses to prevent direct

modification, then detective monitoring controls be implemented to provide management oversight to the changing production environment.

- c. Create a consistent process, such as a listserve, to keep developers apprised of new application vulnerabilities as they become published. Currently, there are over 50 development teams independently trying to monitor and track new vulnerability developments.
- d. Define guidelines for acceptable web functionality and Internet associations to ensure that the CSU has consistent guidance on appropriate content including acceptable advertising and appropriateness of links to other non-CSU Internet sites.
- e. Create a forum or other collaborative method for developers to document and share effective web testing techniques and secure development methods, such as those suggested by OWASP.
- f. Evaluate a systemwide purchase agreement for web development tools to assist resource-constrained campuses in implementing effective solutions. Currently, many development teams use the product Subversion for code management.

Management Response

We concur.

The CO will review campus web development procedures to ensure campuses comply with the CSU change management policy and use preventive or detective controls to manage production code.

The CO will create a forum for web developers to disseminate information about known security issues and share effective testing techniques.

The CO will evaluate the feasibility of a systemwide purchase agreement for web development tools.

The CO will develop a guideline for hosting web pages on CSU-managed web servers.

Target completion date: July 1, 2011

WEB APPLICATION VULNERABILITY MANAGEMENT

The campuses' website development methodologies did not always provide adequate vulnerability testing and lacked software tools for vulnerability assessment.

We found that most of the campus development teams:

- ▶ Did not routinely scan existing production applications for exploitable vulnerabilities.
- ▶ Did not have software tools available to automate and expedite vulnerability testing, and often the testing criteria was not well-defined.

Campus management cited various reasons for inadequate application vulnerability management, including lack of monetary resources, lack of sufficient training, and insufficient personnel resources.

Failure to routinely monitor existing applications for new vulnerabilities could allow the integrity of those systems to degrade over time, allow evolving vulnerabilities to go undetected, and result in the compromise of protected or sensitive information.

Recommendation 7

We recommend that the campuses develop formal management controls over development practices for all departments and colleges that create web applications, and that the CO monitor this activity to ensure that each campus becomes compliant.

Specifically we recommend that the CO:

- a. Ensure that the campuses routinely scan existing production web applications for exploitable vulnerabilities.
- b. Evaluate whether a systemwide purchase agreement for web vulnerability testing tools would help to assist resource-constrained campuses in implementing effective solutions. Currently, some campus development teams use Web Inspect, and some use other tools, for vulnerability testing.
- c. Evaluate the feasibility of independent periodic testing of campus applications for vulnerabilities, possibly using a central CO security function, existing campus information security personnel, or possibly through collaboration between the campus security organizations.

Management Response

We concur.

The CO will review campuses' efforts to conduct routine scans of existing production-level web applications for exploitable vulnerabilities.

The CO will evaluate the feasibility of a systemwide purchase agreement for web-vulnerability testing tools and the feasibility of independent periodic testing of campus web applications for vulnerabilities.

Target completion date: July 1, 2011

SYSTEM SECURITY AND MONITORING

Many of the campuses lacked software tools that would enable them to proactively monitor system logs for intrusion attempts and identify vulnerable network servers and devices.

We found that:

- ▶ Almost all campuses lacked software tools for actively collecting and monitoring system logs for intrusion attempts or other access anomalies. Most campuses did not have policies or practices for logging relevant system activity, for its retention, or for routine manual monitoring.
- ▶ Many campuses either lacked comprehensive network vulnerability scanning tools or did not extend the use of those tools to the decentralized environments. Often central campus information technology (IT) departments did not have sufficient authority to ensure that vulnerable systems that they did not manage would be remediated in a timely manner.
- ▶ The CSU had suspended implementation of IT infrastructure improvements that would enable intrusion detection and prevention for campus networks.

Campus management cited various reasons for lack of automated security software tools, including lack of monetary resources, lack of sufficient training, and insufficient personnel resources.

Failure to routinely monitor system logs could allow intrusion attempts to go unnoticed until after a breach has occurred. A lack of vulnerability scanning of all campus systems allows vulnerable systems to remain unpatched on the network for extended periods, increasing the likelihood of the network being compromised. Intrusion detection and prevention software would allow the campuses to proactively monitor and react to attempts to compromised campus systems.

Recommendation 8

We recommend that the CO:

- a. Survey the campuses to determine their use of security software tools and their need for additional tools and determine whether a systemwide solution would be practical.
- b. Evaluate whether centralized vulnerability scanning of campus networks would be more effective, and whether PCI DSS compliance can be performed and certified from a central location.
- c. Complete the rollout of intrusion detection technologies. In addition, until such technologies are implemented, the CO should monitor which campuses do not have such technologies and include this outstanding risk on the reports to executive management.

Management Response

We concur.

The CO will survey the campuses to assess current usage of security monitoring tools and future needs for additional monitoring tools. The results of the survey will be used to determine whether a systemwide solution would be practical.

The CO will evaluate whether centralized vulnerability scanning of campus networks would be more effective, and whether PCI DSS compliance can be performed and certified from a central location.

The CO will continue its efforts to rollout network-monitoring tools. Campuses that do not have network-monitoring tools will be monitored until such tools have been deployed. The CSU will report on this issue to the systemwide governance committee until the project is completed.

Target completion date: July 1, 2011

PROTECTED DATA

The CSU does not have an adequate process for ensuring that protected data remains secure and is not inadvertently exposed, and does not conduct an annual assessment of protected data.

We noted that:

- ▶ Not all campuses had conducted an assessment to determine the location of protected confidential data and to remove or protect such data.
- ▶ Encryption was not consistently used to protect sensitive data that was stored on campus equipment and that was stored at off-site locations, or transmitted.
- ▶ None of the campuses has established an annual review process to ensure that such data remained protected and that additional copies or new sources of protected data were not exposed.
- ▶ The campuses had differing standards for the types of assets that were tracked by property accounting, and often computer assets under \$1,000 were not tracked. Accordingly, there was no assurance that such equipment would be properly disposed or that sensitive information would be properly wiped.

Campus management cited various reasons for not completing their assessments and stated that since this is a new process, the need for an annual review had not yet surfaced. They also stated that state policy requires tracking of physical inventory valued over \$5,000, but they had extended the policy to include items down to \$1,000 in value.

Inadequate accountability of assets, especially those containing personal confidential information or with access to such protected information, increases the risk of loss and inappropriate use of state resources and increases campus exposure to information security breaches.

Recommendation 9

We recommend that the CO:

- a. Require that each campus conduct an annual evaluation of protected data and provide an annual certification to the CO to ensure such data is adequately protected or deleted, including the use of encryption technologies.

- b. Amend the CSU's property policy to include tracking and secure disposal of all computer equipment that could contain sensitive information.

Management Response

We concur.

The CO will issue a systemwide standard directing campuses to conduct an annual review of Level 1 data as defined in the CSU Data Classification Standard. Campuses will be required to share the results of their annual review with the CO.

The CO will amend its property policy to include the tracking and secure disposal of all computer equipment that contains protected information.

Target completion date: July 1, 2011

APPENDIX A: KEY PERSONNEL CONTACTED

(A complete list of all persons contacted is included in each campus audit report)

<u>Name</u>	<u>Title</u>
<u>Office of the Chancellor</u>	
Benjamin F. Quillian	Executive Vice Chancellor and Chief Financial Officer
George Ashkar	Assistant Vice Chancellor/Controller, Financial Services
Ron Basich	Director, Corporate Information Systems
Sheila Bickham	Director, Operations Support Services
Robert Boyhan	Director of Administration
Mark Crase	Senior Director, Technology Infrastructure
Patricia Cuocco	Senior Director, Policy Planning and Advice
Michel Davidoff	Director, Cyberinfrastructure Services
Cuc Du	Information Security Officer
Richard Fletcher	Associate Director, Corporate Information Systems
Gary Geidel	Director, User Support Services
Laura Guillory	Director, User Services
Gerry Hanley	Senior Director, Academic Technology
Kristy Hawman	Associate Director, Human Resources Services
Melody Kojima	Assistant Director, Purchasing
Cheryl Kwiatkowski	Senior Director, Enterprise Information Management
Jessie Lum	Interim Senior Director, Common Management Systems and Enterprise Systems
Michael McBride	Interim Director, Software Operations and Support Services
Michael McLean	Interim Chief Information Officer and Assistant Vice Chancellor Information Technology Services (At time of review)
Lisa Moske	Director, Systemwide Electronic Information Resources
Colleen Nickles	Assistant Vice Chancellor, Financial Services (At time of review)
Tom Roberts	Director, Contracts and Procurement
Jason Solis	Associate Director, Network and Telecommunications
Berhanu Tadesse	Director, Data Center Services
Michael Trullinger	Associate Director, Identity Management
Cheryl Washington	Interim Senior Director, Information Security Management
<u>California State University, Channel Islands</u>	
Richard R. Rush	President
Herbert Aquino	Information Technology (IT) Infrastructure Manager
Michael Berman	Interim Chief Information Officer
Joanne Coville	Vice President, Administration and Finance
Emily Deakin	Controller
Neal Fisch	Director, Application Solution Group
Anna Pavin	Interim Associate Vice President, Human Resources
Judy Swanson	Manager, IT User Services

APPENDIX A: KEY PERSONNEL CONTACTED

California State University, Chico

Paul J. Zingg	President
Lorraine Hoffman	Vice President, Business and Finance
Hemlata Jhaveri	Associate Director, University Housing and Food Service
Warren Moser	Lead Automotive Mechanic, Facilities Management and Services (FMS)
Neil Nunn	Associate Director, FMS
Sandy Parsons-Ellis	Director, Disability Support Services
Marvin Pratt	Assistant Director, Environmental Health & Safety (EH&S)
Kathleen Purvis	Library Student Personnel and Building Manager, Information Resources
Eric Reichel	Chief of Police, University Police Department
Matthew Thomas	Associate Professor, Political Science Department
Michael Thorpe	Risk Manager, Business and Finance
Kenneth Sator	Director, EH&S
Joe Willis	Director, Public Affairs and Publications

California State University, Dominguez Hills

Mildred Garcia	President
Lynn Anderson	Director, Instructional Computing and Network Services
Ron Bergmann	Chief Information Officer
Jim Bersig	Director, Common Management Systems
Tim Farris	Director, Administrative Information Systems
Tina Lee	Assistant Director, Human Resources
Janie MacHarg	Director, Student Health and Psychology
Mary Ann Rodriguez	Vice President, Administration and Finance
Mark Seigle	Assistant Vice President, Human Resources
Susan Sloan	Chief of Police
Karen Wall	Associate Vice President, Administration and Finance
Sabrina Warrington	Manager, Help Desk
Emmit Williams	Director, Procurement and Contracts

California State University, East Bay

Mohammad H. Qayoumi	President
Richard Avila	Director, Server and Network Support
Shawn Bibb	Vice President, Administration and Finance/Chief Financial Officer
John Charles	Chief Information Officer
James Cimino	Associate Vice President, Human Resources
Michael Clay	Director, College Technology Service
Thomas Dixon	Director, University Police Department
Daniel Legate	Lieutenant, University Police Department
Nyassa Love	Associate Vice President, Business and Financial Services
Kent McKinney	Senior Director of Information Systems
John Sepolen	Director of Procurement and Support Services
Jeffery Smurthwaite	Director of Specialized Technology Services
Lee Thompson	Deputy Chief Information Officer/Information Security Officer

California State University, East Bay (cont.)

Thu Thu Tonnun Director, Administrative Specialized Applications,
Specialized Technology Services

California State University, Fresno

John D. Welty President
Matt Babick Internal Auditor
Richard Boes Chief Information Security Officer
John Briar Director, Campus Information Systems
Jose Diaz Dean, College of Arts and Humanities
Theresa Eurich Director, Auxiliary Operations Information Systems
Robert Harper Dean, School of Business
Joyce Harris Assistant Vice President, Health and Psychological Services
David Huerta Chief of Police
Ellen Jamra Director, Donor and Volunteer Relations
Michael Jenkins Dean, College of Engineering
Jim Michael Associate Director, Information Technology Services Systems
and Data Control

Clinton Moffit Associate Vice President, Finance and Administration
Ramakrishna Nunna Associate Dean, College of Engineering
Janice Parten Director, Human Resources
Andrew Rogerson Dean, College of Science and Math
Dirk Ruthrauff Associate Director, Health and Psychological Services
Cynthia Teniente-Matson Vice President for Administration
Rafael Villegas Information Security Officer

California State University, Fullerton

Milton A. Gordon President
Kerry Boyer Information Security Officer
Dale Coddington Security Architect
Amir Dabirian Chief Information Technology Officer and
Chief Information Security Officer (At time of review)

Willie Hagan Vice President, Administration and Finance/Chief Financial Officer
Bahram Hatefi Director of Internal Audit
Rommel Hidalgo Information Technology Projects Coordinator
Mike Marcinkevicz Director of Network Management

California State University, Long Beach

F. King Alexander President
Scott Apel Associate Vice President, Human Resources Management
Martin Brenner Director of Technology, College of the Arts
Janet Foster Associate Vice President, Information Technology Services
Don Gardner Associate Vice President of Academic Technology
Dixie Grimmet Dean, College of Health and Human Services
Craig Kleen Assistant Director of Network Services
Steve La Director of Network Services
Brian Lawver Director of Advancement Services

APPENDIX A: KEY PERSONNEL CONTACTED

California State University, Long Beach (cont.)

Robert Loesch	Director of Instructional and Research Facilities
Michael Markoski	Director of Administrative Computing Services
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
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

California State University, Los Angeles

James M. Rosser	President
Laura Carlson-Weiner	Director, Advancement Services
Bill Chang	Director, CMS and Enterprise System
Lisa Chavez	Associate Vice President, Administration and Finance (At time of review)
Tanya Ho	University Internal Auditor
Bob Hoffman	Assistant Director, Network Operations Servers and Technology Operations
Monica Jazzabi	Acting Director, Student Health Center
Thomas Leung	University Controller, Business Financial Services
Sal Membreno	Director, Office of Academic Support
Sheryl Okuno	Director of IT Security and Compliance
Peter Qhan	Vice President, Information Technology Services
George Pardon	Vice President, Administration and Finance (At time of review)
Chris Rapp	Director of IT Infrastructure
Lisa M. Sanchez	Director, Human Resources Management

California State University, Monterey Bay

Dianne F. Harrison	President
Kathryn Cruz-Urbe	Provost and Vice President for Academic Affairs
John Fitzgibbon	Associate Vice President for Finance
Gretchen Fuentes	Director, Human Resources Operations
George Lenno	Chief Information Officer
James E. Main	Vice President for Administration and Finance (At time of review)
Susan McFarlane	Director, Administrative Systems Management
Eric Simoni	Associate Director, Information Systems
Henry Simpson	Director, Technology Support Services
Chris Taylor	Director of Network Services

California State University, Northridge

Jolene Koester	President
Hilary Baker	Vice President, Information Technology and Chief Information Officer
Robert Barker	University Controller
Anne Glavin	Chief of Police
Hien Ho	Senior Director, Infrastructure Services
Kevin Krzewinski	Director, Application Development Services

APPENDIX A: KEY PERSONNEL CONTACTED

California State University, Northridge (cont.)

Howard Lutwak	Director, Internal Audit
Tom McCarron	Interim Vice President, Administration and Finance and Chief Financial Officer
Gregory Nicols	Director, Telecomm and Systems Administration
Christian Olsen	Interim Information Security Officer
Benjamin F. Quillian	Senior Director, Administration and User Support Services (At time of review)
Jill Smith	Manager, Employee Relations and Workers' Compensation
Chris Xanthos	Director, Project Management Office

California State Polytechnic University, Pomona

J. Michael Ortiz	President
Al Arboleda	Information Security Officer, Instructional and Information Technology (I&IT)
Edwin Barnes III	Vice President, Administrative Affairs and Chief Financial Officer
Debra Brum	Vice President, I&IT
Curtis Clark	Director, I&IT Web Development
Darwin Labordo	Associate Vice President, Finance and Administrative Affairs
Joe Matsumoto	Director, I&IT Systems
Kevin Morningstar	Executive Director, Student Affairs Information and Technology Service
Lisa Rotunni	Director, Academic Resources
Randy Townsend	Management Information Systems Manager, Foundation
Joice Xiong	Director of Internal Audit, Administrative Affairs
Glendy Yeh	Executive Director of Information Systems, Administrative Affairs

California State University, Sacramento

Alexander Gonzalez	President
Bridgette Bucke	Director, Data Services
Michael Christensen	Interim Associate Vice President, Risk Management Services
Stephen Garcia	Vice President of Administration and Business Affairs/ Chief Financial Officer
Larry Gilbert	Vice President and Chief Information Officer, Information Resources and Technology
Yavette Hayward	Internal Auditor, Auditing Services
Doug Jackson	Assistant Vice President, Academic Computing Resources
Ted Koubiar	Director, Operations and Systems Services
Clinton Lee	Director, Business Information Systems
Kathi McCoy	Director of Auditing Services
Meri McGraw	Information Technology Director, University Enterprises, Inc.
Gregory Porter	Director, Network and Telecommunications
Carlos Rodriguez	Director of Library Systems and Information Technology Services
David Shannon	Director of Procurement/Contract Services
David Wagner	Vice President, Human Resources
Jeff Williams	Information Security Officer

APPENDIX A: KEY PERSONNEL CONTACTED

San Diego State University

Stephen L. Weber	President
Scott Burns	Associate Vice President, Financial Operations
Kevin Carter	Director, Information Systems, Student Affairs
Valerie Carter	Director, Audit and Tax
Tony Chung	Director, Information Systems Management
John Denune	Technology Security Officer
Jahan Jamshidi	Director, Management Information Systems, Aztec Shops
Robert Newhouse	Director, University Computer Operations
Rick Nornholm	Director, Information Technology, Enrollment Services
Rich Pickett	Chief Information Officer
Mike Reeves	Director, Computing Services, San Diego State University Research Foundation
Eric Rivera	Associate Vice President, Student Affairs
John Ross	Academic Affairs Information Technology Coordinator
Sally Roush	Vice President, Business and Financial Affairs
Felecia Vlahos	Information Security Officer

San Francisco State University

Robert A. Corrigan	President
Sheldon Axler	Dean, College of Science and Engineering
Mig Hoffman	Information Security Officer
John Kim	Associate Vice President, Academic Resources
Phoebe Kwan	Director, Computing Services
Franz Lozano	University Budget Officer
Henry McCoy	Director, Academic Personnel/ Human Resources Management Systems
Leroy M. Morishita	Executive Vice President, Administration and Finance
Jon Rood	Chief Information Officer
Alastair Smith	Director, Student Health
Don Taylor	Dean, College of Health and Human Services
Jack Tse	Senior Director, Network and Operations Management
Jo Volkert	Associate Vice President, Enrollment Management
Larry Ware	Associate Vice President, Fiscal Affairs

San José State University

Jon Whitmore	President
Andre Barnes	Chief of Police, University Police Department
Adam Bayer	Director, Energy & Utilities, Facilities, Development, and Operations
Rick Casillo	Associate Director, Employee Support Services, Human Resources (HR)
Maria De Guevara	Associate Vice President, HR
Roger Elrod	Director, Student Health Center
Gloria Gutierrez	Manager of Employee Support Services, HR
Patricia Harris	Director of Media Relations, Public Affairs
Stephanie Hubbard	Associate Director, Residence Life, Housing Coordination
Josee Larochele	Director, Budget Management, University Budget Office
Rose Lee	Vice President for Administration and Finance
Mark Loftus	Associate Director of University Risk and Compliance

APPENDIX A: KEY PERSONNEL CONTACTED

San José State University (cont.)

Ninh Pham-Hi	Director of Internal Control
Frances Roth	Director, Associated Students Child Development Center
Martin Schuller	Director, Disability Resource Center

California Polytechnic State University, San Luis Obispo

Warren J. Baker	President
Sharon Anderson	Director, Administrative Computing Services
Brent Goodman	Director, Institutional Planning and Analysis
Joyce Haratani	Associate Director, Human Resource Services
Timothy Kearns	Vice Provost Information Technology/Chief Information Officer
Lawrence Kelley	Vice President, Administration and Finance
Lorlie Leatham	Director, Fiscal Services
Johanna Madjedi	Director, Communications and Computing Services
Rick Ramirez	Associate Vice President Finance
Linda Sandy	Director, Information Services Infrastructure
Craig Schultz	Director, User Support Services
Terry Vahey	Director of Technology Services, Administration and Finance/ Information Security Officer
Debra Valencia-Laver	Associate Dean, College of Liberal Arts

California State University, San Marcos

Karen S. Haynes	President
Wanda Boller	Manager, Human Resources
Linda Hawk	Vice President, Finance and Administrative Services
Jeff Henson	Analyst Programmer, Systems Development and Software Engineering
Margo Lopez	Director, System Development and Software Engineering
Teresa Macklin	Information Security Officer
Katy Rees	Director, Strategic Planning and Administrative Services
Wayne Veres	Chief Information Officer
Bill Ward	Associate Dean
Michael Yee	System Security Auditor

California State University, Sonoma

Ruben Armiñana	President
Barry Blackburn	Information Security Officer, Information Technology
Geoff Cirullo	Associate Director, Administrative Information Systems
Letitia Coate	Controller
Laurence Furukawa-Schlereth	Vice President, Administration and Finance and Chief Financial Officer
Kurt Koehle	Director, Internal Operations Analysis and Review
Richard Ludmerer	Senior Director, Risk Management
Ruth McDonnell	Director, Contracts and Procurement, Payables
Sam Scalise	Chief Information Officer
Lou Ann Seaman	Director, Administrative Information Systems
Joyce Suzuki	Managing Director, Employee Relations and Compliance Services
Jason Wenrick	Senior Director, Common Management Systems
Deanna Wilson	Managing Director, Payroll and Benefits

APPENDIX A: KEY PERSONNEL CONTACTED

California State University, Stanislaus

Hamid Shirvani	President
Mariette Araya	Common Management Systems Project Director
Frank Borrelli	Property Services Manager
Carol Castillo	Risk Manager
Brian Duggan	Director of Learning Services
Lauren Gee	Compliance Officer
Barney Gordon	Director of Client Services
Suzanne Green	Interim Vice President, Business and Finance
Charles Holmberg	Director of Information Services and Information Security Officer
David Klein	Director of Technology Services
Mary Kobayashi-Lee	Director of Human Resources
Ian Littlewood	Professor of Physics
Stacey Morgan-Foster	Vice President, Student Affairs and Privacy Officer
Kristin Olsen	Director of Public and Legislative Affairs



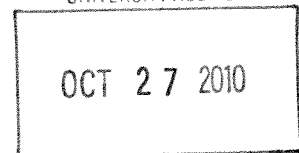
Business & Finance Division
 401 Golden Shore, 5th Floor
 Long Beach, CA 90802-4210

www.calstate.edu

Benjamin F. Quillian
 Executive Vice Chancellor/
 Chief Financial Officer

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

RECEIVED
 UNIVERSITY AUDITOR



THE CALIFORNIA STATE
 UNIVERSITY

Date: October 28, 2010

To: Larry Mandel
 University Auditor

From: Benjamin F. Quillian *B.F.Q.*
 Executive Vice Chancellor & Chief Financial Officer

Subject: Management Response to Systemwide Information Security Audit Report 08-13

Attached is the management response to Audit Report Number 08-13, Systemwide Information Security. Upon acceptance of our response, we will follow up with your office in providing supporting documentation for each recommendation by the anticipated completion dates.

Should you have any questions, please feel free to contact George V. Ashkar, Assistant Vice Chancellor, Financial Services.

BFQ:GVA:gs

Attachment

c: George V. Ashkar, Assistant Vice Chancellor, Financial Services
 Bruce Briggs, Assistant Vice Chancellor, Information Technology Services
 Cheryl Washington, Senior Director, Information Security

CSU Campuses
 Bakersfield
 Channel Islands
 Chico
 Dominguez Hills
 East Bay

Fresno
 Fullerton
 Humboldt
 Long Beach
 Los Angeles
 Maritime Academy

Monterey Bay
 Northridge
 Pomona
 Sacramento
 San Bernardino
 San Diego

San Francisco
 San José
 San Luis Obispo
 San Marcos
 Sonoma
 Stanislaus

INFORMATION SECURITY

SYSTEMWIDE

Audit Report 08-13

SYSTEMWIDE INFORMATION SECURITY

INFORMATION SECURITY GOVERNANCE

Recommendation 1

We recommend that the CO:

- a. Improve independence of the CSU ISMO by either moving the function to a more direct reporting relationship to the Chancellor, or to a department that is independent of day-to-day business operations.
- b. Create a charter for the ISMO that outlines the operational framework for the department and states the overall goals and mission.
- c. Formally delegate authority to the ISMO to monitor systemwide information security responsibilities and consider establishing the campus information security officer as a dotted-line reporting relationship.
- d. Issue the systemwide information security policy and standards, communicate the policy and standards to the campuses, and develop a process to ensure that the policy and standards are implemented by the campuses and periodically reviewed and updated to reflect the current environment.

Management Response

The CO will develop a charter for ISMO that defines the mission and objectives of the systemwide information security program, outlines operational framework for the department, delegates authority to the systemwide ISMO to review CSU information security programs, and directs the ISMO to advise and provide guidance to CSU campuses on security related issues. The CO will evaluate the reporting relationship of the ISMO to identify and mitigate potential conflicts of interest.

The CSU information security policy was approved and communicated to campuses in May 2010. Policies, standards, procedures and guidelines are communicated to the campuses through several channels including but not limited to: ICSUAM, Information Security Advisory Committee (ISAC), and the ISAC listserv.

The CSU information security policy assigns responsibility to the ISMO to conduct an annual review of the systemwide information security policy and, in accordance with the CSU information security policy, “update as necessary to reflect changes in the CSU’s academic, administrative, or technical environments, or applicable laws and regulations.”

Target Completion Date: July 1, 2011

SYSTEMWIDE INFORMATION SECURITY PROGRAM

Recommendation 2

We recommend that the CO:

- a. Develop an information security model for the CSU system and also for the individual campuses, and define the steps necessary to achieve program maturation.
- b. Examine how the CSU could best incorporate the collective resources that are available within the system and develop a platform of cooperation in which all existing CSU information security resources work together in a collaborative effort to create a world-class information security organization.
- c. Create an information security governance model that can be implemented by the individual campuses to ensure that there is consistency in management oversight, in breadth and scope of information security operations, and in assessing risk, planning, and executive reporting.
- d. Develop and implement a common standard for new and existing technologies that establishes a consistent and reliable model that can effectively address information security risks and that establishes a compliance baseline.

Management Response

The CO will develop information security models for the system-wide and individual campus programs. The models will describe steps to achieve program maturity and include strategies for governing campus information security programs.

The CSU Information Security Advisory Committee fosters collaboration among the CSU security professionals. The CO will identify other opportunities to increase collaboration among CSU information security resources.

The CO will develop a standard for new and existing technologies that effectively address information security risks.

Target Completion Date: July 1, 2011

CAMPUS INFORMATION SECURITY OVERSIGHT

Recommendation 3

We recommend that the CO:

- a. Develop and implement a monitoring process for the campus information security offices; track their significant initiatives and impediments to ascertain whether the CO could provide systemwide assistance; and provide a means for executive reporting of the systemwide information security posture.
- b. Develop and implement a centralized program to monitor legislative initiatives and disseminate the information to the campuses. Consider implementing a certification process for campus compliance with applicable laws and regulations.
- c. Ensure that the campuses have plans to comply with the systemwide information security policy; assist the campuses by creating a risk assessment and reporting model to ensure that all information security risks are being properly captured and campus executives are timely presented with risk-based priorities.

Management Response

The CO will develop and implement a process to review campus information security programs and monitor campus efforts to comply with the systemwide information security policy. The ISMO will work collaboratively with campus information security officers to track significant campus initiatives and impediments, and identify opportunities for the CO to provide systemwide assistance. The process will include executive level reporting on the CSU's information security posture.

The CO will develop a systemwide program to monitor and distribute information regarding legislative initiatives. The CO will consider implementing a certification process in the system-wide compliance program.

The CO will work collaboratively with CSU security professionals to identify (or develop, if necessary) risk management and reporting tools to ensure that information security risks are properly documented and campus executives are made aware of risk-based priorities.

Target Completion Date: July 1, 2011

DECENTRALIZED COMPUTING

CAMPUS SECURITY GOVERNANCE

Recommendation 4

We recommend that the CO:

- a. Conduct a study to determine the most effective way to consolidate the physical computing environments to improve information security controls, reduce redundancy, and simplify the overall complexity of the facilities environments.

- b. Based on the results of the study, instruct the campuses to document plans to simplify information security.
- c. Ensure that the campus information security offices have the means and methodology to enable coordination of decentralized desktop support and provide consistent reporting of all desktop security incidents. One approach would be to use a common help desk reporting system for the entire campus that generates work tickets to the decentralized college and departmental support staff.

Management Response

The CO will conduct a study of decentralized computing environments to identify strategies to improve information security controls, reduce redundancies, and simplify operations. Based on the results of the study, the campuses will be directed to document strategic plans to improve information security in their decentralized computing environments.

The CO will work collaboratively with campus information security officers to ensure that desktop support procedures comply with campus and CSU information security policies and standards and desktop security incidents are appropriately reported.

Target Completion Date: July 1, 2011

INCIDENT RESPONSE

Recommendation 5

We recommend that the CO ensure that reliable and consistent incident response procedures are developed and implemented at all campuses and investigate the best approach for providing forensic training. Consideration could be given to creating a central or virtual group of trained individuals that could be deployed to investigate incidents, or the CSU could initiate a systemwide contract with a reliable and respected tech company with expert consultants, to ensure that forensic data is adequately retained and that proper repairs are performed following security incidents.

Management Response

The CO will review campus incident response procedures to ensure compliance with the CSU incident response policy, investigate the feasibility of providing forensic training, and study the feasibility of developing a virtual CSU CSIRT team, or contracting with a company to provide forensics support.

Target Completion Date: July 1, 2011

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

WEB APPLICATION DEVELOPMENT AND MAINTENANCE

Recommendation 6

We recommend that the campuses develop formal management controls over development practices for all departments and colleges that create web applications, and that the CO monitor this activity to ensure that each campus reaches compliance.

Specifically, we recommend that the CO:

- a. Assist the campuses to implement project and process management controls to ensure that change requests are authorized, prioritized and tracked, including approval and testing by appropriate end-user management.
- b. Ensure that process controls prevent programmers from being able to modify production code without management approval, or if staffing limitations do not permit campuses to prevent direct modification, then detective monitoring controls be implemented to provide management oversight to the changing production environment.
- c. Create a consistent process, such as a listserv, to keep developers apprised of new application vulnerabilities as they become published. Currently, there are over 50 development teams independently trying to monitor and track new vulnerability developments.
- d. Define guidelines for acceptable web functionality and Internet associations to ensure that the CSU has consistent guidance on appropriate content including acceptable advertising and appropriateness of links to other non-CSU Internet sites.
- e. Create a forum or other collaborative method for developers to document and share effective web testing techniques and secure development methods, such as those suggested by OWASP.
- f. Evaluate a systemwide purchase agreement for web development tools to assist resource-constrained campuses in implementing effective solutions. Currently, many development teams use the product Subversion for code management.

Management Response

The CO will review campus web development procedures to ensure to ensure campuses comply with the CSU change management policy, and use preventive or detective controls to manage production code.

The CO will create a forum for web developers to disseminate information about known security issues and share effective testing techniques.

The CO will evaluate the feasibility of a systemwide purchase agreement for web development tools.

The CO will develop a guideline for hosting web pages on CSU managed web servers.

Target Completion Date: July 1, 2011

WEB APPLICATION VULNERABILITY MANAGEMENT

Recommendation 7

We recommend that the campuses develop formal management controls over development practices for all departments and colleges that create web applications, and that the CO monitor this activity to ensure that each campus becomes compliant.

Specifically we recommend that the CO:

- a. Ensure that the campuses routinely scan existing production web applications for exploitable vulnerabilities.
- b. Evaluate whether a systemwide purchase agreement for web vulnerability testing tools would help to assist resource-constrained campuses in implementing effective solutions. Currently, some campus development teams use Web Inspect, and some use other tools, for vulnerability testing.
- c. Evaluate the feasibility of independent periodic testing of campus applications for vulnerabilities, possibly using a central CO security function, existing campus information security personnel, or possibly through collaboration between the campus security organizations.

Management Response

The CO will review campuses efforts to conduct routine scans of existing production-level web applications for exploitable vulnerabilities.

The CO will evaluate the feasibility of a systemwide purchase agreement for web vulnerability testing tools, and the feasibility of independent periodic testing of campus web applications for vulnerabilities.

Target Completion Date: July 1, 2011

SYSTEM SECURITY AND MONITORING

Recommendation 8

We recommend that the CO:

- a. Survey the campuses to determine their use of security software tools and their need for additional tools and determine whether a systemwide solution would be practical.
- b. Evaluate whether centralized vulnerability scanning of campus networks would be more effective, and whether PCI DSS compliance can be performed and certified from a central location.
- c. Complete the rollout of intrusion detection technologies. In addition, until such technologies are implemented, the CO should monitor which campuses do not have such technologies and include this outstanding risk on the reports to executive management.

Management Response

The CO will survey the campuses to assess current usage of security monitoring tools and future needs for additional monitoring tools. The results of the survey will be used to determine whether a systemwide solution would be practical.

The CO will evaluate whether centralized vulnerability scanning of campus networks would be more effective, and whether PCI DSS compliance can be performed and certified from a central location.

The CO will continue its efforts to rollout network-monitoring tools. Campuses that do not have network-monitoring tools will be monitored until such tools have been deployed. The CSU will report on this issue to the systemwide governance committee until the project is completed.

Target Completion Date: July 1, 2011

PROTECTED DATA**Recommendation 9**

We recommend that the CO:

- a. Require that each campus conduct an annual evaluation of protected data and provide an annual certification to the CO to ensure such data is adequately protected or deleted, including the use of encryption technologies.
- b. Amend the CSU's property policy to include tracking and secure disposal of all computer equipment that could contain sensitive information.

Management Response

The CO will issue a systemwide standard directing campuses to conduct an annual review of "Level 1" data as defined in the CSU Data Classification Standard. Campuses will be required to share the results of their annual review with the CO.

The CO will amend its property policy to include the tracking and secure disposal of all computer equipment that contains protected information.

Target Completion Date: July 1, 2011



THE CALIFORNIA STATE UNIVERSITY

 OFFICE OF THE CHANCELLOR

BAKERSFIELD

CHANNEL ISLANDS

November 24, 2010

CHICO

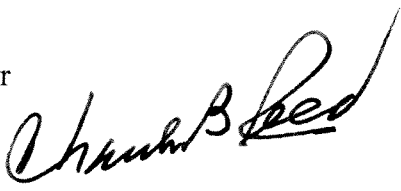
MEMORANDUM

DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed 
Chancellor

FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 08-13 on *Information Security*, Systemwide

LONG BEACH

LOS ANGELES

In response to your memorandum of November 24, 2010, I accept the response as submitted with the draft final report on *Information Security*, Systemwide.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS