

INFORMATION SECURITY
CALIFORNIA STATE UNIVERSITY,
EAST BAY

Audit Report 09-34
January 13, 2010

Members, Committee on Audit

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

Staff

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

BOARD OF TRUSTEES
THE CALIFORNIA STATE UNIVERSITY

CONTENTS

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

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

Security Governance	8
Record Retention.....	8
Employee Separation	8
Decentralized Computing	9
Server Environments.....	9
Technical Vulnerabilities	10
System Development and Change Management	11
Systems Security and Monitoring	12
Control Over User Access.....	12
Network Architecture.....	13
Operating Systems Vulnerabilities.....	13
Password Standards.....	14
Protected Data.....	15
Lost/Stolen Computers.....	15
Disposition of Protected Data	15
Assessment and Inventory of Protected Information	16

APPENDICES

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

ABBREVIATIONS

CMS	Common Management Systems
COS	College of Science
CSU	California State University
DMZ	Demilitarized Zone
DNS	Domain Naming Service
HTTP	Hypertext Protocol
IEC	International Electrotechnical Commission
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
ITS	Information Technology Services
MCS	Mathematics and Computer Science
SQL	Structure Query Language
UPD	University Police Department

EXECUTIVE SUMMARY

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

We visited the California State University, East Bay campus from March 16, 2009, through June 5, 2009, and audited the procedures in effect at that time.

Our study and evaluation identified issues that, if left unattended, could impact the overall control environment. We identified some problems that were listed individually in this report; however, the underlying cause of many of the problems identified was related to the prior (decentralized) structure of campus information technology at the time of the audit, which the campus was in the process of centralizing to enhance controls.

In our opinion, the operational and administrative controls of information security in effect as of June 5, 2009, taken as a whole, were sufficient to meet many of the objectives for a secured computing environment. The overall campus information technology department control environment was satisfactory and provided appropriate safeguards over the critical financial and student systems.

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

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

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

SECURITY GOVERNANCE [8]

The campus had not established a process to ensure appropriate and timely disposal of records/information. The campus did not remind separating employees of their ongoing legal responsibility for maintaining the security of protected data.

DECENTRALIZED COMPUTING [9]

Administration of decentralized departmental server environments required improvement. Technical vulnerabilities existed on a variety of decentralized systems.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT [11]

The campus' web application development process and practices required improvement.

SYSTEM SECURITY AND MONITORING [12]

The campus had not established a process to ensure that periodic management reviews are performed of user access/profiles for several applications that contained confidential data outside of the Common Management Systems. Internet-accessible devices were located within the same segments of the campus' network architecture as internal resources. Technical vulnerabilities existed on selected systems. The campus password practices required improvement.

PROTECTED DATA [15]

Campus reporting and investigation of protected data that might exist on lost/stolen computers was inadequate. The campus could not provide evidence documenting the deletion of protected data from campus computers. The campus had not completed a campus-wide assessment to identify sensitive data on all servers and workstations.

INTRODUCTION

BACKGROUND

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

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

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

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

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

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

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

At California State University, East Bay, the office of information technology services has overall responsibility for the management of campus systems, networks and the decentralized computing environment, with the exception of the College of Science and the mathematics computer science department.

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 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 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 California State University, East Bay campus. Specifically, this configuration testing included assessment of the following technologies:

- ▶ Selected operating system platforms.
- ▶ Border firewall settings.
- ▶ Selected routing and switching devices.
- ▶ Internet footprint analysis.
- ▶ Website vulnerability assessment.

Our study and evaluation were conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors, and included the audit tests we considered necessary in determining that operational and administrative controls are in place and operative. This review emphasized, but was not limited to, compliance with state and federal laws, Board of Trustee policies, and Office of the Chancellor and campus policies, letters, and directives. The audit review focused on procedures currently in effect.

We focused primarily upon the internal administrative, compliance, and operational/technical controls over the management of information security. Specifically, we reviewed and tested:

- ▶ Information security policies and procedures.
- ▶ Information security organizational structure and management framework.
- ▶ Information asset management accountability and classification.
- ▶ Human resources security responsibilities.

- ▶ Administrative and technical security procedures, information processing, and service delivery.
- ▶ Access controls over networks, systems, applications, business processes, and data.
- ▶ Incident response, escalation, and reporting procedures.
- ▶ Compliance with relevant statutory, regulatory, and contractual security requirements.
- ▶ Web application security and applicable change management procedures.
- ▶ E-mail systems management and configuration.
- ▶ Operational security of selected operating system platforms.
- ▶ Security configurations of border firewall settings.
- ▶ Security configurations of selected routing and switching devices.
- ▶ Internet footprints of systems connected to the Internet.
- ▶ Website vulnerabilities stemming from exposures in the server's operating system, server administration practices, or flaws in the web applications programming.

Our testing and methodology was designed to provide a managerial level review of key information security practices, which included detailed testing of a limited number of network and computing devices. Our review did not examine all aspects of information security, selected emerging technologies were excluded from the scope of the review, and our testing approach was designed to provide a view of the security technologies used to protect only key computing resources.

OBSERVATIONS, RECOMMENDATIONS, AND CAMPUS RESPONSES

SECURITY GOVERNANCE

RECORD RETENTION

The campus had not established a process to ensure appropriate and timely disposal of records/information.

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

The vice president of administration and finance/chief financial officer stated that the campus-designated record custodians are responsible for addressing record retention requirements and meeting compliance with systemwide policy. He also stated that a designated campus lead or committee had not been appointed to provide oversight of the campus' record retention practices.

Failure to ensure appropriate and timely disposal of records/information in accordance with legal requirements may result in non-compliance with state and federal laws and regulations and may result in operational inefficiencies and inconsistent record retention practices across the California State University.

Recommendation 1

We recommend that the campus establish a process to ensure appropriate and timely disposal of records/information.

Campus Response

We will establish, by division, the responsible person to create a schedule for appropriate and timely disposal for records/information. Those individuals will be responsible for ensuring the schedules are met. We will complete this by May 1, 2010.

EMPLOYEE SEPARATION

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

The associate vice president of human resources stated that the human resources department was unaware that a security communication reminder was required in the employee separation process.

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

Recommendation 2

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

Campus Response

We concur. We will modify our exit process to include a reminder of the ongoing legal responsibility for maintaining the security of protected data. We will complete this by May 1, 2010.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Administration of decentralized departmental server environments required improvement.

Our review of the decentralized Mathematics and Computer Science (MCS) department and the College of Science (COS) disclosed that:

- ▶ Both departments had not completed a formal assessment to identify and classify confidential information within their decentralized environments.
- ▶ Both departments had not documented an encryption policy or procedures for the storage of confidential information.
- ▶ The periodic review of security or event logs was not documented.
- ▶ Policies and procedures had not been developed to address change management, patch management, password security, hardening standards, or the approval of accounts with privileged access.
- ▶ The MCS department supported a domain naming service (DNS) server that is externally accessible, which had no established minimum baseline security standards.
- ▶ The MCS department had four faculty members manage their own servers, which were not monitored to ensure adequate patch management, antivirus updates, and minimum security standards.

The deputy chief information officer/information security officer stated that information technology services (ITS) was in the process of consolidating decentralized servers, which included the MCS and COS departments.

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

Recommendation 3

We recommend that the campus implement procedures to ensure that decentralized departments:

- a. Identify confidential/sensitive data and assign data classifications to all such data.
- b. Develop and document an encryption policy and procedures for the storage of confidential information.
- c. Develop procedures and checklists to ensure the performance and documentation of security reviews and the creation of event logs.
- d. Develop policies and procedures to address change management, patch management, password security, minimum server security standards, and privileged account provisioning.
- e. Develop and apply minimum server security standards to ensure the DNS server has a proper security posture and place the DNS server on a separate network segment from the campus internal network.
- f. Prohibit faculty from managing their own servers and transition management of servers to ITS.

Campus Response

We concur. The campus is now applying the central IT department's server administration procedures to servers within decentralized departments. Note also that the campus does not expect to have decentralized servers beyond April 2010.

TECHNICAL VULNERABILITIES

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

Our external testing of selected servers disclosed 11 vulnerabilities on a variety of servers. We provided specific details of these vulnerabilities to the campus.

Additionally, the campus did not always adequately manage deployment of servers in the decentralized computing environment, nor did it provide professional standards and guidance related to such deployment. The decentralized servers were not routinely patched, there was no baseline standard for server or application security, and professional application development standards and methodologies were absent or inadequate.

The senior network security analyst stated that the lack of centralized IT oversight and direction had permitted the majority of these vulnerabilities to propagate in the decentralized computing environments.

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

Recommendation 4

We recommend that the campus:

- a. Repair all of the technical vulnerabilities that were identified and presented in detail.
- b. Formalize a security baseline standard that requires the review for security vulnerabilities prior to deployment.

Campus Response

We concur. The campus has repaired the technical vulnerabilities identified in the audit. Additionally, the campus is now applying the central IT department's system security standards to decentralized systems. Note also that the campus does not expect to have decentralized systems beyond April 2010.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

The campus' web application development process and practices required improvement.

Our review of web application development disclosed that:

- ▶ Formal change management procedures were not followed.
- ▶ Programmers had unlimited access to the source code in the production environment and were also responsible for moving their own changes to production.
- ▶ Security reviews had not been established for web application development to address potential vulnerabilities.
- ▶ There was no version control over source code.

The deputy chief information officer/information security officer stated that the creation of a campus web application development process was not part of the change advisory board process.

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

Recommendation 5

We recommend that the campus:

- a. Implement change management procedures to ensure web development occurs in accordance with management guidance.
- b. Develop a security standard that requires the review of web applications for common security vulnerabilities prior to deployment.

Campus Response

We concur. The campus has extended the central IT department's change management procedures to the web development function. Additionally, the campus is now applying the central IT department's application systems security standard to the web development function, requiring web applications to be reviewed for common security vulnerabilities prior to deployment.

SYSTEMS SECURITY AND MONITORING

CONTROL OVER USER ACCESS

The campus had not established a process to ensure that periodic management reviews are performed of user access/profiles for several applications that contained confidential data outside of the Common Management Systems (CMS).

The deputy chief information officer/information security officer stated that the campus began its review with the systems that had the highest use and risk (the PeopleSoft system) and that a periodic review process is being expanded for non-PeopleSoft systems.

Failure to periodically review user access increases the risk of inappropriate access.

Recommendation 6

We recommend that the campus establish a process to ensure periodic management reviews are performed of user access to non-PeopleSoft systems containing protected data on at least an annual basis.

Campus Response

We concur. The campus is now applying its CMS-designed annual user access review process to non-CMS systems that contain protected data.

NETWORK ARCHITECTURE

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

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

The deputy chief information officer/information security officer stated that the campus had taken a policy-based approach that is covered in the campus acceptable use policy. In addition, the deputy chief information officer/information security officer and senior network security analyst both stated that the campus internal network had not been properly segregated due to resource constraints.

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

Recommendation 7

We recommend that the campus separate Internet-accessible devices from other devices within the internal network.

Campus Response

We concur. With the recent installation of new firewall equipment (made possible by the CSU's ITRP2 program), the campus now has the technical resources necessary for implementation of this massive network architectural change. The campus is currently two months into this fourteen-month network segmentation initiative. Expected completion date is May 2011.

OPERATING SYSTEMS VULNERABILITIES

Technical vulnerabilities existed on selected systems.

Our testing of selected servers disclosed various vulnerabilities for which specific details were provided to the campus. One server was running a vulnerable version of Microsoft structured query language (SQL) database, another server was running a vulnerable version of Apache web server, and two servers were running vulnerable versions of remote desktop protocol. Finally, one web server supported hypertext protocol (HTTP) trace and track methods that increase the risk of cross-site scripting attacks.

The senior network security analyst stated that delays in patching servers and delayed vendor supported patches and updates created these vulnerabilities.

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

Recommendation 8

We recommend that the campus:

- a. Repair all the technical vulnerabilities that were identified and presented in detail.
- b. Formalize the security baseline standard that requires the review of servers for security vulnerabilities prior to deployment.

Campus Response

We concur. The campus has repaired the technical vulnerabilities identified in the audit. Additionally, the campus is now applying its central IT department's operating systems security standard to all servers – a standard that requires server operating systems to be reviewed for common security vulnerabilities prior to deployment.

PASSWORD STANDARDS

The campus password practices required improvement.

We noted that:

- ▶ The campus did not have an adequate password policy that it extended to, and enforced for, all departments and/or applications on campus.
- ▶ The campus had an informal and undocumented process for passwords related to certain administrator accounts that control core network services.
- ▶ Password settings for the two primary authentication services were not consistent and did not meet best practice minimum guidelines.
- ▶ One production server and one web server had user accounts with non-expiring passwords.

The deputy chief information officer/information security officer stated his belief that the current campus password policy was sufficient.

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

Recommendation 9

We recommend the campus establish and implement an adequate password policy and ensure that all departments comply with that policy.

Campus Response

We concur. The campus will strengthen its password policy and apply it to all departments and systems. Expected completion date is April 2010.

PROTECTED DATA

LOST/STOLEN COMPUTERS

Campus reporting and investigation of protected data that might exist on lost/stolen computers was inadequate.

We noted several instances where lost/stolen computers were not reported to the information security office.

The lieutenant of the university police department (UPD) stated that UPD was not aware of the campus process for reporting lost computers and therefore did not inform the information security officer.

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

Recommendation 10

We recommend that the campus develop a procedure to report lost/stolen computers that may contain protected data to the information security office.

Campus Response

We concur. We will establish the new procedure by May 1, 2010.

DISPOSITION OF PROTECTED DATA

The campus could not provide evidence documenting the deletion of protected data from campus computers.

The senior network security analyst stated that hard drives are not wiped by the user support services department because the practice of wiping these drives was too time-consuming.

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

Recommendation 11

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

Campus Response

We concur. The campus has established and implemented procedures to ensure that hard-drive wiping is performed and documented.

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

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

The deputy chief information officer/information security officer stated that ITS is still in the process of identifying and analyzing systems and workstations that may contain sensitive/confidential information.

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

Recommendation 12

We recommend that the campus complete a campus-wide assessment to identify sensitive data on all servers and workstations.

Campus Response

We concur. The campus has completed an assessment of its servers to identify sensitive data contained on them. Additionally, the campus will investigate options, costs, and reasonableness/materiality thresholds for scanning the thousands of university desktop and laptop computers and workstations for sensitive data. Expected completion date for this analysis is May 2010.

APPENDIX A: PERSONNEL CONTACTED

<u>Name</u>	<u>Title</u>
Mohammad H. Qayoumi	President
Richard Ainslie	Network Analyst
Richard Avila	Director, Server and Network Support
Shawn Bibb	Vice President, Administration and Finance/Chief Financial Officer
John Charles	Chief Information Officer
Amit Chatterjee	Web Application Administrator/Webmaster
James Cimino	Associate Vice President, Human Resources
Michael Clay	Director, College Technology Service
Jann Davis	Director, University Police Department
Thomas Dixon	Senior Network Security Analyst
James C. Hodges	Lieutenant, University Police Department
Cathey Hurtt	Web Services Team Lead
Daniel Legate	Analyst/Programmer
Nyassa Love	Associate Vice President, Business and Financial Services
Kent McKinney	Senior Director of Information Systems
Rita Peth	Director of Procurement and Support Services
John Sepolen	Coordinator, Special Project/Security
Jeffery Smurthwaite	Director of Specialized Technology Services
Lee Thompson	Deputy Chief Information Officer/Information Security Officer
Thu Thu Tonnu	Director, Administrative Specialized Applications, Specialized Technology Services
Richard Uhler	College Information Technology Consultant, Mathematics and Computer Science Department



CALIFORNIA STATE
UNIVERSITY
E A S T B A Y

Office of the Vice President, Administration
and Finance & Chief Financial Officer

CALIFORNIA STATE UNIVERSITY, EAST BAY
25800 Carlos Bee Boulevard, Hayward, CA 94542-3002
510.885.3803 • 510.885.4745 (fax) • www.csueastbay.edu

March 3, 2010

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

**RE: Campus Responses to Recommendations: Audit Report Number 09-34
Information Security, California State University, East Bay**

Dear Mr. Mandel, *Larry*

Enclosed is our response to the recommendations in Audit Report Number 09-34,
Information Security Audit, at California State University, East Bay.

Upon acceptance of our response, we will follow up with your office, providing
supporting documentation for each recommendation.

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

Sincerely,

A handwritten signature in cursive script that reads "Shawn".

Shawn Bibb
Vice President, Administration & Finance, CFO

SB/ad

c: Mohammad H. Qayoumi, President
John Charles, CIO

California State University, East Bay
Information Security
Audit Report Number 09-34

SECURITY GOVERNANCE

RECORD RETENTION

Recommendation 1

We recommend that the campus establish a process to ensure appropriate and timely disposal of records/information.

Campus Response

We will establish, by Division, the responsible person to create a schedule for appropriate and timely disposal for records/information. Those individuals will be responsible for ensuring the schedules are met. We will complete this by May 1, 2010.

EMPLOYEE SEPARATION

Recommendation 2

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

Campus Response

We concur.

We will modify our exit process to include a reminder of the ongoing legal responsibility for maintaining the security of protected data. We will complete this by May 1, 2010.

DECENTRALIZED COMPUTING

SERVER ENVIRONMENTS

Recommendation 3

We recommend that the campus implement procedures to ensure that decentralized departments:

- a. Identify confidential/sensitive data and assign data classifications to all such data.
- b. Develop and document an encryption policy and procedures for the storage of confidential information.

- c. Develop procedures and checklists to ensure the performance and documentation of security reviews and the creation of event logs.
- d. Develop policies and procedures to address change management, patch management, password security, minimum server security standards, and privileged account provisioning.
- e. Develop and apply minimum server security standards to ensure the DNS server has a proper security posture and place the DNS server on a separate network segment from the campus internal network.
- f. Prohibit faculty from managing their own servers and transition management of servers to ITS.

Campus Response

We concur.

The campus is now applying the central IT department's server administration procedures to servers within decentralized departments. Note also that the campus does not expect to have decentralized servers beyond April 2010.

TECHNICAL VULNERABILITIES

Recommendation 4

We recommend that the campus:

- a. Repair all of the technical vulnerabilities that were identified and presented in detail.
- b. Formalize a security baseline standard that requires the review for security vulnerabilities prior to deployment.

Campus Response

We concur.

The campus has repaired the technical vulnerabilities identified in the audit. Additionally, the campus is now applying the central IT department's system security standards to decentralized systems. Note also that the campus does not expect to have decentralized systems beyond April 2010.

SYSTEM DEVELOPMENT AND CHANGE MANAGEMENT

Recommendation 5

We recommend that the campus:

- a. Implement change management procedures to ensure web development occurs in accordance with management guidance.

- b. Develop a security standard that requires the review of web applications for common security vulnerabilities prior to deployment.

Campus Response

We concur.

The campus has extended the central IT department's change management procedures to the web development function. Additionally, the campus is now applying the central IT department's application systems security standard to the web development function – requiring web applications to be reviewed for common security vulnerabilities prior to deployment.

SYSTEMS SECURITY AND MONITORING

CONTROL OVER USER ACCESS

Recommendation 6

We recommend that the campus establish a process to ensure periodic management reviews are performed of user access to non-PeopleSoft systems containing protected data on at least an annual basis.

Campus Response

We concur.

The campus is now applying its CMS-designed annual user access review process to non-CMS systems that contain protected data.

NETWORK ARCHITECTURE

Recommendation 7

We recommend that the campus separate Internet-accessible devices from other devices within the internal network.

Campus Response

We concur.

With the recent installation of new firewall equipment (made possible by the CSU's ITRP2 program), the campus now has the technical resources necessary for implementation of this massive network architectural change. The campus is currently two months into this fourteen month network segmentation initiative. Expected completion date is May, 2011.

OPERATING SYSTEMS VULNERABILITIES

Recommendation 8

We recommend that the campus:

- a. Repair all the technical vulnerabilities that were identified and presented in detail.
- b. Formalize the security baseline standard that requires the review of servers for security vulnerabilities prior to deployment.

Campus Response

We concur.

The campus has repaired the technical vulnerabilities identified in the audit. Additionally, the campus is now applying its central IT department's operating systems security standard to all servers – a standard that requires server operating systems to be reviewed for common security vulnerabilities prior to deployment.

PASSWORD STANDARDS

Recommendation 9

We recommend the campus establish and implement an adequate password policy and ensure that all departments comply with that policy.

Campus Response

We concur.

The campus will strengthen its password policy and apply it to all departments and systems. Expected completion date is April 2010.

PROTECTED DATA

LOST/STOLEN COMPUTERS

Recommendation 10

We recommend that the campus develop a procedure to report lost/stolen computers that may contain protected data to the information security office.

We concur. We will establish the new procedure by May 1, 2010.

DISPOSITION OF PROTECTED DATA

Recommendation 11

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

Campus Response

We concur.

The campus has established and implemented procedures to ensure that hard-drive wiping is performed and documented.

ASSESSMENT AND INVENTORY OF PROTECTED INFORMATION

Recommendation 12

We recommend that the campus complete a campus-wide assessment to identify sensitive data on all servers and workstations.

Campus Response

We concur.

The campus has completed an assessment of its servers to identify sensitive data contained on them. Additionally, the campus will investigate options, costs, and reasonableness/materiality thresholds for scanning the thousands of university desktop and laptop computers and workstations for sensitive data. Expected completion date for this analysis is May 2010.

THE CALIFORNIA STATE UNIVERSITY
OFFICE OF THE CHANCELLOR



BAKERSFIELD

March 29, 2010

CHANNEL ISLANDS

CHICO

MEMORANDUM

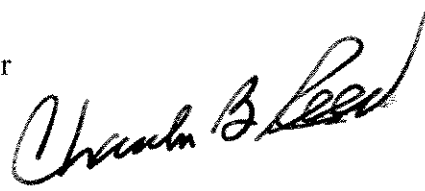
DOMINGUEZ HILLS

EAST BAY

TO: Mr. Larry Mandel
University Auditor

FRESNO

FROM: Charles B. Reed
Chancellor



FULLERTON

HUMBOLDT

SUBJECT: Draft Final Report 09-34 on *Information Security*,
California State University, East Bay

LONG BEACH

LOS ANGELES

In response to your memorandum of March 29, 2010, I accept the response as submitted with the draft final report on *Information Security*, California State University, East Bay.

MARITIME ACADEMY

MONTEREY BAY

NORTHRIDGE

CBR/amd

POMONA

SACRAMENTO

SAN BERNARDINO

SAN DIEGO

SAN FRANCISCO

SAN JOSÉ

SAN LUIS OBISPO

SAN MARCOS

SONOMA

STANISLAUS