The Commonwealth of Massachusetts
AUDITOR OF THE COMMONWEALTH
ONE ASHBURTON PLACE, ROOM 1819
BOSTON, MASSACHUSETTS 02108
TEL. (617) 727-6200

A. JOSEPH DeNUCCI
AUDITOR

No. 2008-0186-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AND CERTAIN ACTIVITIES AT WORCESTER STATE COLLEGE

July 1, 2006 through November 13, 2008

OFFICIAL AUDIT REPORT

FEBRUARY 10, 2009

TABLE OF CONTENTS

INTRODUCTION

Worcester State College (WSC), which was established in 1847, is a Massachusetts institution of higher education offering undergraduate and graduate degree programs in the liberal arts and sciences, teacher education, biomedical sciences, business, and the health professions. Chapter 15A, Section 5, of the Massachusetts General Laws created the Massachusetts State College System of which WSC is a member. On March 7, 2003, WSC received its ten-year accreditation from the New England Association of Schools and Colleges.

The College's mission is to affirm the principles of liberal learning as the foundation for all advanced programs of study. WSC is located on 58 acres on the outskirts of New England's third-largest city and consists of nine major complexes identified as the Administration Building, Sullivan Academic Center, Learning Resource Center, Ghosh Center for Science and Technology, Gymnasium, Student Center, Wasylean Hall, Dowden Hall, and Chandler Village. At the time of our audit, WSC had a combined student population of 5,358 full-time and part-time students with an associated full time-equivalency total of 4,083. At that time, the College employed 1,120 full-time and part-time faculty, administrators, and staff members and was supported by a fiscal year 2009 budget of approximately $70 million.

WSC is governed by a Board of Trustees and is administered under the direction of the College's President. Additional oversight is provided to WSC by the Board of Higher Education, established under Massachusetts General Laws Chapter 15A, Section 1, which is responsible for monitoring each Massachusetts higher educational institution to ensure that state funds support measurable performance, productivity, and results.

The College's academic and administrative functions are supported by computer services provided by WSC's Information Technologies (IT) Department. The IT Department's primary responsibility is to support the College in achieving its mission and strategic goals and objectives by ensuring the availability and support of hardware, software, network, and communication resources. The IT Department provides management services and support for the following constituencies: students, faculty, staff, consortium/commonwealth partners, and the greater Worcester community, including private sector businesses. The IT Department, in consultation with its constituencies, evaluates emerging trends and technologies and assesses the potential legal, security, and operational impact of changes in technology on the College. The IT Department provides assistance and guidance to administrative staff, faculty, librarians, and students regarding the use of IT resources, Internet portal support, computer equipment maintenance, web hosting services, e-mail, and website access.

The IT Department is comprised of four groups: Infrastructure Network, Administrative Services, End User Support Services, and Multimedia. At the time of our audit, the IT Department consisted of 27-full time staff members headed by a Chief Information Officer (CIO) who reports directly to WSC's President. Each of the four groups is under the direction of a director/manager who reports to the CIO.

Computer operations were supported by 76 file servers located in the data center and 1,469 workstations and thin client terminals configured to gain access to IT capabilities through the College's local area network (LAN). In addition, WSC maintained 216 laptop computers that were distributed to departments throughout the College for use by faculty, staff, and administrators. Of the 1,469 workstations, 1,065 were assigned to administrative staff and faculty and 404 were assigned to 30 computer laboratories and classrooms. WSC's file servers were connected through a wide area network (WAN) to the Commonwealth's Information Technology Division's (ITD) mainframe providing access to the Web-based Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

From an administrative perspective, the College uses Colleague, its mission-critical application, to process WSC's financial management, administrative, and student information activities. The Colleague application, developed by Datatel, Inc., encompasses all campus business areas and their respective functions, including student admissions, enrollment, and grading as well as financial accounting, payroll, financial aid, and institutional research.

.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an information technology (IT) general controls examination of IT-related activities at Worcester State College (WSC). The audit, which was conducted from February 6, 2008 through November 13, 2008, covered the period of July 1, 2006 through November 13, 2008. Our audit scope included an examination of IT-related general controls pertaining to IT organization and management, physical security, environmental protection, system access security, inventory control over IT equipment, disaster recovery and business continuity planning, on-site and off-site storage of backup copies of magnetic media, and IT contract management. In addition, our scope included a review of the College's control practices regarding background checks for certain individuals hired or promoted, or staff or students, having contact with children. We also examined WSC's efforts to comply with Payment Card Industry (PCI) security standards and reviewed controls over Personally Identifiable Information (PII).

Audit Objectives

Our primary audit objective was to determine whether the College's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that control objectives would be achieved to support WSC's business functions. The audit included an assessment of the adequacy and effectiveness of controls in place to protect the integrity and confidentiality of data and financial-related information contained within Colleague.

Our audit objective regarding IT organization and management was to determine whether IT-related roles and responsibilities for IT staff were clearly defined, points of accountability were established, appropriate organizational controls were in place and in effect, and whether IT-related policies and procedures adequately addressed the areas under our review. We sought to determine whether WSC had an IT strategic planning process in place from which IT strategic and tactical plans would be developed to help direct the use of technology to fulfill the College's mission and goals. We also sought to determine whether adequate physical security controls were in place and in effect to restrict access of IT resources to only authorized users in order to prevent damage or loss of IT-related assets. We sought to determine whether sufficient environmental protection controls were in place and in effect to prevent and detect damage or loss of computer equipment and data residing on the systems.

Our objective regarding system access security was to determine whether adequate controls were in effect to provide reasonable assurance that only authorized users were granted access to WSC's application

systems and data files, and whether WSC was actively monitoring password administration. We also sought to determine whether Colleague system data was sufficiently protected against unauthorized disclosure, modification, or deletion.

Our evaluation of inventory control over computer equipment was to determine whether adequate control practices were in place and in effect to account for computer equipment, including laptop computers. In addition, we sought to determine whether an annual physical inventory and reconciliation was conducted, and whether the College met Chapter 647 reporting requirements regarding lost or stolen computer equipment.

With respect to the availability of computing capabilities, we sought to determine whether disaster recovery and business continuity strategies would provide reasonable assurance that mission-critical and essential IT capabilities could be regained within an acceptable period of time should IT resources be rendered inoperable or inaccessible. In addition, we sought to determine whether WSC had adequate control procedures for the generation and storage of on-site and off-site backup copies of magnetic media to support system and data recovery objectives.

We sought to determine whether contractual relationships with third-party IT-related service providers were covered by written contracts that were properly signed and dated, and sufficiently detailed the services or deliverables to be provided. We also sought to determine whether third-party contracts contained standard terms and conditions as promulgated by the Operational Services Division and whether incorporated vendors were registered with the Office of the Secretary of State. We sought to determine whether WSC had implemented adequate IT contract management controls to provide reasonable assurance that contract monitoring and evaluation were being performed.

Our audit sought to determine whether the College's procedures were adequate for performing background checks on individuals hired or promoted to positions performing sensitive functions or on individuals accepted into specific academic programs that involve contact with children.

We sought to determine whether WSC was in compliance with Payment Card Industry (PCI) data security standards regarding security of credit card information. We sought to determine whether the College was in compliance with data security standards regarding payment card and transaction data that must be protected. The protection applied to data that is stored, processed, or transmitted through any network component, server, or application that is included in, or connected to, the cardholder data environment.

We also sought to evaluate whether there were adequate controls in place to protect Personally Identifiable Information (PII) and to determine whether the College's control policies and procedures were adequate to comply with the Commonwealth's data breach notification requirements.

Audit Methodology

To determine the scope of the audit, we performed pre-audit survey work regarding WSC's overall mission and IT environment. The pre-audit work included interviews with senior management; a review of policies, procedures, and other internal control documentation; and observation of IT-related areas. To obtain an understanding of WSC's activities and internal control environment, we reviewed the College's mission and primary business functions. We assessed the strengths and weaknesses of the internal control system for selected IT activities, including physical security, environmental protection, system access security, inventory control over computer equipment, business continuity planning, and on-site and off-site storage of backup copies of magnetic media. We also reviewed control practices concerning the College's compliance with PCI standards, PII standards, and CORI background checks. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the organizational structure of WSC's IT Department. For the areas under our review, we determined whether policies and procedures were in place, and in effect, and were documented, reviewed, approved, and communicated to appropriate staff. We reviewed the College's strategic and tactical plans to determine whether WSC's IT activities and functions were properly guided with respect to IT direction and technology. To determine whether WSC's IT-related job descriptions and job specifications were up-to-date, we obtained a current list of the personnel employed by the IT Department, and compared the list to the IT Department's organizational chart. To determine whether job functions reflected current responsibilities, we interviewed IT staff to identify their day-to-day duties. In addition, we reviewed and performed selected preliminary audit tests relevant to documents such as the network configuration, internal control plan, and business continuity plan.

To evaluate physical security, we identified locations housing computer equipment and conducted preliminary walkthroughs of the areas. We reviewed whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to selected facilities housing IT resources and whether authorized personnel were instructed in physical security policies and procedures. Moreover, our review included the completion of a risk analysis questionnaire and interviews with WSC's management who are responsible for physical security for IT computer equipment. We also assessed WSC's physical security to determine the extent to which physical access was restricted for areas housing IT computer equipment by conducting a walkthrough of the data center, selected classroom labs, business offices, on-site and off-site storage areas, and telecommunication closets. We examined the existence of controls, such as locking devices, motion detectors, and intrusion alarms. To gain an understanding of

procedures regarding key management at WSC, we interviewed the individuals responsible for maintaining records of administrators, faculty, and staff who were issued master and sub-master key sets for locks located at various locations throughout the campus. We also reviewed WSC's use of OneCard, which functions as an official college identification card and can be used to allow door access and perform a number of campus-related financial transactions. Furthermore, we obtained listings of key and OneCard holders and compared them to the College's up-to-date employment listing to verify that all were current employees of the College.

To determine whether adequate environmental controls were in place and in effect to properly safeguard computing systems in the data center and areas housing IT resources from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems including sprinklers and fire extinguishers, uninterruptible power supply (UPS), and emergency power generators and lighting. To determine whether temperature and humidity controls were in place, we inspected the data center to ensure the presence of appropriate dedicated air conditioning units and/or HVAC systems. In addition, we reviewed environmental protection controls related to general housekeeping procedures in the data center, computer classrooms, and telecommunication closets, and selected areas housing IT resources.

To evaluate whether only authorized user access could be gained to the College's network and systems, we reviewed the College's access security policies and procedures with the responsible security administrator. To determine whether system access security controls were in place and in effect, we reviewed and evaluated the administration of logon IDs and passwords and selected control practices regarding system access to network resources. To assess whether all users with active privileges were current employees, we obtained the list of individuals granted access privileges to e-mail accounts and other business-related applications, such as Colleague, and compared all users with active access privileges, as of June 11, 2008, to the College's list of then current employees, including faculty, administrative staff, and outsourced staff. To determine whether access privileges that were no longer required or authorized were disabled in a timely manner, we also compared the active network user listing to WSC's listing of terminated employees and their respective termination dates. Furthermore, we reviewed password configuration and whether all persons authorized to access the computing systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine the status of the College's ability to comply with Payment Card Industry (PCI) standards, we obtained and reviewed PCI Industry's data security standards and evaluated the College's PCI self-assessment questionnaire provided by the Office of the State Comptroller. To validate the control procedures associated with the responses in the self-assessment questionnaire, we interviewed College

staff and reviewed the network configuration diagrams. With respect to personally identifiable information (PII), we reviewed Chapter 93H of the Massachusetts General Laws and Executive Order 504 to identify agency responsibilities regarding protection of PII and notification for confidentiality breaches. We interviewed senior management and completed a PII assessment questionnaire regarding the protection of personal information of WSC's faculty, staff, and students.

To determine whether the College complied with Commonwealth of Massachusetts regulations for fixed-asset accounting, we reviewed evidence supporting WSC's performance of an annual physical inventory and reconciliation of the inventory record of computer equipment. To determine whether adequate controls were in place and in effect to properly account for WSC's computer equipment, we reviewed inventory control policies and procedures and requested and obtained the College's inventory system of record for computer equipment. We reviewed the current inventory system of record dated March 4, 2008 for IT equipment valued at $3,595,698 to determine whether the inventory contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the computer equipment. We also performed a data analysis on the inventory records of computer equipment to identify any unusual distribution characteristics, duplicate records, or unusual or missing data elements. To determine whether the inventory system of record for computer equipment was current, accurate, complete, and valid, we used Audit Command Language (ACL) software to select a statistical sample of 225 items, with an associated value of $201,851 out of a total population of 2,495 items. To evaluate whether the system of record accurately and completely reflected the items of computer equipment, we verified the location, description, inventory tags, and serial numbers of the hardware items listed on the inventory record to the actual equipment on hand.

To verify the relevance and completeness of WSC's system of record for computer equipment, we selected 43 additional computer hardware items in adjacent locations to our original inventory sample and determined whether they were properly recorded on the College's inventory record. To determine whether selected computer hardware purchases in fiscal years 2007 and 2008 were accurately listed, we randomly selected nine invoices that were comprised of 392 items, valued at $298,337, and verified whether the amounts recorded on the College's purchase orders and related vendor invoices were properly recorded on the inventory system of record. To determine whether WSC had appropriate control practices in place and in effect to account for and safeguard laptops, we interviewed representatives from the IT and facilities department, reviewed the control form used by each department regarding computer equipment loan policies for employees, and reviewed WSC's documented policies and procedures to control the assignment and use of laptops.

To determine whether WSC complied with Commonwealth of Massachusetts regulations for the disposal of surplus property, we reviewed records and supporting documentation for IT equipment disposed of during the audit period, as well as IT equipment that the College planned to request Commonwealth approval to dispose of as surplus. Finally, to determine whether WSC was in compliance with Chapter 647 of the Acts of 1989 reporting requirements, we reviewed incident reports for missing or stolen IT equipment for the audit period and verified whether these incidents were reported to the Office of the State Auditor.

To assess the adequacy of disaster recovery and business continuity planning, we reviewed the level of planning and the procedures to be followed to resume computer operations in the event that the computing systems become inoperable or inaccessible. We interviewed WSC management to determine whether the criticality of application systems had been assessed, whether an IT risk analysis for computer operations had been performed, and whether a COOP, written disaster recovery and business continuity plan was in place and, if so, whether it had been adequately tested. In addition, we reviewed the status of management's efforts to designate a potential alternate processing site to be used in case of an extended disruption of system availability.

We interviewed the Chief Information Officer responsible for the backup of all mission-critical applications and associated data files and reviewed the current backup procedures in place for their adequacy and completeness, including those in place for the mission-critical Colleague system. To review the adequacy of physical security and environmental protection controls for the on-site and off-site storage areas for backup copies of magnetic media, we assessed relevant policies and procedures, and protective measures such as a combination-locked fireproof safe. We also inspected the daily backup copies of computer media stored on-site to determine whether the provisions for storage, frequency of backup, and adequacy of controls were in place to protect backup media. Furthermore, we interviewed responsible personnel to determine whether they were formally trained in the procedures of performing media backups and were aware of the procedures for on-site and off-site storage of magnetic media, and the steps required to ensure the restoration, protection, and safety of the backup magnetic media.

The review of IT-related contracts with third-party service providers was accomplished by analyzing policies and procedures used to help ensure that the contracts were initiated and processed in compliance with state regulations. For the period of July 1, 2006 through June 30, 2008, we sampled for review 14 IT vendor service contracts with an aggregate maximum obligation of $1,340,977 out of total expenditures of $2,445,042. We consulted with the Office of the Secretary of State to determine whether the selected vendors were properly registered with the Commonwealth. Regarding contract documentation, we reviewed selected contracts to ascertain that the contracts contained original signature

pages with corresponding authorized signatures to ensure compliance with applicable state laws and regulations. Further, contract start dates for work were verified according to the dates of contract signature and compliance with contract terms. Moreover, we evaluated contract documentation to determine whether contract provisions were sufficient to hold the third-party service providers accountable for delivering quality services and whether the College made payments in compliance with contract terms.

To determine whether background checks are performed prior to an individual's employment or change in position, including staff or students who would have unsupervised contact with vulnerable populations such as students, children, or the handicapped or the elderly, we interviewed senior management and reviewed the College's procedures and control practices. To assess effectiveness and compliance with the College's policies and procedures pertaining to mandatory background checks, we reviewed and tested documentation with regard to volunteers and students accepted into specific academic programs. We reviewed Chapter 6, Sections 167-178B, and Chapter 6, Section 178C-178P, of the General Laws and Executive Office of Health and Human Services 101 Code of Massachusetts Regulations (CMR) 15.00-15.16 Criminal Offender Record Checks (CORI). We compared required information outlined within 803 CMR 3.05 Sections 1 and 2, with WSC's CORI Request Form. We then compared CORI Applicant Files to our statistical sample of WSC's students and employee listing of faculty, administrators, and staff.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Criteria used in the audit included Chapter 93H of the Massachusetts General Laws; Executive Orders 490, 491, and 504; Chapter 82 of the Acts of 2007; Chapter 647 of the Acts of 1989; management policies and procedures; and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1) issued by the Information Systems Audit and Control Association, July 2007.

AUDIT CONCLUSION

Based on our audit at Worcester State College (WSC), we found that internal controls were in place to provide reasonable assurance that IT-related control objectives would be met with respect to IT organization and management, on-site and off-site storage of backup copies of magnetic media, third-party provider IT service contracts, environmental protection for areas housing computer equipment, and security requirements related to Payment Card Industry (PCI) and Personally Identifiable Information (PII) standards. However, controls needed to be implemented or enhanced to provide reasonable assurance that computer equipment would be properly accounted for and safeguarded and that IT system capabilities could be regained within an acceptable period of time. In particular, controls pertaining to system access security, hardware inventory, physical security, and disaster recovery and business continuity planning needed to be improved. We also found that the College needed to more effectively monitor and evaluate whether Criminal Offender Record Information (CORI) background checks were being consistently performed prior to an individual's employment or acceptance into a specific academic program at the College.

Regarding internal control documentation, WSC should complete its Internal Control Plan (ICP) to assist management and staff in ensuring that appropriate controls are implemented and exercised to achieve operational objectives and avoid undesired events, such as overspending, operational failures, and violations of law. The completion of the ICP will support the College's efforts to address IT governance objectives and fully implement a control framework that contributes to these needs by linking business requirements, organizing IT activities into a generally accepted process model, identifying and leveraging major IT resources, defining management control objectives, and identifying and ensuring that risks are effectively managed.

Our review of IT management and control indicated that WSC had an appropriate and defined organizational structure and chain of command for the IT Department with assigned reporting responsibilities and documented job descriptions. The College also had documented IT strategic priorities that addressed WSC's IT environment and the mission-critical Colleague application. With respect to the use and safeguarding of information technology, we determined that formal policies and procedures existed, but needed to be updated to more accurately reflect the current IT environment for physical security, inventory control of computer equipment, system access security, background checks, and business continuity planning. Having appropriate and well-documented policies and procedures increases the likelihood that desired control practices will be adequately communicated, administered, and enforced.

With respect to physical security, we found that controls needed to be strengthened to ensure that employees who are terminated or take a leave of absence have their access cards (OneCard) disabled and/or that their door keys are returned to the Campus Police. We found that certain controls were in place and in effect regarding WSC's buildings that house the data center, selected computer labs, telecommunication closets, and the off-site storage location, and that visitors were escorted when accessing the data center thereby reducing the risk of damage and/or theft of computer equipment. Our review of selected areas housing workstations disclosed that on-site Campus Police officers patrol the campus and answer calls on a 24-hour basis throughout the calendar year. However, our audit revealed that WSC needed to strengthen its controls to ensure that employee OneCards are disabled when staff are no longer associated with the College. Although the master and sub-master door keys were properly accounted for, we found that faculty and staff who did not appear on the current payroll had not returned their office and area keys to the Campus Police. As a result, the potential exists for unauthorized access into restricted areas that could result in the damage or loss of IT equipment.

Regarding system access security, our audit revealed that the College needed to strengthen its controls over network resources to ensure that only authorized users have access to application systems and data files. We determined that WSC had documented procedures in place for the activation of user IDs and passwords that allow network access privileges by faculty, staff, and students. We also found that the College had initiated procedures to ensure compliance with the Commonwealth's Information Technology Division's (ITD) policy governing the use of mobile computing devices that may access network resources. We determined that in addition to logging onto the network, a user must also enter a unique UAID and password to logon to the College's mission-critical Colleague application. Although we found that 100% of the Colleague user access accounts tested were for current employees, we determined from our test of active user accounts to the current payroll that controls needed to be strengthened to ensure that WSC disables network access privileges in a timely manner for faculty and staff who are no longer employed by the College. We determined that although password rules were in place to allow for acceptable logon security, we found that WSC did not meet the Commonwealth's Information Technology Division's minimum password requirement of eight characters. The absence of adequate controls over system access security places critical and personally identifiable information at risk allowing unauthorized users to modify, delete, or disclose proprietary data.

Based on our review of Payment Card Industry (PCI) data security standards, we determined that adequate controls were in place to provide for the security of payment cardholder information. We found that WSC had policies and procedures for antivirus and firewall protection, access security controls, and encryption of confidential data. To help protect against intrusion from external sources, we found that the College had installed applications to integrate and enforce network access security including network

antivirus and firewall protection. The controls included Internet Protocol (IP) assignments, password policy, authentication of administrators, authorization of commands, remote access policy, user audit trails, and overall network admission controls. Moreover, we found that WSC had installed software to provide remote access security for Virtual Private Network (VPN) connectivity for both Internet Protocol Security (IPsec) and Secure Socket Layer (SSL). With regard to encryption, we verified that the WSC does not store credit card information and that transmission of sensitive cardholder data is encrypted over public networks through the use of SSL. Based on our review of the College's response to the Office of the Comptroller and Information Technology Division questionnaire, dated May 16, 2008, we found that WSC had acknowledged that they were not in compliance with the PCI data security standards concerning Service Set Identifier (SSID) Broadcast and PCI vulnerability scans. We determined that the College had subsequently initiated the scheduling of quarterly vulnerability scans. We also determined that WSC had chosen not to disable the SSID functionality; however, we verified that the College has a vendor-provided wireless security and management solution in place that requires user authentication, verification, and confirmation. Although adequate controls are in place to comply with PCI Data Security Standards, WSC needs to strengthen its procedures to disable passwords and OneCards for those staff and faculty no longer employed by the College. It is recommended that the College consolidate its existing PCI-related policies and procedures into a single document to more adequately focus on compliance with PCI data security standards.

We determined from our analysis of controls over personally identifiable information that WSC had adopted the controls set forth in the Family Educational Rights and Privacy Act (FERPA) and Health Insurance Portability and Accountability Act (HIPPA) to protect electronic and hardcopy information that can potentially be used to uniquely identify, contact, or locate an employee or student of the College. We also determined that user access to the Colleague system to add, update, and electronically view sensitive information is monitored and approved by the appropriate offices, i.e. Registrar, Finance, and Human Resources. We determined that each office is responsible to oversee access rights within their respective areas. We verified that sensitive data within the Student Information System (SIS) server is encrypted with 128-bit Secured Socket Layer (SSL) certification. Our audit included a review of PII in the College's Student Health Services Department and the Office of Judicial Affairs. We determined that electronically stored PII in both offices was maintained in a secured manner. Although hardcopy PII associated with Judicial Affairs was secured, our inspection of the Student Health Services Department found that health forms containing PII were kept in an easily accessible area pending monthly filing. However, it should be noted that, when left unattended, the Student Health Services Department's office door was secured. We determined from our testing, that 100% of the unique user IDs and passwords to Colleague were disabled for those employees and students no longer affiliated with the College.

Our audit disclosed that WSC needed to improve inventory controls over computer equipment to ensure that the inventory record of IT-related assets is current, accurate, and complete. We determined WSC had inventory policies and procedures in place that included property definitions, asset valuations, acquisition/receiving, reporting of lost or stolen property, and disposition of outdated and unused equipment. Although the College had inventory policies and procedures in place, we found that controls needed to be strengthened to ensure that the inventory system of record for computer equipment having a listed value of $3,595,698 is promptly updated when equipment is relocated, disposed of, lost, or stolen. In addition, we determined from our analysis of inventory records for the entire population of 4,758 IT computer-related items that information was missing within the data fields that indicate purchase order, description, and price. Based on our examination of the 216 laptops listed on the inventory system of record, we found that a majority of employees who had been assigned a laptop had not signed an equipment loan agreement form. The strengthening of asset management controls will help to improve the integrity of the College's inventory system of record, thereby allowing WSC to properly account for computer equipment, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Although on-site and off-site storage of backup media was in place, our review indicated that the level of disaster recovery and business continuity planning needed to be strengthened. We found that WSC had working drafts of disaster planning policies and procedures to support recovery of the College's mission-critical Colleague system, Blackboard applications, Pharos print system, and the Helpdesk Expert Automation Tracking (HEAT) system. We determined that the draft disaster recovery plan included background information for each system, system dependencies, support information, back-up procedures, recovery steps, and data loss risk assessment. However, we found that there was an absence of a formal documented disaster recovery plan to address the resumption of computer-related operations. We determined that although WSC had identified the need for an alternate processing site, the College had not selected an off-site processing location for back-up computer operations. Our audit disclosed that WSC did not have a business continuity plan to provide reasonable assurance that mission-critical and essential information technology operations for administrative and academic functions could be regained effectively and in a timely manner should a disaster render network resources inoperable or inaccessible.

With regard to background checks, we determined the College was inconsistent in the manner in which they performed criminal background checks for faculty, staff, and students who interact with vulnerable populations. Our audit confirmed that WSC was conducting Criminal Offender Record Information (CORI) background checks for prospective employees who would have access to areas that house students and for students enrolled in the College's Nursing Program, Criminal Justice, LEI, and the Division of Graduate and Continuing Education (DGCE) Young Professionals Program. However, due

to the non-uniform manner in which WSC conducts departmental CORI background checks, from our testing we determined that some departments were unaware that CORI checks should be conducted for employees, students, and volunteers in positions that involved the potential for unsupervised contact with children, the disabled, or the elderly. In addition, we found that the College did not maintain complete records for CORI checks performed. Regarding Sexual Offender Record Information (SORI) checks, we found that the College did not perform separate SORI checks for prospective employees. CORI does not include criminal records for out-of-state sexual offenders.

We determined that adequate environmental protection controls, including smoke and fire detection alarms, were in place and in effect to ensure that IT operations were providing a proper environment to safeguard IT equipment located in WSC's data center and selected computer labs throughout the campus. In addition, an uninterruptible power supply was in place to safely shutdown computer operations helping to ensure that systems and data files would not be adversely impacted by a loss of power. However, during our walkthrough of selected telecommunication closets, we determined that environmental protection controls needed to be improved to alleviate excessive heat and humidity. In addition, policies and procedures for environmental protection needed to be developed to ensure that IT resources are safeguarded. We recommend that the College enhance environmental protection controls to prevent loss or damage to IT resources.

Regarding IT-related contracts for fiscal years 2007 and 2008 with third-party vendors, we found that the College exercised adequate management oversight to hold contracted parties sufficiently accountable for their performance. Based on our review of contracts with high dollar maximum obligations, we judgmentally selected 14 vendor agreements with total contract payments of $995,242. With regard to contract documentation for our selected test sample, we found that vendors with contracts in excess of $5,000 were not required to go through the bidding process as they were listed with either the Massachusetts Higher Education Consortium (MHEC) or the Colleges of Worcester Consortium, Inc. (COWC). Our tests of selected original signature pages revealed that all contracts were executed with the proper delegation of authority and in compliance with relevant state laws and regulations. We also determined from our review that the contract agreements accurately documented deliverables to adequately measure results against stated goals and scheduled timelines for completion. In addition, we determined from our testing of WSC's expenditure reports that WSC made payments within budgeted maximum obligations, with the exception of overpayments on two contracts totaling $1,025. Our subsequent review of the two expenditures revealed that proper approvals were received prior to overpayment of the contracts. We recommend that the College more closely monitor expenditures to ensure that they do not exceed maximum obligations of the contract.

AUDIT RESULTS

1. System Access Security

Our audit of Worcester State College (WSC) revealed that system access security for the College's network resources needed to be strengthened to ensure that only authorized users have access to the network, certain application systems, and data files. Although adequate policies and procedures were being followed to authorize and activate user privileges for access to WSC's network resources, controls needed to be enhanced regarding the timely deactivation or deletion of network user accounts for faculty and staff who are no longer employed with the College and generic accounts with limited access privileges that are no longer assigned to an individual or department. We also found that the College was not in compliance with the Commonwealth's Information Technology Division's (ITD) policy concerning password composition regarding the complexity and minimum number of characters required.

We confirmed that users who require access to the Colleague application system had completed the Application for Colleague Account Form and that the forms were signed by the authorized user, department head, and senior level manager. The IT Department assesses the user's system needs, assigns a security class, and configures an appropriate level of access to the application system. We found that the College's documented procedures stated that Human Resources (HR) enters new employee information into the Colleague database. The system creates a user account that is needed to access the College's campus network resources, including Blackboard, WSC e-mail, and WebAdvisor. To obtain their user ID and password, new faculty and staff members must bring their WSC OneCard ID to the IT Department.

With regard to supervisory, super-user, capability, our audit revealed that five IT employees were authorized to have unlimited access to network files, applications, and operator commands. In addition, we determined there were ten users who had expanded access to Colleague system files. Access privileges appeared to be reasonable given the roles and responsibilities of the above five IT employees and ten Colleague users.

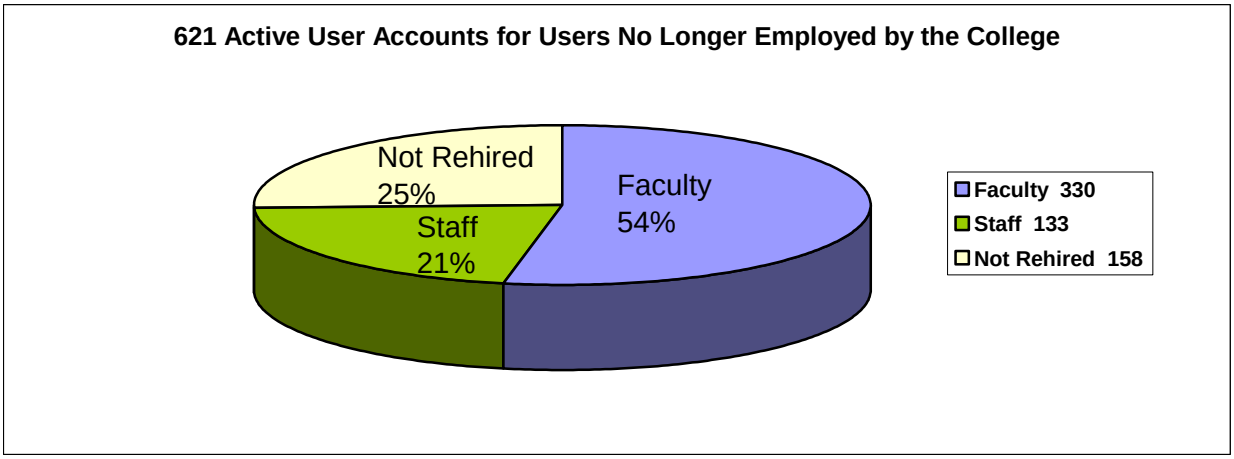
We found that the College has initiated procedures to ensure compliance with ITD policy governing the use of mobile computing devices, such as personal digital assistants (PDA), personal information managers (PIM), and Smartphones that can be used to access network resources. Based on our analysis, we concluded that WSC has the ability to remotely manage mobile computing devices to the extent where they are able to assign discrete passwords, lock devices after a set period of inactivity, and disable devices

in the event of loss or theft. We also confirmed that the College has a policy to not provide user sensitive information over the phone or via e-mail.

We obtained computer system access lists for WSC's local network resources and the Colleague application system and compared the data against the College's payroll listing, dated April 29, 2008. We determined from our testing of 381 Colleague system user IDs that all Colleague users were current WSC employees. We found that the College had a process in place to ensure Colleague user access accounts are either deactivated or removed as soon as an individual's employment status is changed and/or the employee is terminated.

Concerning WSC network logon user IDs, our audit test indicated that of the 1,709 active user accounts, 621 (36%) were for individuals who were not currently employed by the College. The 621 unidentifiable users included 92 (5%) individuals who appeared on the College's termination list dating back to July 2006. There were also nine (1%) generic user accounts that did not have an associated identifiable person or department.

Of the 621 user accounts, we determined that WSC should have deactivated 330 faculty and 133 staff user accounts. We determined the College should have deactivated the remaining 158 active user accounts that were assigned an employment type of "X" for employees who were on temporary leave.



We found that controls were not in place to deactivate user accounts for employees assigned an employment type of "X" who did not return to the College. We determined that user accounts for employees who were on temporary leave from the College remained active and were assigned an employment type of "X". The College's policy is that when an employee is rehired, their employment type reverts back to their original employment type.

The failure to deactivate user and generic accounts in a timely manner places the College at risk to having unauthorized access and use of IT resources. We note that the College took immediate action to deactivate the 621 user accounts identified during our audit.

Regarding password administration, we determined that written procedures were in place and in effect to identify, log, or investigate terminal access violations. We determined that off-campus vendor access to support of application systems would be made available if prior consent were given by appropriate managers through the use of temporary accounts with scheduled password expirations and time-outs.

Although WSC followed with best practices for password history and age, we determined that the College was not in compliance with password requirements for complexity and the minimum number of characters as set forth in 201 CMR 17.00: Standards for the Protection of Personal Information of Residents of The Commonwealth. Our review indicated that there were procedures for the initial authorization to activate new accounts, but that controls were not in place to inform IT of changes in employment status, including terminations, extended leaves of absence, or employee transfers. As a result, individuals may be able to access IT resources that they are no longer authorized to use, such as restricted websites or critical information on WSC's application systems. This may place the application systems and data files at risk to unauthorized access, modifications, or deletions.

At the beginning of our audit, we found that password configuration policy rules were being followed for history (repeat uses of passwords) and age (how long the password can be used); however policy rules for password length and password complexity were not (see chart below). We note that by the close of our audit, WSC had implemented the recommended password requirements to ensure compliance with the Commonwealth requirements and better align password administrative practices with general IT best practices.

Password Requirements	**WSC Policy**	**Recommended Policy**
Password Length	6 Characters	8 Characters
Password Complexity	Disabled	1 upper-case letter 1 lower-case letter 1 number

Generally accepted computer industry standards dictate that IT resources be made available to only approved users and that network and other IT resources be used for only authorized purposes. Access

security controls are also necessary to mitigate risks associated with technological environments, including various internal and external networks. Without deactivating user accounts for users who are no longer authorized to have access to IT systems or by not strengthening password composition, the College is vulnerable to unauthorized access to application systems and data that could place the security and integrity of online information at risk. For example, personally identifiable information could be at risk of a breach of confidentiality allowing for identity theft or fraud against a student or faculty member of the College.

Recommendation:

We recommend that WSC strengthen access security controls to ensure that access privileges for unauthorized users are deactivated or modified when a change in the employee's status results in the user no longer being authorized to access or use IT resources, or when a change in an employee's position or responsibilities requires a change in access privileges. Controls also need to be implemented to ensure that access privileges are deactivated for those employees who temporarily leave the College (assigned an "X" status). The user account can then be reactivated should the employee return to work.

To ensure that only authorized access privileges are maintained, we recommend that the College implement formal notification procedures requiring that a standard form be used by Human Resources or department management to notify IT personnel responsible for access security of changes in employee status, such as terminations, extended leaves of absence, or employee transfers, that would impact the user's level of authorization and access privileges. WSC should also implement controls to periodically review generic user accounts to ensure they are only used by authorized employees and, when appropriate, are deactivated. Sufficient security controls should be exercised to protect the confidentiality and integrity of important and sensitive data and to limit access to data and system functions to only authorized parties.

We commend WSC for updating their password policy to conform to the Commonwealth's regulations concerning complexity and number of characters. We recommend the College periodically review general IT best practices to ensure compliance with current standards.

Auditee's Response

The College has implemented the following measures, which meet or exceed the Audit recommendations, as follows:

1) *In May, 2008 Information Technologies finalized a coordinated effort with Human Resources to strengthen the process whereby information on all job actions is sent to IT immediately as it occurs and not every two months as*

previously designed. Information Technologies tracks information for each resulting job action in the College's the Help Desk ticket tracking system, HEAT. HEAT enables the creation of scripts that assist the College's staff in addressing all issues associated with an employee action.

2) *On November 17, 2008 Information Technologies implemented a strong password requirement for all WSC network accounts. Password policy is automatically enforced at the system level and requires an eight character password that must include one upper case letter, one lower case letter, and one number. Passwords cannot contain any portion of the user's first or last name, or previous password (of the last ten passwords). The lifecycle for all account passwords is 120 days.*

3) *In July, 2008 Information Technologies implemented policy and process that: a) requires an annual July review of all accounts for duplicates, retired, terminations etc. Appropriate action is taken for such accounts, including disabling accounts for long-term absences from the College and deleting account access for terminated, retired, or departed employees.*

4) *In July, 2008 Information Technologies implemented policy and process that deletes account access for all faculty who have not been assigned a course within the past eighteen months. This period of time covers seven semesters (including Fall, Spring, Summer1, 2 and Intersession), which accommodates faculty who teach on a semi-regular basis.*

5) *In December 2008, Information Technologies implemented a 'warning' message that is displayed on a user's screen when USB or CD/DVD devices are connected, to better ensure data security. In February, 2009 Information Technologies will implement a full disk encryption process which will initially cover all WSC owned laptops. Mission critical desktops computers also will be encrypted at this time; the remainder of the College's computers also will be locally encrypted by the end of the current fiscal year.*

The policies related to the above changes can be found at http://it.worcester.edu under "ADDITIONAL Policy Guides…"

Auditor's Reply

We acknowledge that the College has taken steps to strengthen access security controls to ensure that access privileges for unauthorized users are deactivated or modified. By strengthening password composition and other corrective action, the College has reduced the risk of unauthorized access to application systems. While we acknowledge that the annual review of all accounts for duplicates, retired, or terminations is a good control to implement, we suggest that the College consider more frequent review for sensitive or high-risk user accounts.

2. Physical Security

With respect to physical security, we determined that certain controls were in place at WSC's buildings that house the data center, selected computer labs, telecommunication closets, and off-site storage location. We determined that OneCard access is the preferred means of entering and logging employee admission to secured IT areas. Our audit revealed however, that the College needed to strengthen its controls to ensure that the OneCard access cards are disabled and that keys are returned to the Campus Police for those employees who are terminated or take a leave of absence.

Our review disclosed that each shift of Campus Police conducts 24-hour patrols of selected areas housing IT equipment. We determined that WSC had cameras in place in areas that house the data center and that department heads are responsible for securing IT equipment located in the computer labs and classrooms. We also found that classroom overhead projectors were locked in place and security cables protected workstations located in WSC's computer labs.

Although the College had policies in place to issue OneCards and assign access profiles to authorized employees, we found that adequate physical security controls were not in place to ensure that OneCards were disabled when staff are no longer associated with the College. Based on our analysis of 26,703 OneCard holders, we determined there were 1,162 employees with clearance to College facilities that did not appear on the current payroll list. We also found that of the 1,162 active OneCard holders, 110 appeared on the College's list of terminated employees dating back to July 1, 2006. In addition, we determined that OneCard holders identified with an employee type of "X" were faculty or staff who had left the College on a temporary basis and, although they had been removed from Colleague, their OneCards remained active in the Computer Coordinated Universal Retrieval Entry (CCURE) application managed by Campus Police. When an employee returns to the College, their temporary classification is changed and they revert to their original employee classification. Our review found that of 1,162 active OneCard holders who were not on the WSC payroll, 934 were identified with an employment type of "X". We determined that the College did not have adequate controls in place to disable OneCard access cards for employee who do not return to work.

With regard to WSC's door key policy, we found that the College needed to strengthen controls over the maintenance of keys for offices and general areas located throughout the WSC campus. We determined that the College properly accounted for 100% of the 12 master keys and 79 sub-master keys assigned to 32 individuals. However, we found from our test of 585 office and general area keys assigned to 287

individuals, that there were 66 (23%) individuals associated with 110 (19%) keys who did not appear on current payroll listing. Of the 66 individuals, we found that 34 (12%) individuals who appeared on the termination listing dating back to July 2006 had 59 (23%) keys assigned to them. Based on our review of the titles associated with the 66 employees and our meeting with the Deputy Chief of Campus Police, we determined that staff who had not returned their keys did not have access to areas housing the data center or strategic areas of the IT Department.

Generally accepted computer industry practices indicate that appropriate physical security controls need to be in place to ensure that the information technology assets and information are safe and secure. Physical security is one of the cornerstones to information system security along with system access security. The failure to provide adequate physical security controls places the College at risk to unauthorized access to IT resources that could result in unauthorized use, modification, destruction, damage, theft, and loss or reduction in IT services. In addition, it could also result in the loss of personal information creating a substantial risk of identity theft or fraud against a resident of the Commonwealth.

We note that during our audit, the College has taken action to enhance the documented procedures for managing the issuance and return of keys thereby ensuring that newly terminated employees return their keys prior to leaving the College.

Recommendation:

WSC's senior management should update its Internal Control Plan to include policies and procedures regarding physical security of IT equipment housed in the data center, telecommunication closets, and computer labs. Formal policies and procedures will help ensure that adequate controls over all aspects of physical security are in place and in effect. Part of these policies would include the assurance that OneCards are disabled in order to protect IT-related assets and critical components from unauthorized access, damage, or theft.

The College should perform a physical security risk assessment of the entire campus, and identify potential threats and exposures to computer resources, including equipment, communication infrastructure, software, media, and proprietary documentation. We recommend the College define and ensure that faculty and staff have an adequate understanding of the control objectives regarding physical security over IT resources. Policies, procedures, and responsibilities for physical security should be enhanced and, where required, should be approved and distributed to appropriate faculty and staff members.

We recommend the College initiate procedures to ensure that OneCards are disabled for faculty and staff assigned an employment category of "X" who do not return to work We recommend that WSC review their policies and procedures to ensure that monitoring mechanisms include formal reporting of security incidents, adherence to established procedures, and identification of security problems and their resolutions. We recommend an immediate reconciliation of keys to current employees to ensure that appropriate access privileges have been granted. WSC should also attempt to retrieve keys from terminated employees or consider re-keying locks to designated areas.

Auditee's Response

The College's Information Technologies Department is assisting Campus Police, who administers the CCURE door access system, in an effort to put in place policies and procedures which will meet or exceed the audit recommendations for door OneCard access Such policies and procedures will closely mirror the Information Technologies protocols already in place that address network access, including an annual reconciliation of CCURE records against current payroll (and as appropriate, student enrollment records). Campus Police anticipates having such policies and procedures in place by second quarter of 2009.

Physical access to key Information Technologies areas (primary and secondary data centers, switch closets and PBX rooms) will be reviewed by IT personnel on a quarterly basis. With regard to the key aspect of security, Campus Police has begun implementation of a key record tracking system to coincide with parking badge assignments. Re-keying the campus is under consideration, although financial constraints may preclude this from occurring in the next fiscal year. Those areas where terminated employees may have keys which have not been returned have been re-keyed as needed.

Auditor's Reply

We commend the actions being taken by WSC to improve physical security controls throughout the College campus. The College should closely monitor the efforts of the Campus Police to ensure that OneCard policies and procedures are in place by second quarter of 2009. We also commend the College's implementation of a key record tracking system. This should be helpful in maintaining an accurate record of who has been assigned keys and to what areas they have been granted access. Combined with employment exit procedures, it should help ensure that keys, or other security devices, are returned to the College. We understand that WSC is under financial constraints that preclude re-keying of the entire campus and agree with the procedure to re-key certain areas. The College's actions with regard to physical security will enable WSC to reduce the risk of unauthorized access that could lead to property damage, vandalism or theft.

3. Disaster Recovery and Business Continuity Planning

We determined that Worcester State College (WSC) did not have a comprehensive disaster recovery plan (DRP) and business continuity plan (BCP) to provide for the timely restoration of mission-critical and essential business functions should IT systems be rendered inoperable or inaccessible. Although the College had working drafts of disaster planning policies, a Continuity of Operations Plan (COOP), and a best practices document regarding disaster recovery, an alternate processing site had not been designated and a sufficiently detailed recovery and contingency plan had not been finalized to ensure that processing could be regained for mission-critical and essential IT systems within an acceptable period of time. The absence of a formally documented recovery and contingency plan to address disaster recovery places at risk the College's ability to resume computer-related operations to enable WSC to continue its mission as an institution of higher education.

We determined that, although WSC has identified the need for an alternate processing site, the College has not completed its plans for the selection of an off-site location for back-up computer operations. IT contingency planning is a coordinated strategy involving plans, procedures, and technical measures that enable the recovery of IT systems, operations, and data. IT contingency planning represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. IT contingency planning fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning.

We found that WSC had an Emergency Response Plan (ERP) that had been prepared by the Emergency Management Plan Committee and revised in 2007. This plan provides the response procedures for occupants of a facility in the event of a situation posing a potential threat to the health and safety of personnel, the environment, or property. Such events would include a fire, hurricane, criminal attack, or a medical emergency. Although the ERP may be appended to the BCP, it would probably be executed separately.

While management had informally assessed the relative criticality of their computing systems and developed various policies, the College had not outlined or tested comprehensive recovery strategies to address various disaster scenarios that would have resulted in seriously degraded or lost IT processing capabilities. In addition, if a disaster should occur, there were no contingency plans developed by departments to address critical functions throughout the College. As part of WSC's Business Practices document, risk is discussed in a number of paragraphs; however, it lacks a level of specificity to

determine the extent of potential risks and exposures to IT operations and scenarios. Although WSC understands the needs of recovering data processing systems, the risk analysis should identify the relevant threats that could significantly degrade or render IT systems inoperable or inaccessible, the likelihood of the threat, and expected frequency of occurrence for each disaster scenario. Additionally, WSC had not completely documented the necessary tasks and responsibilities for all relevant WSC personnel to carry out the College's duties and business objectives under various disaster scenarios. As a result of the weaknesses noted, should a disaster occur, the Colleague application system supported by the IT Department might not be restored within an acceptable period of time, thereby jeopardizing the College's essential operations.

An up-to-date effective BCP should identify the manner in which essential services would be restored or replaced without the full use of the data center facility or loss of network communications. The plan should identify the policies and procedures to be followed, detailing the logical order for restoring critical data processing functions, either at the original site or at an alternate processing site. In addition, the plan should describe the tasks and responsibilities necessary to transfer and safeguard backup copies of data files, program software, and system documentation from off-site storage to the site being used for restoration efforts.

Recommendation:

WSC should complete a business continuity plan that incorporates criticality and impact assessments, business continuity planning development, risk management, recovery plan testing and maintenance, training, and communication. We recommend that recovery strategies be documented to address various disaster scenarios that could adversely impact IT operations. We recommend that the College designate an alternate processing site and that recovery and business continuity plans be subject to appropriate testing to determine their viability. To help ensure that the College reacts optimally in the event of a disaster, the business continuity plan should be correlated to WSC's COOP detailing the College's current mission-critical Colleague system and a risk analysis that assesses various disaster scenarios.

WSC should ensure that the business continuity plan provides recovery strategies with respect to all potential disaster scenarios. The plan should assign specific staff with roles and responsibilities and present detailed steps for them to follow in recovering mission-critical and essential IT systems and operations. The plan should also address the telecommunications and security issues that would arise if the College had to conduct off-site computer operations. In addition, the BCP should document vendor protocol for the emergency use of computers suitable for operating the WSC's mission-critical

application. The College should conduct periodic training for the staff and ensure that a complete hard copy and electronic copy of the plan is stored in a secure off-site location.

Auditee's Response

The College is aware that a comprehensive business continuity and disaster recovery plan must be developed according to segment best practices and in a timely fashion. The institution recognizes that such planning is necessary to ensure that its business processes and delivery of services can be maintained in the event of a catastrophic hardware failure or data loss. While Information Technologies has an extensive library of policy and procedure documents that form the basis of a business continuity and recovery plan (and the construction of a secondary offsite fallback data center is nearing completion), such materials need to be aggregated into a single location and format for greater usability in the event that a situation arises. Information Technologies has introduced the necessity for comprehensive business continuity and disaster recovery planning at the President's Executive Leadership Team, which received strong support from each of the College's five divisions; the President and the Executive Leadership also recognize that business continuity and disaster recovery planning must factor in the specific business needs of each division and that it should not focus solely on the restoration of IT equipment.

As a result, the College will engage an outside consultant who will provide the institution with a preliminary risk analysis; a second consultant already has been engaged to more thoroughly assess the College's PCI/PII compliance. Additionally, IT will provide COBIT training for its staff and key non-IT decision makers as a way to facilitate a common understanding of the dependencies associated with technology planning and implementation. This February, the College will convene a disaster recovery and business continuity working group, whose charge will be to draft a full working disaster recovery and business continuity plan. The deliverable date for this comprehensive document will be July 1, 2008. After the full working draft has been compiled, yet another third party consultant will be engaged to review the document and offer an assessment of its feasibility and the practices that it contains. A final disaster recovery and business continuity plan will be made available to the President's Executive Leadership team by September 1, 2009 for its formal approval.

Auditor's Reply

We note that the College is aware of the need for a comprehensive business continuity plan to ensure that business operations and IT services can be recovered and maintained in the event of a catastrophic IT systems failure or loss of processing capabilities. We are pleased that the College plans to develop comprehensive disaster recovery and business continuity plans and will soon have access to a secondary data center to serve as an alternate processing site. We are hopeful that, with the support of the President's Executive Leadership Team and the engagement of outside consultants, the College will be

able to achieve its timetable for completion of a final disaster recovery and business continuity plan. It should be noted that until the recovery and business continuity plans have been completed and tested, WSC remains at risk of not being able to recover IT processing capabilities within an acceptable period of time

4. Background Checks

Although the College conducts background checks for faculty and staff candidates for employment and for individuals in certain departments and related programs, background checks were not conducted for all required departments nor when an employee transfers to another position within the College, which would require a Criminal Offender Record Information (CORI) check. Our audit revealed that the College was conducting CORI checks for faculty and staff at the time of employment based on the area of responsibility in accordance with WSC's CORI policy, dated July 2005. A new CORI background check for individuals who are transferring to another position that would require an increased level of trust may identify something that had occurred since the person was employed by the College that would make them unsuitable for the new position. Moreover, we determined that WSC's procedures do not ensure that background checks are performed for contract workers, or volunteer employees, hired for certain positions of special trust and responsibility, such as those with the potential for direct contact with children 18 years of age or younger who participate in the College's Athletic Department Summer Camp, Student Affairs Upward Bound Program, and Occupational Therapy's Bike Riding Program. We also determined that WSC does not conduct Sexual Offender Registry Information (SORI) background checks for any out-of-state prospective employees.

Our review of the College's CORI policies and procedures, Student Guide, and Website disclosed that 11 departments are required to conduct CORI background checks. The departments are Human Resources, Education, Nursing, Criminal Justice, Health Sciences, Occupational Therapy (Bike Riding Program), Communication Disorders, Athletics (Summer Camp Program), Student Affairs (Upward Bound Program), Division of Graduate and Continuing Education (DGCE Young Professionals Program), and the Latino Educational Institute. We determined that WSC's CORI checks conducted by Human Resources are limited to those faculty and staff who have access to areas that house students; i.e. Facilities, Resident Life, and Campus Police.

We determined that CORI checks for students in the Education Department are performed by the Worcester Public Schools. Our test of CORI checks conducted by the Worcester Public Schools found

100% compliance for the entire population of 406 students enrolled in WSC's Education Department during fiscal years 2007 and 2008. We also confirmed 100% compliance based on our test of CORI checks performed by WSC during fiscal years 2007 and 2008 for the 529 students enrolled in the College's Nursing program, 544 students enrolled in Criminal Justice, 39 students associated with the LEI, and the three students enrolled in the DGCE Young Professionals Program. We determined that CORI investigations for the Health Sciences internship program were not required during the past three fiscal years.

Our audit found that CORI background checks were not performed in a uniform manner across all departments. We determined that some departments were unaware that CORI investigations should be performed for students, volunteers, and employees in positions that involved the potential for unsupervised contact with children, the disabled, or the elderly. Based on our review, we determined that WSC did not perform CORI checks for students enrolled in the Student Affairs-Upward Bound Program, Occupational Therapy's Bike Riding Program, and Communication Disorders.

We were unable to conduct CORI testing for the Athletics Department Summer Camp Program since they do not have a consistent method for maintaining a record of CORI requests. The audit team also was unable to conduct testing for faculty and staff that have access to areas that house the students, as Human Resources did not maintain a record of CORI investigations due to concerns over privacy. However, the Criminal History Systems Board's record keeping guidelines state that CORI must be secured in a locked file cabinet when not being inspected and may be kept for up to three years for purposes of defending against any employment discrimination action.

We confirmed during our review of the College's policies and procedures and meetings with Human Resources that there are no mechanisms in place to conduct Sex Offender Registry Information (SORI) checks. The CORI and SORI databases are not linked; therefore, CORI background checks only provide relevant information regarding convictions in Massachusetts and do not include any crimes committed in another state. For example, an individual convicted of a sex crime in Connecticut, who subsequently moved to Massachusetts and as required by law registered as a sex offender, would go undetected on a Massachusetts CORI background check.

The College risks not being able to detect unacceptable employee actions when CORI and SORI background checks are not performed for all individuals who have the potential for unsupervised contact with vulnerable populations. In addition, M.G.L. 71, Section 38R indicates that periodic background reinvestigations should be performed at least once every three years, consistent with the sensitivity of the

employee's position. Compliance to state laws pertaining to CORI checks reduces the risk to public safety and minimizes the risk of departments engaged in providing activities or programs to children 18 years of age or less.

Recommendation:

We recommend that the College modify their CORI policy to centralize the responsibility for conducting CORI checks for all departments; thereby ensuring that CORI checks are performed on all prospective employees applying for positions of trust or who would work with vulnerable populations as defined by state law. The policy should require that adequate background checks be conducted on volunteers and on current employees who would be considered for transfers to similar type positions. A centralized approach would also ensure that appropriate personnel receive training and updates that will help the College consistently meet the Commonwealth's CORI regulations and minimize risk to WSC's students and increase public safety of the general population. The College should also strengthen its policy to ensure that CORI records are maintained in a secure manner for a minimum of three years.

We further recommend that the College expand their background check policies and procedures to require that SORI checks be conducted on any current or prospective employee who has recently moved to the Commonwealth and is either in or applying for a position that has contact with a vulnerable population. Per Chapter 6, Section 178I, of the General Laws, the College "shall receive at no cost from the board a report to the extent available pursuant to Sections 178C to 178P, inclusive, which indicates whether an individual identified by name, date of birth or sufficient personal identifying characteristics is a sex offender." However, this report is only available to the College by submitting a formal request for SORI from the Sex Offender Registry Board. Since all CORI checks provided by the Criminal History Systems Board contain Massachusetts' criminal history information only, the College may, if it deems necessary, also obtain a CORI check for out-of-state prospective employees. The Criminal History Systems Board website contains contact information for requesting CORI in other states.

We recommend that assurance procedures be exercised to ensure that the process of conducting background checks is being consistently performed prior to an individual's employment or acceptance into a specific academic program at the College.

Auditee's Response

> *The College is aware of the importance of CORI/SORI checks in maintaining a safe working environment. While CORI/SORI checks are completed by individual academic and administrative departments as part of their specific business responsibilities, the College recognizes that greater oversight needs*

to be in place to facilitate the development of appropriate institutional CORI/SORI policies, operational practices to ensure timely requests for CORI/SORI background checks, and processes to review results that might negatively impact the College, members of its community, and/or its visitors. To address these issues, the College will designate the Office of Human Resources as the central coordinating and oversight agency for CORI/SORI background checks, effective at the start of the 2010 fiscal year. Additionally, the Office of Human Resources will establish a CORI/SORI working group that will meet on a regular basis to develop and review local CORI/SORI policies and procedures.

Auditor's Reply

We commend the College's efforts to designate the Office of Human Resources as the central coordinating and oversight entity for CORI/SORI background checks and to establish a CORI/SORI working group to develop and review local CORI/SORI policies and procedures. The actions to be taken should strengthen governance over the process of conducting background checks thereby helping to ensure that appropriate policies are followed and that necessary background checks are performed.

5. Inventory Control Over Computer Equipment

Our audit disclosed that inventory control practices over computer equipment needed to be strengthened to ensure that WSC was maintaining a current, accurate, and complete inventory record of computer equipment. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when computer equipment is relocated or taken out of service. We also determined that WSC should improve controls to ensure that all data fields contained in the inventory system of record are properly completed. The quality of data that makes it appropriate for a given use is defined as the state of completeness, consistency, timeliness, accuracy, and validity. In addition, we found that WSC should enhance its procedures to confirm that a Loan Agreement Form is completed for each employee who is assigned a laptop. Based on our test results, the integrity of the IT inventory system of record for computer equipment could not be adequately assured. The failure to properly account for inventory of computer equipment hinders WSC's ability to evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

We determined from our testing that WSC was 100% compliant with respect to controls regarding the purchasing, receiving, and recording of newly-acquired computer equipment. We also found that the College was in compliance with policies and procedures for the reporting of surplus property to the Operational Services Division (OSD) and the communication of Chapter 647 documentation concerning missing or stolen items to the Office of the State Auditor. However, we found that documented policies and procedures needed to be enhanced regarding the maintenance, monitoring, and reconciliation of the

inventory system of record for computer equipment. With respect to the recording of IT resources, we found that WSC lacked appropriate controls to detect errors in updating the inventory system of record with regard to relocations, additions, and changes of computer equipment.

Our inventory tests of WSC's inventory system of record were conducted against 4,758 IT-related assets with an associated value of $3,595,698. We tested by inspection, the existence and the recorded location of our statistical sample of 171 items valued at $134,505. Furthermore, to verify the integrity and completeness of the inventory system of record, we judgmentally selected 83 additional IT-related items in adjacent locations to the items selected in our statistical sample. We determined that 100% of the 83 items were properly identified on WSC's listing of inventory computer equipment. However, based on our test of the 171 IT related items, we determined that 34 items valued at $15,699 representing a 20% error rate, were not at the locations indicated on the inventory system of record. Of the 34 items, we determined that 16 (9%) items totaling $7,266 could not be located. The remaining 18 (11%) items with an associated value of $8,433 were either in the wrong location or incorrectly recorded on the inventory system of record. Although we were able to account for 100% of the 54 laptops tested; we found that 11 (20%) of the items were not located in the rooms recorded on the College's inventory system of record.

We determined the College was 100% compliant with the Office of the Comptroller inventory system of record guidelines for data fields including tracking ID, location, serial number, and manufacturer. However, we found that WSC should improve data integrity by ensuring that all data fields are populated with the appropriate information. Based on our test of 14 data fields consisting of 4,758 records, we determined there was a significant amount of information missing from certain data fields including purchase order (45%), description (61%), and price (13%). The failure to adequately record purchase order information, description of items, and asset costs results in the inventory system of record not being maintained at an acceptable level of data integrity. The College needs to ensure that appropriate controls are in place for data entry and improve its monitoring and validating of information to ensure the accuracy and completeness of the information contained in the inventory database.

The College's "Laptop Use On or Off-Campus Policy", dated August 23, 2006, states that, "All users issued a laptop, whether temporary or long-term, will need to agree to and sign a current Equipment 'Loan' Form." We found that of the 216 laptops listed on the inventory system record, 174 did not have an Equipment Loan Agreement Form. This represents an 81% error rate. The absence of an Equipment Loan Agreement Form could contribute towards misuse or loss of the College's laptops. As a result, there is an increased risk that laptops may be lost or stolen.

Recommendation:

To ensure that WSC adequately maintains its IT inventory, the College should strengthen its current practices to ensure compliance with policies and procedures concerning moves, adds, and changes to the inventory system of record. We recommend that inventory control policies and procedures concerning changes to the status of IT related assets should be enhanced by increasing supervision and oversight to help ensure that all items of computer equipment are properly recorded in a timely manner on the College's inventory database.

We recommend that the inventory system of record be periodically verified through reconciliation to the physical inventory. To maintain proper internal control, staff not responsible for maintaining the inventory system of record should perform the periodic reconciliation of IT related assets. We also recommend that WSC refer to the policies and procedures outlined in the Office of the Comptroller's "Internal Control Guide" to help achieve the goal of ensuring the integrity of the inventory record and enhancing knowledge of the IT infrastructure. The College's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

With respect to IT configuration management, the College should update missing information in its inventory data fields with specific attention to Purchase Order, Description, and Price. In addition, the agency's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage. The inclusion of this information will help ensure that the College's IT-related equipment will be properly accounted for during the College's annual physical inventory.

In order to ensure safeguarding of laptops, we recommend that the WSC strengthen its controls to maintain complete and up-to-date signed acknowledgements that users have received or returned their laptops, thereby minimizing the risk of lost or stolen equipment.

The recommended control procedures should provide increased assurance that all IT-related equipment is recorded on the inventory record in a complete, accurate, and timely manner to enable WSC to produce a complete record of all IT-related equipment.

Auditee's Response

> *Since the arrival (and subsequent departure) of the Auditing Team, Information Technologies has made great efforts with regard to ensuring that existing inventory control policies and procedures are adhered to by all Information Technologies personnel in the strictest of manner. The audit*

itself served as an excellent reference point for IT staff as to why detailed policies and procedures are in place for IT inventory control and why it is critical that they are followed assiduously. The laptop distribution procedures also have been tightened, and several additional levels of checks and balances have been added, such as keeping on file a physical signature on an equipment loan agreement from all members of the College community who receive loan of computer equipment. Additionally, Information Technologies, on an ongoing basis, will continue to update historical data (e.g., original cost and purchase information, etc.) in the inventory database as necessary. As noted during the audit, physical inspection continues year round in order to exceed the required annual update.

Auditor's Reply

We commend the actions initiated by the College to improve inventory controls through implementation and monitoring of detailed IT policies and procedures. Strengthening inventory control procedures, including laptop distribution procedures and periodic reconciliation of the entire IT inventory, will improve the integrity of the inventory system of record and assist the College in making IT infrastructure and configuration management decisions.

6. Internal Control Plan

Our review disclosed that Worcester State College's Internal Control Plan, dated August 2005, was incomplete and did not include sufficient details on internal control objectives and controls nor a risk assessment as required by the Office of the State Comptroller. As a result, the current internal control document does not provide adequate guidance to ensure that appropriate controls are implemented and exercised so that operational objectives are met and that undesired events are prevented or detected and corrected in a timely manner. A more comprehensive internal control plan would also help the College to optimize its efforts in ensuring the integrity, security and availability of the College's systems and records, and in protecting and effectively using its resources.

Chapter 647 of the Acts of 1989, an Act Relative to Improving Internal Controls Within State Agencies, establishes the minimum level of quality acceptable for an internal control system in operation throughout Commonwealth departments, agencies, and colleges. Chapter 647 states, in part, that "Internal control systems for the various state agencies and departments of the Commonwealth shall be developed in accordance with internal control guidelines established by the CTR." Subsequent to the passage of Chapter 647, the Office of the State Comptroller issued written guidance in the form of the Internal Control Guide for Managers and the Internal Control Guide for Departments. In these guides, the Office of the State Comptroller stressed the importance of an internal control plan and the need for state entities to develop internal control policies and procedures.

We acknowledge that College management recognizes the need to complete a comprehensive internal control plan. We also acknowledge that the need to have a sufficiently-documented internal control plan does not mean that there is a widespread absence of policies, procedures or control practices throughout the College. The internal control plan should strengthen the College's framework of control and address the control requirements set forth by the Office of the State Comptroller.

Recommendation:

We recommend that the College's Internal Control Officer work with WSC's various departments to identify and document operational and control objectives and risks, and identify existing control policies, procedures and management control practices. We recommend that the process of completing the internal control plan include identifying any gaps in required controls and developing a plan to design, implement and exercise any additional controls required. Lastly, we recommend that the internal control plan address the components of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) control model and ensure compliance with the Office of the State Comptroller's internal control guidelines.

Auditee's Response

> *The College intends to revise the ICP to reflect a high level, department-wide summarization of risks and controls for all of its business processes, supported by lower level policies and procedures. Furthermore, the ICP shall be directly aligned with our organization's mission statement, goals and objectives, and components of internal control as recommended by COSO. A Strategic Planning process is currently underway at the College that has wide representation from the campus community. As this process continues, the Internal Control Officer will be working with the firm CBIZ Accounting Tax and Advisory of New England, LLC. to perform an enterprise risk assessment (ERM) necessary to develop our Internal Control Framework. Our ICP will encompass strategic goals and reflect the concepts of broad-based objective setting, event identification, and risk response in consideration of all programmatic and functional areas of the College. A strong ICP, embraced by the College community and compliant with the Office of the State Comptroller's internal control guidelines, is slated for completion before the end of the fiscal year*

Auditor's Reply

We are pleased that the College plans to revise their internal control plan to ensure compliance with Chapter 647 of the Acts of 1989 and the Office of the State Comptroller's guidelines.

References

803 CMR 3.05 Sections 1 and 2

Chapter 6, Sections 167-178B of the General Laws

Chapter 6, Section 178C-178P, of the General Laws

Chapter 11, Section 12, of the Massachusetts General Laws

Chapter 15A, Section 5, of the Massachusetts General Laws

Chapter 93H of the Massachusetts General Laws

Chapter 82 of the Acts of 2007

Chapter 647 of the Acts of 1989

Committee of Sponsoring Organizations of the Treadway Commission (COSO)

Comptroller General of the United States

Control Objectives for Information and Related Technology (version 4.1)

Criminal Offender Record Checks (CORI)

EOHHS 101 Code of Massachusetts Regulations (CMR) 15.00-15.16

Executive Orders 490, 491, and 504

Generally Accepted Government Auditing Standards (GAGAS)

Human Resources Compensation Management System (HR/CMS)

Information Systems Audit and Control Association (ISACA)

Massachusetts Management Accounting and Reporting System (MMARS)

Office of the Secretary of State

Office of the State Auditor

OneCard

Operational Services Division

Payment Card Industry (PCI) security standards

Personally Identifiable Information (PII) 1, 2, 3

State Comptroller Internal Control Guidelines

U.S. Government Accountability Office