A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

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

No. 2006-0203-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON INFORMATION TECHNOLOGY CONTROLS AND CERTAIN ACTIVITIES AT QUINSIGAMOND COMMUNITY COLLEGE

July 1, 2004 through June 16, 2006

OFFICIAL AUDIT REPORT
DECEMBER 19, 2006

2006-0203-4T

TABLE OF CONTENTS

INTRODUCTION

Quinsigamond Community College (QCC), which was established in 1963, is a Massachusetts institution of higher education offering associate degree and certificate programs. QCC also offers continuing education programs on a full-time and part-time basis. Chapter 15A, Section 5, of the Massachusetts General Laws created the Massachusetts State College System, of which QCC is a member.

Quinsigamond Community College's mission is to serve the diverse educational needs of central Massachusetts by providing affordable, accessible, and high quality curriculum that leads to career and lifelong learning. The College's main campus is a 47-acre facility located on West Boylston Street in Worcester, Massachusetts and is comprised of eight buildings that include student, learning, and athletic centers. At the time of our audit, QCC had a combined student population of 8,558 full-time and part-time students with an associated full time-equivalency total of 3,879. At that time, the College employed 771 full-time and part-time faculty, administrators, and staff members and was supported by a fiscal year 2006 budget of approximately $40 million.

QCC is governed by a Board of Trustees and is administered under the direction of the QCC's President. Additional oversight is provided to QCC by the Board of Higher Education, which is responsible for monitoring each Massachusetts higher educational institution to ensure that state funds support measurable performance, productivity, and results. From October 19 through October 22, 2003, QCC was subject to a re-accreditation process by the New England Association of Schools and Colleges. All divisions of QCC were reviewed with regard to 11 standards and a risk assessment as part of this important process. On April 22, 2004, QCC received a ten-year accreditation.

QCC's administrative and academic mission and operations are supported by the automated services provided by QCC's Information Technology (IT) Department. According to QCC, the IT Department's mission is to provide a stable technology infrastructure for electronic communications and delivery of student services and course content, and to gather accumulated information to be used for reporting on the operations of QCC. The QCC's IT Department is comprised of four groups: Academic Computing/ Instruction Technology, Information Systems, Network and Telecommunications Services, and Web Services. At the time of our audit, the IT Department consisted of 18-full time staff members. Each of the four groups has a director/manager under the direct control of a Chief Technology Officer who reports directly to QCC's Vice President for Administrative Services. The IT Department provides assistance and guidance to administrative staff, faculty, librarians, and students regarding the use of IT resources,

including the use of administrative computer systems, Internet portal support, personal computer maintenance, web hosting services, print servers, and e-mail.

Computer operations were supported by 39 file servers located in two data centers and approximately 1,179 workstations configured in a local area network (LAN). Of the 1,179 workstations, 771 were assigned to administrative staff and faculty and 408 were assigned to student computer laboratories and classrooms. QCC'S file servers were connected through a wide area network (WAN) to the Commonwealth's Information Technology Division (ITD) mainframe, which provides access to the Web-based Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS), the Commonwealth's accounting system. In addition, QCC maintained 98 notebook computers that were distributed to departments throughout the College for use by faculty, staff, and administrators.

From an administrative perspective, IT-related systems are used to process QCC's financial management, administrative, and student information activities. In this area, the primary application is the Jenzabar CX system. This system functions as QCC's database and application server for administrative systems, including admissions, student and administrative financial accounting, student grades, and enrollment. The Cognos suite of information management tools is used to further analyze data for purposes of reporting and institutional research. The Financial Aid Department uses the federally supplied software, EdExpress, which processes financial aid-related information internally and then, using a dedicated dial-in modem, uploads this data to the federal Department of Education.

Our Office's examination focused on selected IT general controls and QCC's control practices over the Criminal Offender Record Information and Sexual Offender Record Information background checks.

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 Quinsigamond Community College (QCC) for the period of July 1, 2004 through June 16, 2006. The audit was conducted from February 2, 2006 through June 16, 2006. Our audit scope included an examination of IT-related general controls pertaining to organization and management, physical security, environmental protection, system access security, inventory controls over IT equipment, disaster recovery and business continuity planning, on-site and off-site storage of backup magnetic media, and IT-related contract management. In addition, our scope included a review of the College's control practices regarding the Criminal Offender Record Information (CORI) and Sexual Offender Record Information (SORI) background checks required for certain individuals that have the potential for unsupervised contact with children, the disabled, or the elderly.

Audit Objectives

Our primary audit objective was to determine whether QCC's IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support QCC's business functions. In this regard, we sought to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available when required.

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 whether IT-related policies and procedures adequately addressed the areas under review. We also sought to determine whether QCC had implemented IT-related strategic and tactical plans that help direct the use of technology to fulfill the College's mission and goals. We determined 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 unauthorized use, damage, or loss of IT-related assets. We also determined whether sufficient environmental protection controls were in place 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 had been implemented to provide reasonable assurance that only authorized users were granted access to QCC's

application systems and data files. We evaluated whether procedures were in place to prevent and detect unauthorized user access to automated systems and IT resources, including the Jenzabar application, through the local area network (LAN) file servers and microcomputer workstations. In addition, we determined whether Jenzabar system data was sufficiently protected against unauthorized disclosure, modification, or deletion and whether QCC was actively monitoring password administration.

With regard to inventory control over IT equipment, including notebook computers, we reviewed and evaluated control practices regarding the accounting for computer equipment. In addition, we determined whether an annual physical inventory and reconciliation was conducted and whether inventory controls met Chapter 647 reporting requirements.

With respect to the availability of automated processing capabilities and access to IT information resources, we sought to determine whether business continuity strategies would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should computer systems be rendered inoperable or inaccessible. In addition, we sought to determine whether QCC had adequate control procedures for the generation and storage of on-site and off-site backup 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, and whether the contract agreements sufficiently detailed services or deliverables to be provided, and were properly signed and dated. 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 evaluated whether QCC had implemented adequate controls with regard to IT contract management to provide reasonable assurance that monitoring and evaluation were being performed.

We also sought to determine whether selected laws, regulations, and control practices regarding the completion of CORI and SORI background checks and the submission of supporting documents were performed prior to an individual's employment, changes in position, or acceptance into a specific academic program at the QCC.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of QCC's mission and business objectives. Through pre-audit interviews with managers and staff and reviews of documents, such as descriptions of QCC's organization and operations, we gained an understanding of the primary business functions supported by QCC's automated systems. We documented the significant

functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical by QCC.

Regarding our review of IT organization and management, we interviewed senior management, completed questionnaires, and analyzed and reviewed the organizational structure and reporting lines of QCC's IT Department. We obtained, reviewed, and analyzed relevant IT-related policies and procedures and strategic and tactical plans to determine their adequacy. To determine whether QCC's IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities and technological expertise requirements, we obtained a current list of the personnel employed by the IT Department, including their duties and job descriptions, and compared the list to the IT Department's organizational chart, each employee's statements concerning their day-to-day IT-related responsibilities, and the technology in use at the time. In addition, we reviewed relevant documents, such as the network configuration, strategic and tactical plans, internal control plan, and business continuity plan, and performed selected preliminary audit tests.

To evaluate physical security, we determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to computer facilities and selected areas housing IT resources, and whether authorized personnel were specifically instructed in physical security policies and procedures. Moreover, our review included the completion of a risk analysis questionnaire and interviews with QCC's senior management and QCC's Department of Public Safety, referred to as Campus Police, who are responsible for physical security for IT computer equipment. We also assessed QCC's physical security program and determined the extent to which physical access was restricted for areas housing IT computer equipment by conducting a walkthrough of the data centers, classroom labs, business offices, on-site and off-site storage areas, and selected telecommunication closets. We examined the existence of controls, such as motion detectors and intrusion alarms. Regarding key management at QCC, we interviewed the individual responsible for maintaining records of administrators, faculty, and staff that were issued brass key sets for the administrative offices within the College. Further, we obtained a listing of current brass keyholders and compared it to a QCC employment listing to verify that all keyholders were current employees of the College.

To determine whether adequate environmental controls were in place to properly safeguard automated systems in the data centers and areas housing workstations from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (i.e., sprinklers and fire extinguishers), an uninterruptible power supply (UPS), and emergency power generators and lighting. To determine whether proper temperature and humidity controls were in place, we inspected the data centers 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 centers, selected areas housing workstations, computer classrooms, and wiring closets.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated workstations. To determine whether the College's control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We determined whether QCC's internal control documentation included control practices, such as an acceptable use policy for IT resources and a formal security statement.

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated selected control practices regarding system access to network resources and reviewed the security procedures with the security administrator responsible for access to the automated systems on which the College's application systems operate. In addition, we reviewed control practices used to assign QCC staff access to the application programs and data files. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. To determine 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 Jenzabar, and compared all users with active access privileges, as of February 7, 2006, to the personnel roster of current employees, including faculty, administrative staff, and outsourced staff. Furthermore, we determined whether all persons authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes.

To determine whether adequate controls were in place and in effect to properly account for QCC'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 system of record, dated February 2, 2006, valued at $2,544,218, to determine whether it 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 and made note of any unusual distribution characteristics, duplicate records, or unusual or missing data elements. To determine whether the system of record for computer equipment was current, accurate, complete, and valid, we used Audit Command Language (ACL) to select a statistical sample of 212 items, inclusive of 58 notebook computers, with an associated value of $405,430 out of a total population of 2,744 items in order to achieve a 98%

confidence level. 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 QCC's system of record for IT related equipment, we randomly selected 43 additional computer hardware items in adjacent locations and determined whether they were properly recorded on the College's inventory record. To determine whether selected computer hardware purchases in fiscal years 2005 and 2006 were accurately listed, we randomly selected 49 invoices comprised of 492 items, valued at $523,181, and verified whether the amounts recorded on the College's purchase orders and invoices were properly recorded on the inventory system of record. To determine whether QCC had appropriate control practices in place and in effect to account for and safeguard notebook computers, 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 QCC's documented policies and procedures to control the assignment and use of notebook computers.

To determine whether the College complied with Commonwealth of Massachusetts regulations for fixed-asset accounting, we reviewed evidence supporting QCC's performance of an annual physical inventory and reconciliation of IT assets. Further, to determine whether QCC complied with Commonwealth of Massachusetts regulations for disposal of surplus property, we reviewed records and supporting documentation for IT-related equipment disposed of during the audit period, as well as IT-related equipment that the College planned to request Commonwealth approval to dispose of as surplus. Finally, to determine whether QCC was in compliance with Chapter 647 of the Acts of 1989 reporting requirements, we reviewed incident reports for missing or stolen IT-related 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 automated systems become inoperable or inaccessible. We interviewed QCC management to determine whether the criticality of application systems had been assessed, whether risk analysis to computer operations had been performed, and whether a written 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.

As part of our review of the adequacy of generation and storage of backup copies of magnetic media, we assessed relevant policies and procedures, as well as the adequacy of physical security and

environmental protection controls for on-site and off-site storage of magnetic media. We interviewed the Chief Technology Officer responsible for the automated full live backup of the IBM UNIX midrange and Windows 2000 network, and we reviewed the current backup procedures in place for their adequacy and completeness, including procedures for the mission-critical Jenzabar system. We also inspected the on-site daily backup copies of computer media to determine the provisions for storage, frequency of backup, and adequacy of controls in place to protect backup media. Further, we interviewed responsible personnel to determine whether they were formally trained in the procedures of performing backups and were aware of the procedures for on-site and off-site storage of magnetic media and the steps required to ensure the protection and safety of the backup magnetic media. Further, we sought to determine whether IT department personnel were cognizant of, and trained in, all procedures required to restore systems via backup magnetic media that would be required under disaster or emergency circumstances. Also, we examined the off-site storage facility to determine whether the area had adequate physical security and environmental controls. To evaluate the physical security and environmental controls for off-site backup magnetic media, we examined the combination-locked fireproof safe being used to store off-site backup magnetic media.

We sought to assess the internal control process for awarding, paying, and monitoring third-party IT service contracts. We sought to determine whether provider service contracts had been properly put out to bid and awarded and whether vendor payment vouchers were reviewed and approved, and contained the required authorized signatures. In addition, we sought to determine whether QCC had implemented adequate controls to provide reasonable assurance that monitoring and evaluation of provider service contracts was being performed in accordance with applicable Massachusetts General Laws and generally accepted business practices.

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, 2004 through June 16, 2006, we reviewed 16 IT vendor service contracts for fiscal year 2005 and seven IT vendor service contracts for fiscal year 2006. The Commonwealth's Secretary of State's Office was consulted to determine whether the incorporated vendors selected were properly registered with the Commonwealth. Regarding contract documentation, we reviewed selected contracts to ascertain that the contracts contained the original signature pages with corresponding proper signatures to ensure compliance with applicable state laws and regulations. Moreover, we evaluated contract documentation provided to us by the College to determine whether contract provisions were sufficient to hold the third-party service providers accountable for delivering

quality services and whether payments were made properly. Further, start dates for work under contract were verified according to the dates of contract signature and compliance with contract terms.

To assess the effectiveness and compliance with laws, rules, policies, and procedures of the College as they pertain to the Criminal Offender Records Information (CORI) and Sexual Offender Record Information (SORI) background checks, we analyzed and tested actions taken for prospective and current employees, volunteers, and students. In this regard, we reviewed and analyzed 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 (CMR) 15.00-15.16 Criminal Offender Record Checks. We compared and contrasted required information outlined within 803 Code of Massachusetts (CMR) 3.05 Sections 1 and 2, with QCC's CORI Request Form and CORI Applicant Files to our statistical sample of QCC's Employee Listing of faculty, administrators, and staff. We also conducted interviews with specific QCC Human Resources personnel, associated faculty, and public safety officials to ascertain information regarding the CORI and SORI background checks and analyzed all program specific documentation.

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. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT), as issued by the Information Systems Audit and Control Association, July 2000.

AUDIT CONCLUSION

Based on our audit at Quinsigamond Community College (QCC), we found that internal controls in place provided 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, and third-party provider IT service contracts. However, our audit revealed that controls needed to be implemented or enhanced to provide reasonable assurance that QCC's IT environment would include controls to properly account for and safeguard IT resources and ensure system availability when required. In particular, controls pertaining to system access security, hardware inventory, physical security, environmental protection, and disaster recovery and business continuity planning needed to be improved. We also found that the College needed to improve its effectiveness for monitoring and evaluating the Criminal Offender Record Information (CORI) and Sexual Offender Record Information (SORI) background checks performed prior to, and during, an individual's employment or acceptance into a specific academic program at the College.

Our review of IT management and control indicated that management was aware of the need for internal controls and had an appropriate and defined organizational structure for the IT Department with assigned reporting responsibilities and documented job descriptions for IT staff. The College also had documented IT strategic and tactical plans that address QCC's IT environment and the Jenzabar application. With respect to the use and the safeguarding of information technology, we determined that formal policies and procedures were in existence, but needed to be updated to more accurately reflect the current IT environment for physical security, environmental protection, management and control over IT resources, and system access security. Having appropriate and well-documented policies and procedures increases the likelihood that desired control practices will be adequately communicated, administered, and enforced. In addition, QCC needed to develop and implement policies and procedures for business continuity planning.

With respect to physical security, we found the College could not provide reasonable assurance that computer equipment was safeguarded from unauthorized use, damage, loss, or theft. Our audit did reveal, however, that certain physical security controls were in place regarding QCC's buildings that house the data centers, computer labs, selected telecommunication closets, and the off-site storage location. Visitors are escorted when accessing the data centers reduce the risk of damage and/or theft of computer equipment. Our review of selected areas housing workstations disclosed that on-site Campus Police make periodic rounds nightly to verify that all office doors are locked and that all campus buildings are secure. However, we found that former employees at QCC were never required to turn in

their brass key sets. As a result, the potential exists for unauthorized access into restricted areas. In addition, documentation of stated control practices with respect to policies and procedures for physical security needed to be enhanced to more accurately reflect the current IT environment for physical security.

We determined that adequate environmental protection controls were not in place to ensure that IT operations were providing a proper environment to safeguard IT equipment located in QCC's data centers and selected telecommunication closets. However, we found that adequate environmental protection controls, such as fire prevention and detection controls, smoke and fire detectors and alarms, as well as fire extinguishers, were in place throughout the QCC campus. In addition, we found that an uninterruptible power supply was in place for the data centers, computer labs, and selected telecommunication closets housing IT resources to help prevent damage to, or loss of, computer equipment. However, environmental protection controls need to be improved to alleviate excessive heat and humidity issues within the data centers as well as three of the four-telecommunication closets reviewed. The audit team also determined that the data centers did not have an automatic fire-suppression system, water alarms, raised floors, or adequate general housekeeping procedures. In addition, documentation of stated control practices with respect to policies and procedures for environmental protection needed to be enhanced to more accurately reflect the current IT environment.

With regard to access security controls, we reviewed the existence and adequacy of policies and procedures regarding network security and IT security management. With respect to logon ID and password administration, we determined that adequate controls were in place to provide reasonable assurance that the College had granted access privileges and activated user access for authorized persons. Appropriate procedures were in place regarding authorization to access network resources and activation/deactivation of access privileges. The employee's manager assigned access levels to staff based upon job duties. Staff were required to sign a formal security statement regarding password protection and confidentiality. According to IT management, the security administrator periodically reviewed security logs, including access logs. However, Jenzabar application and campus network domain user accounts were found to be active for individuals no longer employed by QCC. We noted that a number of these individuals had been separated from the College for over three years. Our audit also revealed that documentation of stated control practices with respect to policies and procedures for monitoring user privileges needed to be enhanced. Although we did not review network security, QCC would benefit by an in-house evaluation of firewall and port management controls.

Our audit revealed that QCC could not provide reasonable assurance that the system of record for computer equipment, with a listed value of $2,544,218, could be relied upon, since a complete annual

physical inventory and reconciliation was not being performed to assist in verifying the accuracy and completeness of the inventory record. The absence of a reliable inventory of computer equipment hinders QCC's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives. Our data analysis of the entire population of 2,744 IT hardware items indicated that there were no missing fields of information with respect to asset number, location, model and serial number, and value. However, we found that 126 IT purchases made during fiscal years 2005 and 2006 were not included in the inventory system of record and our inventory test of 212 items, totaling $405,430, indicated that 33 pieces of computer equipment, totaling $63,481, that were listed on the inventory record could not be located. An additional test of 43 hardware items, traced from multiple physical locations back to the inventory listing, indicated that all of the information regarding the items description, tag, serial number, and location from the selected items was the same as the information on the inventory list. Also, our inventory test of 58 notebook computers and 29 video projectors indicated that all the equipment could be found.

Regarding surplus property and equipment, our audit revealed that QCC was aware of, and in compliance, with Operational Services Division's policy and procedures regarding surplus computer equipment. Although QCC's internal control policies included control and reporting requirements set forth in Chapter 647 of the Acts of 1989, our audit revealed that the College had not complied with the requirements of Chapter 647 of the Acts of 1989 since QCC had failed to notify the Office of the State Auditor of approximately $13,366 of missing or stolen computer equipment during fiscal year 2005.

Although we determined that procedures regarding the generation of back-up copies of magnetic media and the storage of the back-up magnetic media at secure on-site and off-site locations were adequate, our review indicated that the level of disaster recovery and business continuity planning needed to be strengthened. We found that there was a general absence of documented plans to address disaster recovery and business continuity for automated operations. Our audit disclosed that the College did not have a comprehensive disaster recovery and business continuity plan to provide reasonable assurance that mission-critical and essential data processing operations for administrative and academic functions could be regained effectively and in a timely manner should a disaster render automated systems inoperable or inaccessible. We also found that although an alternate processing site had been selected, user area plans had not been established to document the procedures required to regain business operations in the event of a disaster.

Regarding IT-related contracts with third-party vendors, we found that the College exercised adequate management oversight to hold contracted parties sufficiently accountable for their performance. Regarding contract documentation for our selected test sample, we found that all vendors were listed with

the Secretary of State's Office, Massachusetts Higher Education Consortium (MHEC), and Colleges of Worcester Consortium, Inc. (COWC); and therefore QCC was not required to go through the bidding process. In addition, 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. However, the College needed to have vendors more accurately document their deliverables in order to adequately measure results against the accepted stated goals of the contract and to complete established initiatives within scheduled timelines. In addition, we also determined from our testing of QCC's budget reports that QCC made overpayments on four contracts totaling $13,724, or 3.7%, of the College's overall total contract expenditures. We recommend that the College more closely monitor IT contract deliverables and maximum contract amounts.

Our audit revealed that QCC was conducting CORI background checks for prospective permanent employees, volunteers, and students. Although QCC's Academic Policies and Procedures require that ". . . SORI (Sexual Offender Registry Information) background check is required of all students accepted into the [Nurse Education Department] program," none was done during our audit period. In addition, based on our audit testing, we concluded that CORI and SORI checks were not performed on a consistent basis. We determined that QCC did not require that CORI or SORI background checks be performed for contracted employees in positions that involved the potential for unsupervised contact with children, the disabled, or the elderly.

AUDIT RESULTS

1. System Access Security

Our audit of the Quinsigamond Community College (QCC) revealed that system access security over the College's mission-critical Jenzabar application, accessed through the campus local area network (QCC network), needed to be strengthened to ensure that only authorized users have access to QCC's application systems and data files. We found that although adequate procedures were being followed to authorize and activate user privileges to the College's automated systems, controls regarding timely deactivation of user accounts and the degree of documented access security policies and procedures needed to be strengthened.

Regarding authorization, we determined that control procedures granting users access to the Jenzabar application system were generally adequate. We found that QCC had an established process for authorizing new employees to access the Campus Network and Jenzabar application. The documented procedures indicated that the IT Division would be notified by the Human Resources Department (HRD) of new employee hiring together with information regarding the individual's position and assigned department. Based on this input, which is deemed as authorization for system access, the IT Department establishes e-mail and login accounts for the new users. If the new employee were a Jenzabar application user, the IT Department would assess the user's system needs, assign a security class, and configure an appropriate level of access to the Jenzabar application system. Regarding password administration, the College had written procedures in place for the requesting, approval, and assignment of new passwords for all automated systems and had required users to complete an "New Account Request Form" in order to be assigned a user ID and password. We determined that QCC management and the network system default required a mandatory timeframe for changing passwords and limited the number of invalid access attempts to three. We also found written procedures in place and in effect to identify, log, or investigate terminal access violations.—

With respect to procedures to disable or remove access privileges from the system, our audit revealed that the College had no written policies and procedures in place to provide reasonable assurance that the Human Resources Department would notify the IT Department when access privileges should be deactivated for users no longer authorized or needing access to the mission-critical Jenzabar application and QCC network.

We obtained the computer system access lists for the Jenzabar application and QCC network and compared the lists against QCC payroll listing, dated February 24, 2006. Our audit tests concerning the Jenzabar application indicated that of the 298 authorized users, 58 (19%) were individuals no longer

associated with the College, some for over 36 months. Our audit test concerning the QCC network indicated that of the 877 authorized users tested, 234 (27%) could not be associated with current personnel, some dating back to 1999. The 234 unidentifiable users included 139 individuals no longer with QCC and 95 generic user accounts that did not have an associated identifiable person. Because 11 individuals had an active combination of the Jenzabar application and QCC network access after separating from QCC, unauthorized additions, modifications, or deletions of critical data files (i.e., student billing balances) could have occurred. The failure to deactivate user accounts in a timely manner also places the College at risk to unauthorized use of established privileges (using another individual's user account having higher access privileges) or to unauthorized access.

Our audit revealed that 15 employees (83% of the IT Department) had supervisory (super-user) capability with unlimited access to files, applications, and operator commands. The high percentage of super-users may create a security environment with increased vulnerabilities and risks of improper changes to data files to the Jenzabar application and program changes to QCC's network. Access to computer systems, program applications, and data files should be authorized on a need-to-know, need-to-perform, as well as a need-to-protect basis.

To ensure that only authorized access privileges are maintained, the HRD and department heads should notify the IT Department in a timely manner of any changes in the individual's status that could impact the user's level of authorization and access privileges. For example, as soon as the College is aware, either at the HRD or department level, of a change in employee status that would impact an employee's authorized access to application systems or IT resources, the IT Department should be notified so that prompt modification, or deactivation, of access privileges can be made. Our review indicated that there were procedures for the initial authorization to activate new accounts, but that policies were not in place to inform the IT Department of changes in employment status, including terminations. As a result, critical information on QCC's automated systems may have been vulnerable to unauthorized access, modifications, or deletions.

Generally accepted computer industry standards dictate that IT resources be made available to only authorized users and that resources be used for only authorized purposes. To help ensure that only authorized users have access to IT resources, appropriate controls need to be implemented to prevent and detect access to restricted systems by unauthorized individuals. 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. QCC's control practices include formal procedures to ensure that authorized users are granted access privileges to automated systems and assigned logon IDs and passwords. However, QCC needs to implement controls to ensure that access privileges for

unauthorized users are modified, disabled, or deleted from the system when there is a change in the employee's status. The notification process and subsequent actions should be formalized to reduce the risk that access privileges become inappropriate or unauthorized. Controls should be in place to monitor user access accounts and to detect unauthorized access to IT resources. Appropriate corrective controls should be in effect to mitigate risks of unauthorized access. Overall, monitoring and evaluation mechanisms should be in place to provide assurance that control practices are in effect to address control objectives. Access security controls are also necessary to meet risks associated with technological environments, including the Internet.

Recommendation:

With respect to authorization of users having access privileges to automated systems, QCC should review all persons with access to its mission-critical Jenzabar application and QCC network to ensure that they are currently employed and that their privileges are appropriate for their assigned responsibilities. In addition, the security administrator and department heads should periodically review access to automated systems and verify that only appropriate access privileges are granted. QCC should minimize the number of super-users to only those employees with the appropriate delegation of authority.

With regard to deactivation of logon IDs and passwords, QCC should implement formal procedures and develop a standard form whereby the HRD or department heads notify IT Department personnel responsible for access security of changes in employee status, such as terminations, extended leaves of absence, or employee transfers. Documented control practices should include procedures for the timely notification of changes of employment status to IT Department staff. Once notified of the change in employment status, IT Department staff should immediately modify, disable, or remove the logon ID and password. Appropriate staff should be instructed regarding compliance with these policies and procedures. After the policies and procedures are formally documented, all appropriate standards, policies, and procedures should be forwarded and explained to all responsible employees.

Auditee's Response

> *The College agrees with the recommendation regarding system access security. The College has already taken action to remove employees that are no longer considered affiliated with the College. Further, the College will formalize the exit process and begin training supervisors in proper exit procedures for employees. As a result of the audit the College has re-written the system access policy to include reference to eligibility requirements for special employees as well as time tables for the periodic termination of the accounts. The policy is currently being applied in a provisional manner and is moving through the governance process for permanent adoption.*

The College also agrees with the finding regarding the level of access permissions assigned to information technology staff members. This practice evolved due to low staffing levels and the need to distribute functions amongst Information Technology Staff. As a result the College has begun a functional reorganization that will restrict full system access to a small core network administration group. To address the workload shift created by this reorganization the department is adding additional information technology staff.

Auditor's Reply

We are pleased that the College will take steps to improve controls for system access security, including the action taken to remove employees who are no longer affiliated with the College. System access security controls will be enhanced by formalizing the communication process between department heads and HRD of changes in employee status and the training of supervisors in proper exit procedures for employees. Re-writing the system access policy to include reference to eligibility requirements for special employees will also enhance access security controls.

With regard to the setting of timetables for the periodic termination of accounts, we recommend that employees' accounts be disabled or terminated at the time employees change departments or leave QCC. Limiting the level of access permissions assigned to information technology staff members will also reduce the College's risk. Furthermore, once the College has formally documented access security policies and procedures, we suggest that QCC periodically review them to continually meet the needs of changing IT environments and risk management objectives.

2. Criminal Offender Record Information and Sexual Offender Record Information Background Checks

Our audit revealed that although QCC was conducting Criminal Offender Record Information (CORI) background checks for prospective permanent employees, volunteers, and students, the College was not performing CORI background checks for certain current or contracted employees. We also determined that Sexual Offender Registry Information (SORI) background checks were not being performed, as required by QCC's academic policies and procedures.

Although not specific to QCC, Massachusetts Community Colleges are to refer to the Massachsuetts' Executive Office of Health and Human Services (EOHHS) for their administration of the College's Criminal Offender Record Information Process. For example, EOHHS regulations requires applicants who are hired to fill positions that could create the potential for unsupervised contact with children, the disabled, or the elderly be required to undergo a CORI background check. During our audit, we requested, but QCC could not provide, a listing of all contracted personnel currently employed at the College. However, we were advised by the College that contracted employees were performing work in

and around QCC's daycare facility. We determined that QCC procedures do not ensure that background checks of these contracted employees hired for certain positions of special trust and responsibility, such as those with the potential for direct contact with children at the College's day care facility, are ever completed.

Although CORI background checks are performed on applicants being offered a position with the College, similar checks are not performed when an employee transfers to another position within the College. The new position could be one that a new CORI background check might find unsuitable for the employee. Our audit test determined that from a statistical sample of 38 faculty, administrators, and staff employed by QCC, 19 did not have a CORI background check performed. Further analysis revealed that a total of 166 individuals fell into the category of never being required to have a CORI background check performed. We determined that those individuals hired before the law took effect were "grandfathered" in and were not required to have a CORI background check performed. In addition, accepted standards suggest periodic background reinvestigations should be performed at least once every five years, consistent with the sensitivity of the position. However, College officials have not assigned different levels of sensitivity to job positions and have not performed reinvestigations.

Our audit also revealed that that the College did not perform SORI background checks as required by QCC's academic policies and procedures. Although QCC's senior management asserted that CORI background checks would identify any SORI convictions, we found that the CORI and SORI databases are not currently linked. The CORI background check only provides relevant information regarding convictions in Massachusetts and does not include any crimes committed in another state. For example, an individual convicted of a rape in New Hampshire, who subsequently moved to Massachusetts and as required by law registered as a sex offender, would go undetected on a Massachusetts CORI background check. In addition, Chapter 6, Section 178I, of the General Laws, states that 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 Sex Offender Registry Information from the Sex Offender Registry Board. The College risks not being able to detect unacceptable employee actions when CORI and SORI background checks are not performed for individuals who have the potential for unsupervised contact with children, the disabled, or the elderly.

Recommendation:

We recommend that the College ensure that a CORI background check be completed for any contracted employee who has or could have the potential for unsupervised contact with children, the disabled, or the elderly. In addition, QCC should put in place proper monitoring and evaluation procedures to ensure that QCC is in compliance with its adopted EOHHS regulations. We also recommend that QCC perform an updated CORI background check on an employee who transfers to another position within the College that may require unsupervised contact with vulnerable individuals. Completion of an updated CORI background check would include any offences that occurred after employment that might preclude an individual from candidacy for a new position. Lastly, QCC should perform SORI background checks for specific individuals as outlined by state law and QCC's academic policies and procedures.

Auditee's Response

The College agrees with the audit team and has begun to strengthen our CORI/ SORI procedures. Based on the audit recommendation, the SORI process was instituted for all students in Healthcare and Early Childhood effective September 2006. The CORI process was already in place. All Healthcare and ECE students have CORI and SORI checks done at a minimum, annually.

The College will begin a process by which those longer serving College employees who were previously "grandfathered" through the system as a result of being hired prior to 1999/2000, will now be required to undergo a CORI review should they transfer into an area of the College in which contact with so called "vulnerable populations" is a regular aspect of the job. Additionally current employees of the College working in such sensitive areas will be required to undergo CORI review every five years.

A statement to vendors and potential bidders has been added to the College's Purchasing website: Prior to commencing services, a vendor (or successful bidder) may be required to certify in writing that it has conducted criminal record and sex offender background checks through the Commonwealth's Criminal History Systems Board and Sex Offender Registry Board, respectively, for all employees, subcontractors or agents of the vendor (or successful bidder) who will be providing services to the College where they may have direct and unmonitored contact with children. The vendor (or successful bidder) further certifies that no individual with a criminal record or a classification as a registered sex offender shall be permitted to provide services at the College under this Agreement without the vendor (or successful bidder) first disclosing such record or classification to a designated representative of the College. The College reserves the right to reject any employee, subcontractor or agent of the vendor (or successful bidder).

All Requests for Proposals (RFPs) which the College sends to potential service vendor bidders will include the above statement. All Purchase Orders and Service Contracts generated by the College will incorporate the above statement into its "Terms &

Conditions". Child Study Center staff will be notified whenever contract vendors are to be scheduled to provide services in and around the Child Study Center.

Auditor's Reply

We are pleased that the College concurs with the finding for the CORI/ SORI procedures. We acknowledge that the SORI process was instituted for all students in Healthcare and Early Childhood effective September 2006 and that the College will begin a process to review "grandfathered" employees in the system as a result of being hired prior to 1999. In addition, we believe requiring employees to undergo a CORI review should they transfer into an area of the College in which they could have contact with "vulnerable populations" will help minimize risk and exposure to the College. We are also pleased that the College will ensure that all contracted employees that may have direct and unmonitored contact with children will have criminal record and sex offender background checks completed before providing services to the College.

3. Disaster Recovery and Business Continuity Planning

We determined that QCC's IT Department had established a Disaster Response Procedures (DRP) document, dated September 2003. However, we found that it did not include a comprehensive business continuity and contingency planning strategy. Although the IT Department had on-site and off-site storage of backup magnetic media available for recovery efforts and provisions for using QCC's satellite location for minimal alternative operations, the College had not formalized an agreement with an alternate processing site that would be available to regain computer operations should the data centers be damaged or inaccessible for an extended period of time. While QCC management had informally assessed the relative criticality of their automated systems, we found that QCC had not outlined a comprehensive approach to ensure the continuity of essential services in the event of a disaster. If a disaster should occur, there are no contingency plans developed by departments to address critical functions throughout the College. As part of QCC's DRP, there was a section on risk assessment that lacked a level of specificity to determine the extent of potential risks and exposures to IT operations and scenarios. Although QCC identified the cost of recovering the systems, the amounts should be updated and the risk analysis should identify the relevant threats that could significantly degrade or render the systems inoperable or inaccessible, the likelihood of the threat, and frequency of occurrence for each disaster scenario. Additionally, QCC had not completely documented the necessary tasks and responsibilities for all relevant QCC 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 Jenzabar application

that is supported by the IT Department might not be restored within an acceptable period of time, thus jeopardizing essential College operations.

Without a comprehensive, formal, and tested recovery and contingency plan, the College's ability to regain mission-critical processing capabilities and access to information related to its various application systems would be impeded. Business continuity and contingency planning has assumed added importance given the potential processing disruptions that could be caused by man-made events. Further, the College had not implemented or tested a formal business continuity plan for a timely post-disaster restoration of mission-critical business functions processed through the local area network servers or the applications residing on the workstations.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions should a disaster cause significant disruption to computer operations. Generally accepted practices and industry standards for computer operations support the need to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops and maintains appropriate contingency and recovery plans.

An up-to-date effective disaster recovery plan should provide specific instructions for various courses of action to address different types of disaster scenarios. The plan should identify the manner in which essential services would be provided without full use of the data processing facility or network communications and, accordingly, the manner and order in which processing resources would be restored or replaced. 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:

The College should update its DRP and formally assess the criticality of automated systems to identify application priorities and critical resources. An analysis should be conducted to identify in detail the risks and exposures relating to QCC's data processing operations and computer environment. The College should identify potential processing alternatives and resources to be used should a disaster disrupt its data processing or business operations. Based upon these results and input solicited from management and user departments, a written disaster recovery and business continuity plan should be developed, reviewed, and tested to the extent possible, and approved and implemented by senior management.

Senior management should ensure that a written business continuity and contingency plan is developed containing, at a minimum, guidelines on how to use the continuity plan consisting of emergency procedures to ensure the safety of all affected staff members; response procedures designed to regain IT processing capabilities to a required level; procedures to safeguard and reconstruct the primary site; coordination procedures with public authorities; communication procedures with stakeholders (employees, key customers, critical suppliers, and management); and critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media.

QCC should develop procedures to ensure that the criticality of systems is periodically reassessed; that the impact of changes in user needs, automated systems, or the IT environment is evaluated; and that staff is adequately trained in executing recovery plans. Upon a major change to systems or equipment, or at least annually, the disaster recovery plan should be reviewed, updated, and tested to ensure that it is current, accurate, and complete, and remains viable. The business continuity plan, or specific sections of it, should be distributed to appropriate personnel and a complete hard copy and electronic copy of the plan should continue to be stored in a secure off-site location.

Auditee's Response

> *The audit confirmed a weakness in the College's business continuity/disaster recovery procedures. The College agrees and is committed to addressing this critical weakness as best our resources will allow.*
>
> *The College has already begun a campus-wide discussion to update the disaster response/business continuity procedures and develop alternatives to maintain basic business function should a crisis or outage occur. This includes discussions with our ERP vendor (Jenzabar) for assistance with a risk analysis of all business functions as they relate to that system. The College is also pursuing a collaborative agreement to provide an alternate data center location.*

Auditor's Reply

We are pleased that the College is conducting campus-wide discussions to update the disaster response/business continuity procedures and developing alternatives to maintain basic business functions should a crisis or outage occur. After the plan's completion, it should be reviewed and updated annually, or whenever there is a significant change to the processing requirements, risks, or changes to the College's IT infrastructure. Designation of an alternate processing site and documented procedures for the generation and secure storage of backup copies of magnetic media are an integral part of any recovery strategy and should be documented, maintained, and appropriately monitored.

4. Inventory Controls over Computer Equipment

Our audit disclosed that inventory control practices over computer equipment needed to be strengthened to ensure that IT resources would be properly accounted for in QCC's system of record for property and equipment. We determined that adequate controls were not in effect to ensure that QCC was maintaining a current, accurate, and complete perpetual inventory record of computer equipment. We found that controls needed to be strengthened to provide prompt notification and update of the inventory record when equipment is relocated, disposed of, lost, or stolen. In addition, the inventory system of record did not appear to be adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation was not being performed. As a result, the integrity of the inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders QCC's ability to properly account for IT resources, evaluate the allocation of equipment, identify missing equipment, and meet IT configuration objectives.

Although we determined that the College had documented internal controls regarding the purchasing and receiving of IT resources, we found that documented policies and procedures needed to be enhanced regarding the maintenance, compliance monitoring, and reconciliation of the system of record for IT resources. For example, although documented procedures were in place requiring an annual campus-wide inventory to be conducted at the end of each fiscal year, we could not find documentation to support an annual physical inventory. Although the College had adequate policies and procedures for the disposal of surplus property and Chapter 647 reporting requirements, these requirements were not being followed. We found that QCC did not submit proper documentation to the Operational Services Division (OSD) regarding surplus equipment and did not submit required reports of stolen or missing items to the Office of the State Auditor (OSA).

We found that although the College's inventory record had certain fields of information including location, description, serial and tag number and cost, the system of record lacked data fields to properly account for IT-related computer equipment, such as condition and acquisition dates. The College should also include a data field for "condition of item" to support IT configuration management by noting the asset's status, such as being repaired, obsolete, or designated for surplus. The inclusion of this information will help ensure that the College's IT-related computer equipment will be properly accounted for during the College's annual physical inventory.

With respect to the recording of IT-related assets, we found that QCC lacked appropriate and adequate management oversight to prevent and detect errors in recording identifying data for received computer equipment into QCC's inventory system of record. Our tests indicated errors and inconsistencies in identifying data recorded by staff on QCC's computer hardware inventory listing.

Specifically, audit tests performed on 492 computer hardware items, valued at $523,181 selected from invoices during fiscal years 2005 and 2006, revealed that 126 items valued at $123,007 were not recorded on the inventory records. Because of the rate of data input errors, the failure to record asset costs and acquisition dates, and inadequate management of the system of record, an acceptable level of data integrity did not exist for QCC's inventory system of record for IT equipment at the time of our audit. The College needs to ensure that appropriate controls are in place for data entry and improve its monitoring and validating of information contained in the system of record to ensure the accuracy and completeness of the information contained in the inventory database.

QCC provided an inventory system of record that listed IT-related assets as of February 1, 2006 with a total value of $2,544,218. Our inventory tests were conducted against the 2,744 IT-related assets identified on the inventory system of record. Based on a statistical sample of 212 items of computer equipment, valued at $405,430, selected from the inventory record, we verified by inspection the existence and the recorded location of the computer equipment as listed on QCC's inventory record. We found that 33, or 16%, of the 212 items, valued at $63,481 that were selected from the system of record, were not at the locations indicated on the inventory record, including five items that could not be found by the College. However, we were also able to determine that 10 of the 33 sample items drawn from the system of record had been designated by QCC as obsolete property. Of the remaining 179 items from our sample of computer equipment that were recorded on the inventory, our test indicated that all the items were properly tagged, included correct serial numbers and manufacturer's identification, and were listed on the inventory with proper descriptions. Furthermore, to verify the accuracy and completeness of the inventory system for computer equipment, we randomly selected 43 additional items of computer equipment from floor locations and determined that all items were on QCC's system of record. In addition, our inventory test of 58 notebook computers and 29 video projectors indicated that all the equipment could be found.

Our audit further indicated that QCC's monitoring of IT equipment inventory needed to be strengthened. Specifically, QCC's senior management had not performed an annual physical inventory during our audit period and could not provide verification records for our audit period supporting any complete annual physical inventory or a reconciliation of IT-related equipment to QCC's inventory system of record. The absence of fully documented policies and procedures regarding inventory verification hindered QCC's ability to ensure the integrity of its inventory system of record as it pertained to IT-related assets.

Our examination of computer equipment that had been designated as surplus property indicated that QCC had not complied with Commonwealth of Massachusetts regulations for the disposal of surplus

equipment. Although adequate documentation was in place to support the initial request to obtain approval from the State Surplus Property Officer, the College did not submit the documentation to the OSD for approval as outlined in the Surplus Property policies and procedures manual. An audit test of 30 surplus IT items disclosed that ten items tested were still on the inventory listing, thereby overstating inventory valuations. We found that the College needed to enhance its documented policies and procedures regarding the steps to be followed in designating computer equipment as surplus and disposing of it. Our audit also revealed that QCC had not complied with Chapter 647 of the Acts of 1989 by failing to submit reports to the Office of the State Auditor of lost or stolen equipment. (Please refer to Audit Result No.3)

Recommendation:

To ensure that the inventory of IT resources is adequately maintained, QCC should strengthen its current practices to ensure compliance with policies and procedures documented in the Office of the State Comptroller's (OSC) "MMARS Fixed Asset Subsystem Policy Manual and User Guide," and its associated internal control documentation, and the OSD's guidelines regarding the accounting for, and disposal of, property and equipment.

We recommend that inventory control policies and procedures related to the receiving function should be enhanced by increasing supervision and oversight to help ensure that all items of computer equipment received are properly recorded on the College's inventory list in a timely manner and adequately safeguarded. The functions of receiving, tagging, recording, and distribution of assets should be segregated to reduce the risk of undetected data entry errors, unrecorded items, and loss of IT-related equipment. The College should enter all IT-related equipment on the inventory system of record when received, including cost and date of acquisition. A member of the IT staff should assist in the verification of equipment deliveries and the subsequent tagging of equipment.

The College should perform an annual physical inventory and reconciliation of its IT resources to ensure that an accurate, complete, valid, and current inventory record of IT resources is in place. We recommend that the inventory system of record be maintained on a perpetual basis and that it be periodically verified through reconciliation to physical inventory, acquisition, and disposal records. To maintain proper internal control, staff not responsible for maintaining the inventory system of record should perform the periodic reconciliation of computer equipment. We also recommend that QCC refer to the policies and procedures outlined in the OSC'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 items that have been transferred to surplus property, traded in for new equipment, or donated, should be deemed obsolete and deleted from the master inventory listing in a timely manner. In addition, the inventory responsibilities for recording, maintenance, disposition, and reconciliation of the inventory and configuration information should be assigned to provide appropriate segregation of duties and management review and oversight. We believe that it would benefit QCC to use a single inventory system to support inventory and IT configuration management requirements versus maintaining records in both the IT and finance departments.

With respect to IT configuration management, the data fields in the IT inventory should be expanded to include the condition and status of the IT resource. In addition, the College should consider including data fields that record information related to hardware or software maintenance and whether the IT resource is a core requirement for disaster recovery and business continuity planning. Furthermore, all IT resources should be included on the inventory to support IT configuration management objectives. 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 QCC to produce a complete record of all IT-related equipment on a perpetual basis. 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.

Auditee's Response

The College agrees with the recommendation that inventory procedures need to be strengthened. As a result of the audit the Information Technology department has scheduled the installation of the Arrival system that will allow us to incorporate bar-code readers into the acquisition and relocation processes. All staff with authority to move equipment will be assigned a device. Additionally, while the College does perform a full physical inventory of items defined as fixed assets (valued between $1,000 and $50,000) annually, an annual full physical inventory of information technology items under $1,000 has been adopted.

To date the 126 items noted as not being on the departmental inventory are in the process of being re-tagged and reconciled with the master departmental database. This oversight occurred during the transition of inventory of Information Technology related non-GAAP Fixed Assets to the College's master database.

We are now fully compliant with surplus property regulations. As discovered by the audit, although we had obtained approval from OSD before disposition of any item, we had failed to send the documentation into OSD indicating that this had been accomplished. Thanks to this finding we are now submitting this documentation to all the proper commonwealth agencies.

Auditor's Reply

We commend the actions initiated by QCC to improve inventory controls. We believe a single comprehensive inventory control system for all IT-related assets located throughout the College is an important component for the College's overall internal control structure. Strengthening inventory control procedures will improve the integrity of the system of record regarding computer equipment and assist the College in making IT infrastructure and configuration management decisions. We are also pleased with the College's compliance with OSD's regulations for the disposition of surplus property and that submitting documentation to all the proper agencies of the Commonwealth will help ensure quality in QCC's inventory system of record. We believe that controls to ensure adequate accounting of computer equipment will be strengthened by perpetually updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory to the system of record.

5. Noncompliance with Chapter 647 Reporting Requirements

Our audit disclosed that QCC did not comply with Chapters 647 of the Acts of 1989 during our audit period by failing to report to the OSA the thefts of four video projectors, four flat screen monitors, and one computer file server. Chapter 647 of the Acts of 1989, an Act Relative to Improving the Internal Controls within State Agencies, requires state agencies to immediately report unaccounted for variances, losses, shortages, or thefts of property to the OSA. Chapter 647 also requires the OSA to determine the internal control weaknesses that contribute to or cause an unaccounted for variance, loss, shortage, or theft of funds or property; make recommendations to correct the condition found; identify the internal control policies and procedures that need modification; and report the matter to appropriate management and law enforcement officials. The College did not report the following incidents to the OSA:

Item/Description	**Historical Cost**	**Date of Incident**
2 Infocus Video Projectors	2 @ $3,500 totaling $7,000	10/18/04
1 Infocus Video Projector	$2,400	10/20/04
1 Flat Screen Monitor	$379	11/02/04
1 Infocus Video Projector	$1,800	11/12/04
1 Flat Screen Monitor	$379	12/06/04
1 Acer Flat Screen Monitor	$379	12/22/04
1 Acer Flat Screen Monitor	$379	02/09/05

1 Computer File Server	$650	05/06/05
9 Items of Computer Equipment	**Approximate Total: $13,366**	

According to QCC, the thefts of the four video projectors, four flat screen monitors, and the file server occurred in separate incidents during fiscal year 2005. The primary contributing factor leading to the thefts was that QCC had placed the equipment in unlocked classrooms throughout the campus. The incidents occurred sometime after the last class ended and were reported missing the next morning to the Campus Police. QCC officials indicated that it was their policy at the time to leave specific computer equipment in an unlocked classroom so that faculty and students would have easy access to the classroom and the computer equipment during the day.

Chapter 647 of the Acts of 1989 requires that access to resources be limited to authorized individuals only, and that the restrictions on access to resources depend on the vulnerability of the resources and the perceived risks. The agency head is responsible for maintaining accountability for the custody and use of resources and assigns qualified individuals for that purpose. Interviews conducted with QCC staff indicated that although QCC's Internal Control Plan requires reporting such incidents, the plan had not been adequately implemented and executed by responsible College officials.

Generally accepted industry standards and sound business practices require that adequate controls be implemented to account for and safeguard fixed assets against loss, theft, or misuse. Chapter 647 of the Acts of 1989, states, in part, that "… the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that] periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts." Moreover, the OSC's "Internal Control Guide for Departments," promulgated under Chapter 647 of the Acts of 1989, notes that fixed assets should be accounted for per existing regulations, that they be safeguarded to ensure that they are being used as intended, and that a property officer be designated to manage QCC's inventory system of record.

Recommendation:

QCC should implement a comprehensive inventory control system that will comply with Chapter 647 of the Acts of 1989 and immediately report all instances of unaccounted for variances, losses, and thefts of funds or property to the OSA. The inventory control system should include control mechanisms for safeguarding and preventing future losses of IT resources.

Auditee's Response

We agree with the finding that there were gaps in the chapter 647 reporting procedures. During FY2005 the College strengthened controls to meet state standards regarding the Fixed Asset inventory. This included the strengthening of procedures related to chapter 647 reporting and as of March, 2005, all chapter 647 requirements have been met.

Further, as a result of this audit the College is strengthening the procedures associated with items not classified as fixed assets managed through departmental data bases. Prior to that time the general inventory data base had not been merged with the IT inventory data base and while stolen items were being reported to public safety the inventory manager was not always notified.

As a result of the audit procedures have been modified to ensure full compliance with chapter 647 reporting procedures.

Auditor's Reply:

We commend QCC's response acknowledging that there were gaps in the Chapter 647 reporting procedures and the College's actions to strengthen controls in order to meet the Commonwealth's standards regarding reporting requirements of lost or stolen equipment.

6. Physical Security and Environmental Protection

With respect to physical security and environmental protection, although we found certain controls in place at the data centers, classroom labs, business offices, on-site and off-site storage areas, and selected telecommunication closets, we found that physical security and environmental controls needed to be strengthened. We found that the College needed to strengthen controls over the maintenance of keys for all areas throughout the QCC facility. We also found that environmental controls for the areas housing the file servers and the telecommunication closets needed to be strenghtened.

With regard to QCC's key policy, our test of the list of 451 key holders disclosed that there were 155 individuals (34%) associated with 286 keys who did not appear on QCC's current payroll listing. We also found that the 155 individuals not on the payroll listing included 23 terminated employees, 18 of whom had 21 master keys that potentially allow key holders access to restricted IT areas. Lack of controls to enforce QCC's key policy for the return of keys from transferred or terminated employees increases the risk of unauthorized entry to restricted areas, including computer labs and telecommunications closets, that could result in the potential loss of the College's assets, including computer equipment and data.

Although QCC's Campus Police maintain policies that include provisions for checking physical security of the data centers, computer labs, and telecommunication closets, we found during our on-site walkthrough and subsequent observations of areas housing IT-resources, that the door to one of the data

centers located in the Administration building was not locked. We also determined that although visitors are escorted when entering the IT Department and data centers, there was no formal visitors log or listing of personnel authorized to access the data centers and other secure areas. Due to the absence of controls regarding physical security, we found that the College could not provide reasonable assurance that computer equipment will be safeguarded from unauthorized use, damage, loss, or theft.

We determined that adequate environmental protection controls were not in place to ensure that IT operations are providing a proper environment to safeguard IT equipment located in the College's data centers and selected telecommunication closets. Although the data centers that run the mission-critical Jenzabar application, campus network domain, and email system do not have an HVAC system, we found that each of the main data centers has a dedicated air conditioning unit located in the ceiling and two supplemental window air conditioners. During our walkthrough of the IT areas, we determined the temperature in one of the telecommunication closets registered at 92 degrees. We also found that there were battery operated temperature controls in two of the data centers that were not functioning and there were no humidity controls in any of the rooms inspected by the audit team.

We found that the data centers were protected by an uninterrupted power supply (UPS) and have handheld fire extinguishers, smoke detectors, and an alarm system, which notifies the Campus Police and QCC's fire and security company. However, we also observed storage of old obsolete equipment, cardboard boxes with old binders, and generally bad housekeeping in the data centers and wiring closets. Although there was a policy for no smoking and no food allowed in the data centers, there were no signs posted to reinforce the rule. We observed that the data centers did not have a raised floor, flood protection, water detectors, or sprinkler systems. In the datacenter housing the email system and Jenzabar application, there was a functioning sink that acted as a drain for the air conditioner. The audit team advised the CTO, who subsequently shut off the water supply. We determined that the overall environmental protection of the data centers was not adequate, thereby increasing the risk of damage to IT equipment that support the College's mission critical system and campus network domain.

Generally accepted computer industry practices indicate that appropriate physical security and environmental protection controls need to be in place to ensure that the information technology assets are operating in a safe and secure processing environment. Appropriate physical security and environmental protection controls also serve to protect employees or other persons from undue harm. Computer assets should be protected and properly safeguarded against loss or damage due to heat, humidity, water, or fire. The College should adopt appropriate physical security and environmental protection policies and procedures that require computer assets be protected from unauthorized access, use, damage, or theft.

Recommendation:

We recommend an immediate reconciliation of the brass key sets to current employees to ensure that appropriate access privileges have been granted. QCC should also attempt to retrieve keys from terminated employees or consider re-keying locks to designated secure areas. In addition, QCC should enhance the documented procedures for managing the brass key sets. The procedures should require periodic reconciliation of the brass key sets to current employees and a return of all keys upon employment termination. The College should also consider implementing an electronic keycard system for secure areas such as the data centers. QCC's senior management should update its Internal Control and Policy Manual to include policies and procedures regarding physical security and environmental protection of IT equipment housed in the data centers, telecommunication closets, and computer labs. Documented internal controls will help to ensure that QCC's IT equipment and related assets are properly safeguarded from unauthorized use, damage, loss, and theft. The College should perform an environmental protection risk assessment of the entire campus, and identify any and all potential threats and exposures to computer resources, including equipment, communication infrastructure, software, media, and proprietary documentation.

We recommend the College define and ensure that the staff has an adequate understanding of the control objectives regarding physical security and environmental protection. Policies, procedures, and responsibilities for physical security and environmental protection should be written, reviewed, approved, and distributed to all appropriate staff members. We also recommend that the College assign a single point of accountability regarding physical security and environmental protection for the data centers, wiring closets, computer labs, and off-site storage areas. The assigned responsibilities should be comprehensive, understandable, and properly communicated. The College should also establish adequate mechanisms to monitor and evaluate the effectiveness of physical security and environmental controls. Monitoring mechanisms should include formal reporting of lapses in security, adherence to established procedures, and identification of security problems and their resolutions.

QCC should also establish adequate controls to prevent and detect water damage regarding the data centers. In addition, QCC should install water detection devices and consider the installation of a raised floor within the data centers to help ensure the safeguarding and protection of the equipment. The College should also consider the purchase of plastic covers for critical IT equipment to help provide some level of protection against the risk of water damage from the floors above. We also recommend that the College conduct an inspection of all their computer labs to ensure that they all contain easily accessible fire extinguishers. To further support the safeguarding of equipment, we suggest that QCC maintain a

floor plan of the data centers and wiring closets indicating the location of equipment, power sources, and physical security and environmental protection controls.

Auditee's Response

The College concurs with the auditors finding regarding the physical security and environmental security. We are facing significant challenges in our existing facilities. Due to space restrictions we have had no alternative but to use the server rooms for limited storage and as a work room. The College is extremely concerned about the status of the datacenter environment as well as the inconsistent documentation of the brass key inventory. Equipment formerly stored in the datacenter has been removed and properly disposed of. The College is in the process of developing a bid for the consolidation of the three (3) server rooms into a single datacenter that will meet the NCPI (Network Critical Physical Infrastructure) guidelines for an organization of QCC's size. This issue has a high priority for the College. In the interim the College has consulted an engineer regarding the existing environmental systems in the server rooms. Specific actions are pending the report. The College is also planning to install key-card access to secure the main server rooms. The current Intrusion/Heat Alarm System will be updated to include water detection devices in the computer Data Center rooms.

A Building Access and Key Policy has been formulated and processed through the College Governance system and approved by the College Trustees, June 2005. This policy provides for the authorization of new keys assigned and for an inventory of all campus keys to be performed on an annual basis. Re-keying of strategic locations on campus will occur as a result of the audit findings. The College acknowledges the inconsistency in the implementation of the exit process and will begin training supervisors in proper exit procedures for all employees.

Auditor's Reply

We are pleased that the College concurs with the finding for physical security and environmental protection. Although we understand the significant challenges that you are facing in your existing facilities and the steps taken to utilize the server rooms for limited storage and workrooms, the overall housekeeping should be up to the standards for data centers and server rooms, since the data center contains the critical business functions for the College. We are also pleased that the key management policy has been formulated and processed through the College's Governance system, and approved by the College Trustees.