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. 2006-0200-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF CONTROLS OVER
INFORMATION TECHNOLOGY-RELATED ASSETS AT
MOUNT WACHUSETT COMMUNITY COLLEGE

July 1, 2003 through October 31, 2005

OFFICIAL AUDIT REPORT

FEBRUARY 28, 2006

TABLE OF CONTENTS

INTRODUCTION

Mount Wachusett Community College (MWCC) is a two-year Massachusetts institution of higher education offering over 40 associate degree and certificate programs, as well as adult basic education/GED programs, education and training for business and industry, and non-credit community service programs. The College, which was established in 1963, is a member of the Massachusetts State College System organized under Chapter 15A, Section 5, of the Massachusetts General Laws. The College's mission is to provide academic preparation for transfer to four-year institutions, career preparation for entry into occupational fields, developmental courses to prepare students for college-level work, job retraining, and lifelong learning opportunities.

Mount Wachusett Community College is governed by a Board of Trustees and is under the direction of the College's President. The Board of Higher Education provides additional oversight to each public Massachusetts higher educational institution to help ensure that state funds support measurable performance, productivity, and results. The College is accredited by the New England Association of Schools and Colleges. The College's main campus is located in Gardner, Massachusetts with satellite sites located in Leominster, Fitchburg, Orange, Devens, and Winchendon. The enrollment for fiscal year 2005 was 8,313 full-and part-time students. At the time of our audit, the College employed 623 full-time and part-time faculty, administrators, and staff members, and was supported by a fiscal year 2005 budget of $31,018,170.

The College's Information Systems and Services (ISS) Department supports MWCC's administrative and academic operations. The ISS Department comprises 12 staff members and a Vice President of Data Management and Institutional Assessment, who reports directly to the President. The ISS Department provides a range of services to assist and guide administrative and academic staff in the use of computer-based systems, Web services, print servers, IT security, and e-mail. The College's network is a 100% switch-based Ethernet that comprises Cisco, 3Com, and HP networking equipment. The Cisco Catalyst switch, to which 19 wiring closets located throughout the multi-campus network are connected, is the center of the gigabit backbone that was upgraded in 2004. Five uninterruptible power supply systems provide backup power for the ISS data center's 25 production and development servers that support the College's distance learning, academic curriculum, and administrative processing at the main campus in Gardner.

At the time of the audit, the College indicated that it had 1,353 computer workstations, including 137 notebook computers that were connected to the College's network. Virtual LANS are used primarily within the network to prevent and help isolate network connectivity issues,

separate students from faculty and staff, and add a level of security. College Internet connectivity is provided with one T1 line from the University of Massachusetts Information Technology Services (ITS) department, which functions as the College's Internet Service Provider. Access to the Internet is provided to student at labs and classrooms through Comcast Cable Internet Service. There are 450 computers with Internet access available for student use with open labs at the Gardner campus. In addition, the Gardner Campus has six wireless access points for use and is restricted through Media Access Control (MAC) address registration.

From an administrative perspective, IT systems are used to process the College's financial management, administrative, and student information activities. The Sungard SCT Banner system (Banner), a vendor-supplied software product, is the primary mission-critical system at the College area. The Banner modules being utilized by the College are Finance, SIS (Student), Human Resources, Payroll, Financial Aid, and Alumni. The self-service Banner modules used are Student, Advisor, and Prospect. The College uses the Fixed Asset Management Solutions (FAS) system to maintain its fixed-asset inventory.

The College's course management software is Blackboard. This system is hosted and maintained by Bridgewater Community College. The Distance Learning server, personal Web server, and streaming server are all connected to the campus network via the Internet. Support for the 100% online and formally supported Web-assisted courses is provided by two instructional technologists who report to the Dean of Distance Learning and Academic Computing.

MWCC also has access to and uses the State Human Resource Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS). The College uses both the HR/CMS and the Banner payroll module to electronically update MMARS and the Banner finance subsystem with payroll expense information.

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) examination of controls over computer equipment at Mount Wachusett Community College (MWCC) covering the period of July 1, 2003 through October 31, 2005. The audit, which was conducted from July 18, 2005 through October 31, 2005, consisted of a general control examination of the College's internal controls regarding accounting for and safeguarding of computer equipment. We examined the College's policies and procedures regarding the receiving, recording, accounting for, and disposition of computer equipment. We reviewed the College's inventory system of record for computer equipment for validity, accuracy, and completeness. In addition, we assessed controls regarding physical security and environmental protection over and within selected administrative offices, computer laboratories, and wiring closets located at the College's data center and main campus. We assessed the College's compliance with applicable laws and regulations regarding fixed assets of the Commonwealth. Based on a request by the College to review its disaster recovery plan, we reviewed the adequacy of controls regarding business continuity and contingency planning to ensure system availability and the generation and storage of on-site and off-site backup copies of magnetic media to assist in recovery efforts.

Audit Objectives

Our primary audit objective was to determine whether MWCC had adequate controls in place and in effect to provide reasonable assurance that the College's computer equipment would be properly received, accounted for, and safeguarded. We sought to determine whether MWCC's internal controls, including policies, procedures, practices, and organizational structures, provide reasonable assurance that the College's business objectives in the area of inventory control would be achieved. We evaluated whether undesired events, such as unauthorized use, loss, or theft of computer equipment, would be prevented or detected, and, if detected, corrected. In conjunction with our primary audit objective, we sought to determine whether MWCC had documented, approved, and implemented policies and procedures regarding the proper recording, accounting for, and safeguarding of computer equipment.

With respect to the College's adherence to applicable laws and regulations regarding fixed assets of the Commonwealth, we sought to determine whether MWCC's policies and procedures adequately described requirements to ensure compliance with inventory control procedure laws.

We evaluated compliance with Chapter 647 of the Acts of 1989 regarding requirements for reporting lost or stolen equipment to the Office of the State Auditor, and fixed-asset management regulations from the Office of the State Comptroller's "Internal Control Guide for Departments." We also reviewed policies pertaining to the accounting of assets, including Office of the State Comptroller's Memos 310, and 313A. In addition, we determined whether the College complied with 802 Code of Massachusetts Regulations (CMR) 3.00 titled "Disposition of Surplus State Property."

We sought to determine whether adequate physical security controls were in place and effect to restrict access to the College's data center and areas containing IT resources in order to prevent unauthorized use, damage, or loss of IT-related assets. Furthermore, we sought to determine whether adequate environmental protection controls were in place in these areas to prevent damage to, or loss of, computer equipment.

Regarding system availability, we determined whether adequate business continuity and contingency plans were in place to provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period should the automated systems be unavailable for an extended period. In addition, we determined whether MWCC had adequate control procedures for the generation and storage of on-site and off-site backup media to support system and data recovery objectives.

Audit Methodology

To determine our audit scope and objectives, we obtained an understanding of MWCC's mission, organizational structure, and primary business functions. We performed pre-audit steps, including interviewing certain College management and staff and reviewing the College's statutory authority and website. We gained an understanding of the primary business functions and the automated systems that support them. We reviewed selected IT internal control documentation, such as the College's IT risk assessment and IT policies and procedures. We determined whether documented, authorized, and approved policies and procedures had been implemented for the control areas under review. We determined whether the policies and procedures provided management and users with sufficient standards and guidelines to comply with statutes, regulations, and policy directives related to inventory control, physical security, environment protection, and disaster recovery and business continuity planning.

We interviewed management regarding internal controls for physical security and environmental protection over and within the data center housing, administrative offices, classrooms, and computer laboratories housing computer equipment. In addition, we interviewed

management regarding physical security and environmental protection for the network closets located throughout the College, and the on-site and off-site storage areas for backup media. We performed a preliminary walkthrough of the data center located at the Gardner Campus.

To determine whether computer resources were being properly accounted for, we first evaluated the degree to which MWCC had documented, authorized, and approved control policies and procedures for receiving, recording, monitoring, and disposing of computer equipment. We then assessed the degree to which the College's inventory system of record was readily available and contained data relevant to the accounting and management of IT resources. We reviewed fixed-asset reporting requirements for institutions of higher education required by the Office of the State Comptroller (OSC) as of February 2004, and determined whether the College had complied with the requirements. With respect to the receiving and recording of purchased computer equipment, we reviewed the adequacy of operational and management controls, including documentation of the College's segregation of duties and extent of management supervision over the receiving and recording of newly acquired computer equipment.

To identify and obtain the College's system of record for computer equipment, we interviewed the Vice President of Data Management and Institutional Assessment, Vice President of Administrative Services, and the Chief Information Officer. We obtained and reviewed both the College's inventory system of record of MWCC's fixed assets and an extracted spreadsheet inventory listing of computer equipment. The inventory listing of computer equipment as of July 18, 2005 contained 1,480 pieces of computer equipment valued at $2,015,570. We also assessed the degree to which the inventory record for IT resources would assist IT configuration management, and whether the existing inventory control policies and procedures addressed the requirements of the College.

We reviewed the data from the inventory list of computer equipment to determine whether the records contained adequate fields of information to identify and account for IT resources and support IT configuration management. To assess the degree of integrity of the information on the College's inventory system of record for computer equipment, we determined whether data within the 13 data fields was accurate and valid based on a sample of items drawn from the inventory system of record. We assessed the degree of completeness for the 13 data fields used based on a 100% review of the system of record for computer equipment. Additional fields were available in the Fixed Asset Management Solutions system (FAS) software to provide more comprehensive information regarding the assignment, identification, status, and configuration management of computer equipment, but were not being used at the start of our audit.

To determine whether computer hardware purchases in fiscal years 2004 and 2005 were accurately listed on the College's system of record for computer equipment, we examined the data recorded on the College's purchase orders and invoices and compared them to the data recorded on the inventory system of record. To accomplish this, we selected 385, or 100%, of the purchased and leased items for fiscal year 2004 and 2005 valued at $472,762 from the College's list of invoices for computer equipment and compared the information on each item's invoice to data contained in the inventory system of record.

To determine whether the College's inventory system of record was current, accurate, and valid, we used audit software to select a statistical sample of 75 computer items, valued at $91,188, from the 1,480 computer items appearing on the inventory listing. We verified, by visual inspection, the location and condition of the 75 computer items and compared the tag numbers attached to the item, serial numbers, description, manufacturer, and other identifying information from the data recorded on the system of record to the actual computer hardware on the floor. To further assess the integrity and completeness of MWCC's system of record for computer equipment, we selected 72 additional computer items in adjacent locations and, while conducting our visual inspection of these 75 computer assets, determined whether they were properly recorded on the College's inventory system of record.

To determine whether MWCC had appropriate control practices in place and in effect to account for and safeguard notebook computers, we interviewed staff from the ISS Department, Receiving Department, and the library. We requested and reviewed the College's documented policies and procedures for assigning and recording notebook computers. We also reviewed the control forms used by the College regarding compliance with policies for loaning computer equipment to faculty, staff, and, for short durations, students. Furthermore, we conducted an inventory test of MWCC's notebook computers, which included a review of 31 notebook computers for location, serial number, asset tag, manufacturer, condition, and description.

To determine whether the College's computer equipment was adequately safeguarded from loss, theft, and damage, we performed audit tests of the controls to prevent and detect unauthorized physical access to computer equipment. These tests included inspection of physical access controls, such as locked doors and alarms in the data center, selected administrative offices, classrooms, computer laboratories, and five of the 19 network wiring closets located throughout the College. We also evaluated controls for staff authorized to access the data center and network closets through interviews with management and a review of the authorized access list.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems) in administrative offices, classrooms, the data center, and selected computer laboratories. In addition, we reviewed environmental controls in the data center with respect to an uninterruptible power supply (UPS), emergency power generators, and emergency lighting. We reviewed general housekeeping procedures to determine whether only appropriate supplies and equipment were placed in the data center and network closets. To determine whether proper temperature and humidity controls were in place, we checked for the presence of appropriate dedicated air conditioning units in the data center. Further, we reviewed control procedures to prevent and detect water damage to automated systems and on-site storage for computer-related backup media.

Based on a request by College management, we reviewed MWCC's Disaster Response Plan (DRP), dated June 2005, and interviewed management to determine whether the College's application systems would be made available on a timely basis should the automated systems be rendered inoperable or inaccessible. To determine whether the College could regain mission-critical and essential operations in a timely manner should computer systems be unavailable for an extended time frame, we reviewed whether the College had performed criticality assessments of its application systems and whether risks and exposures to computer operations had been evaluated. We also determined whether a documented, comprehensive business continuity strategy was in place and whether an alternate processing site had been selected.

To determine whether controls were adequate to ensure that software and data files for business applications would be available to assist in recovery efforts should the automated system be rendered inoperable, we interviewed the Director of Networking Services responsible for generating backup copies of magnetic media. To determine whether backup copies of magnetic media were safeguarded and protected from damage or loss, we reviewed the adequacy of physical security and environmental protection controls at the on-site location by observation and the off-site location by interview. Furthermore, we reviewed control procedures regarding logs maintained for backup copies of magnetic media transferred to and returned from the off-site storage location.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted computer industry control practices, and auditing standards. Audit criteria used in the audit included management policies, procedures and control guidelines outlined in Control Objectives for Information and Related

Technology (CobiT), as issued by the Information Systems Audit and Control Association, in July 2000.

AUDIT CONCLUSION

Based on our audit at the Mount Wachusett Community College (MWCC), adequate control practices were not in place and in effect to provide reasonable assurance that computer equipment was properly accounted for in the College's inventory system of record. In addition, physical security and environmental protection controls needed to be strengthened to provide reasonable assurance that IT resources would be properly safeguarded and protected from damage, loss, or theft. Regarding the availability of systems, although MWCC had developed a rudimentary disaster recovery plan and had provisions for on-site and off-site storage of backup magnetic media, comprehensive recovery strategies needed to be developed, documented, and tested to provide reasonable assurance that business operations could be regained in a timely manner should automated systems be rendered inoperable or inaccessible.

Although Mount Wachusett Community College had appropriate policies and procedures for ordering, purchasing, and receiving IT equipment and had made a good effort to develop a framework for inventory control, adequate inventory controls were not in effect regarding the initial recording, reconciliation, and update of IT equipment information on the College's inventory system of record. Inventory control policies and procedures needed to be enhanced to ensure that the College's system of record would be properly maintained regarding computer equipment relocation, loss, or disposal. In addition, the College needed to properly monitor the system of record by performing appropriate reconciliations of computer equipment on hand and records of increases or reductions in IT equipment to the inventory system of record.

Our examination of MWCC's inventory system of record indicated that an acceptable level of data integrity did not exist for data records of computer equipment at the time of our audit. Although the College was using appropriate data fields, our tests revealed the 13 data fields used did not always contain complete or accurate information. At the time of our audit, there were 1,480 computer items, valued at $2,015,570, recorded on the College's IT system of record, dated July 18, 2005. Our review of the completeness of data recorded in the data fields for the population of 1,480 computer items indicated that required information was missing for up to 35% for tag numbers and 39% for purchase orders. Our review of the accuracy and validity of the system of record revealed that computer items purchased in fiscal years 2004 and 2005 were not all properly recorded on the inventory system of record. Specifically, we found the College was not correctly or completely entering data into the system of record to initially record and account for computer equipment.

Our test of 75 records randomly selected of the College's computer equipment to verify the items from the system of record to the actual item on the floor indicated that 25 items, or 33% of the sample drawn, could not be located as recorded on the inventory system of record. Furthermore, nine of the 25 items could not be located as of the end of our fieldwork. Our test of an additional judgmental sample of 72 items from various locations and traced back to the system or record indicated that 12 computer items, or 17% of the 72 IT items tested, were not recorded on the College's inventory system of record. In addition, the College could enhance information regarding the identification, status, and assignment of computer items, as well as assisting IT configuration management decisions by using additional data fields currently available in their system.

The College had documented policies and procedures for surplus and disposal of computer equipment as required in 802 CMR 3.00, "Disposition of Surplus State Property." Our review of records and supporting documentation for computer assets that were disposed of during the audit period revealed that MWCC had complied with the Commonwealth of Massachusetts regulations for the disposal of surplus property. However, the College's inventory system of record did not always clearly delineate the status of the equipment as active or inactive. Our review of the College's compliance with Chapter 647 of the Acts of 1989 regarding the reporting requirements for missing or stolen assets revealed that incident reports for missing or stolen computer equipment for the audit period were filed with the campus police and properly reported to the Office of the State Auditor.

Our audit test of notebook computers selected from a population of 137 items indicated that 31 notebook computers used in classrooms and the library for short-term use were readily locatable and were properly recorded on the College's system of record. However, based on the level of information recorded in the system of record and related documentation, we determined that controls needed to be strengthened to better record the equipment assignment and to monitor the use of notebook computers assigned to faculty and staff.

Although the College had certain physical security and environmental protection controls in place, we determined that physical security and environmental protection controls needed to be strengthened to protect computer equipment from damage, loss, or theft. Regarding physical security, we found the data center was located in a non-public area with locked and alarmed entry and exit points. In addition, cameras were installed at the entrances of all buildings, security checks were performed on a daily basis seven days a week, and logs were maintained of unusual events. However, we found that doors to the computer labs and classrooms containing computer equipment were often unlocked, and a list of staff authorized to access the data center and other

secure areas was not maintained. Regarding environmental protection, we found that fire extinguishers were installed throughout the College, and the data center was subject to separate temperature controls and an uninterruptible power supply to permit a controlled shutdown and prevent a sudden loss of data. However, environmental protection controls needed to be strengthened since the College did not have an automated fire suppression system, and the data center did not have an emergency shutdown switch or emergency lighting. In addition, although the College had a fire emergency plan in place, not all staff had received training in emergency procedures.

Regarding system availability, we found that the College had some elements of a disaster recovery plan, but did not have a formal and tested business continuity strategy for the timely restoration of business functions provided by automated systems. We found that a recently drafted version of the "Disaster Response Plan" needed to be formalized and strengthened to be used in the event that IT resources are rendered inoperable or inaccessible. Without sufficient business continuity planning, a possible long-term loss of the College's computer operations could hinder access to processing capabilities and electronic data needed to perform essential business functions. Although the College generated and stored backup copies of magnetic media at their on-site and off-site locations, an alternate processing site had not been designated, and the off-site storage location for backup media lacked adequate physical security and environmental protection controls to safeguard backup copies.

Subsequent to the completion of our audit, the College initiated corrective action on our initial conclusions and provided evidence of improvements being made to inventory control, physical security, environmental protection, and disaster recovery and business continuity planning. The College has initiated a complete physical inventory and reconciliation to the inventory system of record of IT resources and an evaluation of the data center and disaster recovery plan. The College should continue its initiative to address IT governance by further to developing and implementing a framework of IT controls and processes.

AUDIT RESULTS

1. Information Technology-Related Inventory Controls

Our audit disclosed that Mount Wachusett Community College (MWCC) needed to strengthen inventory controls over IT equipment to provide reasonable assurance that the College's computer equipment would be properly recorded and accounted for and that the inventory system of record would be monitored and maintained. Although we found MWCC had appropriate policies and procedures for ordering, purchasing, and receiving IT equipment, the College lacked formalized inventory control policies and procedures to ensure the integrity of the initial recording of computer equipment, adequate data maintenance, and the monitoring and reconciliation of inventory records. Furthermore, the College needed to establish detailed records on the assignment of notebook computers to faculty and staff.

Our review of MWCC's policies and procedures regarding inventory control over computer equipment disclosed that the policies were essentially general policy outlines and departmental duties that lacked specific procedural detail and guidance. Although the College was able to provide an inventory system of record for computer equipment with appropriate data fields available, we found that the inventory system was not maintained on a perpetual basis and did not provide an adequate level of complete and accurate information. In addition, the College did not take advantage of available data fields within the system of record to support IT configuration management

MWCC was able to provide us access in a timely manner to its complete computerized inventory system of record maintained on the College's Fixed Asset Management Solutions system (FAS). The College also provided us with a subset of the system, noting it to be the College's official system of record for computer equipment, dated July 18, 2005, containing 1,480 items valued at $2,015,570. Our analysis of MWCC's inventory system of record indicated that the College was using 13 of the 51 data fields available, including activity (status), purchase order numbers, cost centers, acquisition dates, descriptions (limited), current asset numbers, room location, building location, serial numbers, vendors, unit cost, model numbers, and manufacturer. However, the system of record did not use data fields for equipment condition, assigned user, operational status, disposal information, acquisition method (purchased, leased or donated), or maintenance status. These additional data fields, for example, would provide a more comprehensive, auditable inventory record of IT-related fixed assets. There are a number of data fields available through the FAS system that could be used to further ensure that

the College's computer equipment will be properly accounted for and to support IT configuration management.

With respect to the recording of computer equipment on the inventory system of record, our audit disclosed that data entry controls needed to be strengthened to ensure the complete and accurate recording of information for newly acquired computer equipment. We found that MWCC's documented policies and procedures did not describe the staff responsibilities for recording computer equipment received, specific information that should be entered into certain data fields, or the timeframe required for recording information on acquired computer equipment on the College's inventory system of record. As a result, essential identifying information needed for proper inventory control and to uniquely identify computer equipment was not accurately and consistently entered into the College's inventory system of record.

With respect to data completeness, our data analysis of the population of 1,480 hardware items disclosed that MWCC failed to fully record required information on its inventory system of record for all computer equipment. As indicated in the table below, we found that MWCC did not record unit costs for 7.7%, or 114 items of the computer equipment listed; purchase order numbers for 39%, or 585 items of the computer equipment listed; and asset tags for 35%, or 523 items of the computer equipment listed on the inventory system of record for IT resources.

Inventory Data Fields	Number of Items Missing Information in Data Field	Percent of Missing Information
Purchase Order	585	39.5%
Asset Tag	523	35.3%
Unit Cost	114	7.7%
Vendor	112	7.6%
Cost Center	45	3.0%
Manufacturer	39	2.6%
Acquisition Date	38	2.6%
Model Number	37	2.5%
Building	34	2.3%
Serial Number	28	1.9%
Room	19	1.3%
Description	10	0.7%

With respect to the recording of computer assets, we found that MWCC lacked appropriate and adequate management oversight to verify inventory records and prevent or detect errors in the recording of information pertaining to computer equipment in the College's inventory system of record. Our tests indicated that information was inaccurate for a significant number of data fields in the College's computer equipment inventory. Specifically, our audit tests comparing

data on invoices for computer equipment purchased during fiscal years 2004 and 2005 to the MWCC computer equipment listing detected 527 errors in 350 of the 385 hardware items tested. In addition, there were 35 pieces of computer equipment purchased during that period that did not appear on the inventory system of record. The following chart depicts the data fields reviewed and the number of instances where exceptions were noted.

Inventory Data Fields	Number of Items Lacking Accurate Information in Data Field	Percent of Inaccurate Information
Description	288	82.3%
Unit Cost	97	27.7%
Purchase Order	81	23.1%
Invoice Number	28	8.0%
Serial Number	19	5.4%
Cost Center	9	2.6%
Vendor	5	1.4%

Because of the rate of data input errors and inadequate management of the system of record, an acceptable level of data integrity did not exist for the College's inventory system of record for IT equipment at the time of our audit. The College needs to improve its monitoring of information contained in the system of record to ensure the accuracy and completeness of the information in the inventory system. Accurate, complete, and timely recording of information and monitoring of the system of record will help ensure that the College's IT resources are properly accounted for on a perpetual basis. Further, an appropriate level of management oversight, and detection and correction controls would help decrease the risk of data entry errors, unrecorded items, and loss or theft of IT equipment. By failing to record the proper information for computer equipment on the College's inventory system of record, MWCC was not in full compliance with the Office of the State Comptroller's fiscal year 2005 fixed assets requirements and Memorandum 313A.

During our audit, MWCC was unable to provide documentation supporting a physical inventory of computer assets and performance of a reconciliation of the physical inventory to the College's inventory records. MWCC's failure to document the maintenance, monitoring, and reconciliation of its inventory records added to the risk of unauthorized use, loss, or theft of computer equipment and to the risk that inventory-related data may become unreliable. The College could not provide documentation to verify that an annual physical inventory and reconciliation of its system of record for computer equipment had been performed for fiscal year 2004.

In our audit testing based on a statistical sample of 75 computer assets, valued at approximately $91,188, randomly selected from the inventory record that were compared to actual items of equipment located on the floor, we found that 25 out of 75 items, or 33%, could not be located within the College at the location recorded on the inventory. Subsequently, MWCC management was able to locate 16 of these pieces of computer equipment at other locations, presumably relocated from their initial installations. However, at the close of our audit, nine of the 25 pieces of computer equipment could not be located.

Our judgmental test of verifying 72 items selected from the floor from various locations at the College and traced to the inventory record revealed that computer items were not always recorded on the inventory list. We determined that 12 computer items, or 17% of the 72 items selected, were not recorded in the College's inventory system of record and that the inventory record contained incorrect data for 38, or 53%, of the 72 items tested. Based on our inventory test, we determined that monitoring controls need to be implemented to ensure that all computer equipment would be adequately accounted for and that an accurate and complete listing of computer equipment would be maintained.

Our audit disclosed that the College had complied with Chapter 647 of the Acts of 1989, which requires all departments to submit reports to the Office of the State Auditor regarding lost or stolen Commonwealth assets. In an interview with MWCC Campus Police personnel and in our subsequent review of campus security incident reports, we found evidence indicating that one of the College's computer assets had been stolen between July 1, 2003 and October 31, 2005 and was reported to the Office of State Auditor on February 7, 2005.

We determined that MWCC assigned notebook computers for use by faculty and staff without maintaining a control register of assigned notebook computers. Our audit test of notebook computers selected from a population of 137 items indicated that 31 notebook computers used in classrooms and the library for short-term use were readily locatable and were properly recorded on the College's system of record. However, our audit found that MWCC did not have adequate controls in place and in effect to monitor the assignment and use of notebook computers assigned to faculty and staff based on recorded information contained in the system of record and related supporting documentation. By improving controls over notebook computers, the College could reduce the risk of unauthorized use, loss, or theft of these assets.

Recommendation:

We recommend that senior management strengthen the College's documented internal control policies, procedures, and practices regarding inventory control of IT equipment in the

areas of recording and inventory verification to help ensure that computer equipment is adequately accounted for and that the inventory system is properly maintained. We recommend that more detailed policies and procedures be developed for recording asset information in the inventory system of record for newly acquired computer equipment.

We recommend that the inventory system be maintained on a perpetual basis whereby additions or deletions of computer equipment, or changes to information on individual computer equipment records, would be made in a timely manner. In addition, we recommend that the inventory records be periodically verified through reconciliation to computer equipment acquisition and disposal records and actual equipment on hand. We recommend that the College implement either cyclical physical inventories and reconciliation or perform an annual physical inventory of computer equipment and reconciliation. We further recommend that the College maintain supporting documentation of the physical inventory and reconciliation performed to the perpetual inventory system of record. To maintain proper internal control, staff not responsible for maintaining the College's system of record for fixed assets should perform the periodic reconciliation.

We recommend that the College consider expanding the information within the inventory system to include data fields that would better support management decision-making regarding IT configuration management.

With respect to notebook computers, we recommend that the College develop a centralized policy requiring staff and faculty who are assigned notebook computers to sign a user responsibility agreement. Procedures to support the policy should be documented and implemented to help ensure that the equipment is used for approved purposes and that appropriate security measures are taken to reduce the risk of loss or misuse of the equipment. We recommend that the College complete its ongoing effort to record and maintain more detailed information on computer equipment, such as notebooks, assigned to faculty and staff.

Auditee's Response

> *The College has reviewed and strengthened the College's inventory control procedures over IT equipment. The updated policies, procedures, and practices are currently being reviewed by the Inventory Control Quality Improvement Team. They do include more detailed steps for recording information in the FAS system.*
>
> *A full physical inventory was undertaken by the College in late August through September 2005. College IT equipment, at all college sites, was carefully inventoried and recorded. This information was loaded into the FAS system. An effort was also made to verify existing financial/accounting data currently in the*

system and add this information where missing. This data has also been entered into the FAS system. A review is currently being completed identifying any data fields still incomplete. Unused fields have also been activated for use in identifying IT configurations of all applicable technological equipment.

The Data Reconciliation effort is also identifying items which have been deemed surplus by the College. These items will be "deactivated" to ensure that the only items in the inventory marked "active" are those that were found in the physical inventory. Any required paperwork, that should have been completed to report surplus and/or missing items, will be prepared and submitted to the appropriate state agency.

The more complete and explicit inventory control policies and procedures also incorporate a clearly defined process for periodic reconciliation and back-up documentation management. From this point forward, a full physical inventory and data reconciliation effort will occur annually (scheduled for June, 2006). To ensure completeness and accuracy through the course of the year, inventory records will be reconciled quarterly by the Director of Facilities and Administration—a newly created position. This position is responsible for overseeing the inventory control process, procedures, and data support and records documentation systems and for assuring that the strengthened policies and procedures are followed through quarterly inventory reviews and reconciliations.

The College designated the Library as the distributor of laptops as "loaners" to faculty and staff. The ISS department is designated responsible for the oversight of permanently assigned laptops. A draft of a strengthened Laptop User Responsibility Agreement (URA) has been prepared for review and discussion with the Inventory Control Quality Improvement Team. In addition, the strengthened Inventory Control Policies and Procedures have been modified to make clear that all laptops loaned out, or permanently assigned, must have complete paperwork including signatures both at the point of sign out and return.

Auditor's Reply:

We are pleased that the College is taking steps to strengthen the integrity of the fixed-asset inventory system of record for IT resources and improve inventory control policies and procedures. Strengthening inventory control procedures will enhance resource knowledge for IT infrastructure management decisions. We believe that controls to ensure adequate accounting of IT resources, including laptop computers, will be strengthened by updating the inventory record when changes in status or location occur and then routinely, or on a cyclical basis, reconciling the physical inventory and records of acquisitions and deletions (trade-in, loss, obsolesces, etc.) to the system of record. Maintenance of a perpetual inventory, coupled with routine reconciliation, should also improve the detection and subsequent accounting for any lost, stolen, or surplus equipment.

2. Physical Security and Environmental Protection Controls

We determined that MWCC needed to strengthen physical security and environmental protection controls to provide reasonable assurance that computer equipment will be safeguarded from unauthorized use, damage, loss, or theft. Based on our review of documentation from the ISS Department and Campus Police, observation of physical sites and existing controls, and interviews with management and staff, we determined that policies and procedures were not adequately documented and that adequate physical security and environmental protection controls were not in effect.

We found that certain physical security controls were in place. Our audit disclosed that the data center and the network closets were located in non-public areas and that entry and exit doors were kept locked. We determined that the College has a central alarm system and also relies on intrusion detection and alarm for the data center. We found that the MWCC had surveillance cameras located at various locations throughout the College, operating 24 hours a day, providing a videotape of individuals entering and exiting the college buildings. We found that Campus Police maintained logs that included data on security patrols and reports of unusual events and unauthorized attempts to enter campus buildings. According to management, the buildings throughout the campuses were locked after normal business hours. Although the above controls help to safeguard IT resources, we found that other physical security controls were not in effect.

During our on-site observations of areas housing IT-resources, doors to computer labs and classrooms containing computers and overhead projectors were found unlocked. Moreover, there was no formal listing of personnel authorized to access the data center and other secure areas. In addition, ISS management did not maintain logs of all unusual events activities regarding the data center. Although the College had a written fire emergency plan in place, there was no indication that all staff had been trained in emergency procedures.

Our review revealed that there were certain environmental protection controls in place at the data center, such as air conditioning for areas housing the servers, fire extinguishers, and a thermometer. We also found that uninterruptible power supply (UPS) devices were in place to permit a controlled shutdown and to prevent a sudden loss of data. However, regarding environmental protection, we found that there were no documented policies and the procedures at the College and the data center did not have a sprinkler system; heat, smoke, and fire detection devices; an emergency shut off for the computer systems, emergency lighting, or a water detection device. For network closets, adequate environmental protection controls were in place at the locations reviewed on the Gardner Campus. Network closets were well maintained and properly secured.

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. Computer assets should be protected and properly safeguarded against loss or damage due to heat, humidity, water, or fire. Appropriate physical security and environmental protection controls also serve to protect employees or other persons from undue harm. The College should adopt appropriate physical security and environmental protection policies and procedures requiring that computer assets be protected from unauthorized access, use, damage, or theft.

Recommendation:

We recommend that MWCC's senior management strengthen the College's documented internal control policies, procedures, and practices regarding physical security and environmental protection of IT equipment in the areas of the data center, classrooms, and computer labs to ensure that the College'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 that the College define and ensure that there is an adequate understanding by all staff 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. MWCC needs to establish a single point of accountability for physical security as well as environmental protection. We also recommend that the College formally assign responsibility regarding physical security and environmental protection for the data center, classrooms, 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.

Our audit revealed that, although the MWCC had certain environmental protection controls in place within the data center, the environmental protection controls needed to be strengthened to adequately protect critical IT equipment. Specifically, although adequate air conditioning and temperature controls were in place, we recommend that controls to prevent or detect and correct

water and fire damage need to be addressed. Policies and procedures relating to environmental protection controls should be in place to provide an adequately controlled environment within which computer equipment can operate under appropriate conditions and to safeguard hardware and software from environmental damage due to extreme heat, fire, excess humidity, power outages, water problems, dust and dirt, and/or other environmental hazards. The College should implement and post-emergency procedures in the data center to help ensure staff safety in the case of an emergency. We also recommend the College document environmental problems and their resolution as well as adequate controls to prevent and detect water damage regarding the data center. In addition, the College should consider the purchase and installation of water detection devices within the data center 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. To further support documentation, we suggest that a floor plan of the data center be maintained indicating location of equipment, power sources, and physical security and environmental protection controls.

Auditee's Response:

> *The College has made short term control improvements, i.e. installing a unique lock set for all IT related entrances, that could be implemented within this budget year with existing resources; and, have identified improvement actions that will be implemented next fiscal year when the new budget is implemented. In addition, the College has reinforced its policy requiring all classrooms, labs and facilities holding IT assets remain locked when not in use.*
>
> *A list of employees with current access rights to the data center is being prepared and will be reviewed by Vice President of Data Management and the Executive Vice President for approval. The CIO will institute an entry and exit log for the remainder of this year to assure authorized personnel always sign in and sign out of the Data Center and that a record is always maintained of entries. The College is investigating the options of more stringent controls including an ID card entry system for the Data Center that maintains a computerized record of those who enter and exit, and surveillance cameras.*

Auditor's Reply:

We commend the initial actions being taken by the College to improve physical security controls throughout the College campus. We agree that certain security procedures and personnel are in place, however, certain controls for physical security should be implemented or improved for areas housing IT resources and equipment. The College should institute and

monitor any access policy to its data center. Improvements in physical security would enable the College to reduce the risk of damage to property, equipment, and records from vandalism or theft.

3. Business Continuity and Contingency Planning

We found that the College's business and ISS departments had not formulated a comprehensive business continuity planning strategy. Our review of disaster recovery planning disclosed that although MWCC had formulated a Disaster Response Plan, the plan lacked specific details and criteria to ensure timely restoration of the College's data and systems. Although the ISS Department had on-site and off-site storage of backup media available for recovery, the College had not identified, or formalized an agreement with, an alternate processing site to use to regain processing should the data center be damaged or become inaccessible for an extended period of time. Furthermore, College management had not fully assessed the relative criticality of their automated systems and had not conducted a risk analysis to determine the extent of potential risks and exposures to IT operations.

The risk analysis, once developed, should identify the relevant threats that could significantly degrade or render the systems inoperable, the cost of recovering the systems, and the likelihood of the threat and frequency of occurrence for each disaster scenario. Additionally, the tasks and responsibilities necessary to carry out the completion of the College's duties and business objectives under various disaster scenarios for all relevant College personnel had not been documented. As a result of the weaknesses noted, if a disaster were to occur that adversely impacted IT operations, the automated systems, including the Banner application, could not be restored within an acceptable period of time, jeopardizing essential college operations.

Without a comprehensive, formal, and tested recovery and contingency plan, the College's ability to regain critical processing capabilities and access information related to its various application systems would be impeded. Given the absence of comprehensive recovery plans, a significant disaster impacting the College's automated systems could seriously affect the College's ability to regain critical and important data processing operations. Further, the College had not implemented or tested a formal business continuity plan for a timely post-disaster restoration of mission-critical important business functions processed through the local area network servers or the application systems residing on the workstations.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions enabled by technology 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 appropriate contingency and recovery plans, if required.

An 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 ways 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 fully assess the criticality of its automated systems to identify application priorities and critical resources. An analysis should be conducted to identify risks and exposures relating to the College's data processing operations and IT environment. The College should identify potential processing alternatives and resources to be utilized 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, tested to the extent possible, approved by senior management, and implemented.

Senior management should ensure that the written business continuity and contingency plan developed contains, at a minimum, guidelines on how to use the continuity plan; emergency procedures to ensure the safety of all affected staff members; response procedures meant to bring the business operations back to their prior state or acceptable operational level before the incident or disaster; 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.

We further recommend that procedures should be developed 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 are 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 of the plan should be stored in a secure off-site location.

Auditee's Response:

> *SunGard Collegis, Inc., serving as Mount Wachusett Community College's outsource IT management agent, prepared the College's Disaster Recovery Plan. During the audit, Collegis representatives were asked (November 2005) to provide the College with a proposal identifying action steps and services that could be provided by SunGard Availability Services to help the College develop a more comprehensive and complete College Disaster Response Plan. This request included 1) the conduct of a risk assessment as a vital first step in the plan development process; and, 2) a project plan incorporating professional facilitation/templates for use by an institutionally appointed Disaster Response Team comprised of key College personnel charged with developing essential business continuity plans.*
>
> *The College will continue to pursue this project, formalizing a Scope of Work that incorporates the COBIT Standards and Guidelines, to ensure that the College's efforts also meet best practices as to IT Management criteria. The intention is to procure professional services to conduct a risk assessment and to provide facilitation to the members of the Disaster Response Plan Improvement Team. In addition, College ISS Management staff, upon the auditors' recommendation, is in the process of seeking an alternative back-up/restore processing site with other colleges and/or The Board of Higher Education.*

Auditor's Reply:

Documenting and testing comprehensive business continuity and contingency plans provide a strong basis for regaining mission-critical and essential IT and business operations within an acceptable period of time. Importantly, appropriate controls need to be exercised to also ensure the integrity and security of the system and related IT resources. Well-developed recovery strategies help diminish the time needed to recover processing and network capabilities. In addition to having a documented business continuity plan, the College should ensure that recovery strategies are formally reviewed and periodically tested to ensure their viability. Certainly, conducting a thorough risk assessment is a sound first step. The business continuity plan that is developed should address various disaster scenarios and clearly identify cooperative efforts necessary to assist in recovery efforts. Modeling a business continuity strategy by incorporating generally accepted disaster recovery and business continuity practices and CobiT

standards and guidelines should help ensure that all key elements of a comprehensive business continuity strategy are addressed.

Appendix

Mount Wachusett Community College

February 1, 2006

Mr. John W. Beveridge
Deputy Auditor
Office of the Auditor of the Commonwealth
One Ashburton Place, Room 1819
Boston, MA 02108

Dear Mr. Beveridge:

I am writing to formally respond to the audit recommendations presented in the ***Office of State Auditor's Report on the Examination of Controls Over Information Technology-Related Assets at Mount Wachusett Community College*** which was presented to me and the appropriate College staff on January 19, 2006. I would like to thank your staff for their professionalism and thoroughness in performing this review.

The State Auditors Office's IT auditing team's findings and recommendations are deemed by the College to be fair and accurate assessments of areas where the College needs to strengthen its controls over information technology related assets and initiate quality improvements. Mount Wachusett Community College has been actively reengineering its IT management infrastructure, operations, and policies and procedures. The State IT Audit provided great improvement insights and was a fortuitous tool in assisting the College in this reengineering and improvement initiative.

Committed to implementing a progressive, more proactive, and best practice Information Technology function and management system, College leadership worked collaboratively with the audit team and commenced corrective strengthening actions during the course of the on-site IT audit as auditors shared improvement needs and ideas with the institutional and IT management team.

The following represents the College's response to the ***Office of State Auditor's Report on the Examination of Controls Over Information Technology-Related Assets at Mount Wachusett Community College.*** Responses are provided for specific audit findings and recommendations. In addition, attached to this response is a detailed Project Plan developed shortly after the final exit interview with the auditors when the draft report with findings and recommendations was reviewed with college leadership.

The Project Plan presents a detailed action plan with objectives and follow-up tasks to be completed by year's end for many of the improvement actions already underway. This response narrative and the associated Project Plan demonstrate the institution's commitment to implementing the recommendations made by the auditing team and building a stronger and more effective IT oversight and management system.

The College has reviewed and strengthened the College's inventory control procedures over IT equipment. The updated policies, procedures, and practices are currently being reviewed by the Inventory Control Quality Improvement Team. They do include more detailed steps for recording information in the FAS system.

A full physical inventory was undertaken by the College in late August through September 2005. College IT equipment, at all college sites, was carefully inventoried and recorded. This information was loaded into the FAS system. An effort was also made to verify existing financial/accounting data currently in the system and add this information where missing. This data has also been entered into the FAS system. A review is currently being completed identifying any data fields still incomplete. Unused fields have also been activated for use in identifying IT configurations of all applicable technological equipment.

The Data Reconciliation effort is also identifying items which have been deemed surplus by the College. These items will be "deactivated" to ensure that the only items in the inventory marked "active" are those that were found in the physical inventory. Any required paperwork, that should have been completed to report surplus and/or missing items, will be prepared and submitted to the appropriate state agency.

The more complete and explicit inventory control policies and procedures also incorporate a clearly defined process for periodic reconciliation and back-up documentation management. From this point forward, a full physical inventory and data reconciliation effort will occur annually (scheduled for June, 2006). To ensure completeness and accuracy through the course of the year, inventory records will be reconciled quarterly by the Director of Facilities and Administration—a newly created position. This position is responsible for overseeing the inventory control process, procedures, and data support and records documentation systems and for assuring that the strengthened policies and procedures are followed through quarterly inventory reviews and reconciliations.

The College designated the Library as the distributor of laptops as "loaners" to faculty and staff. The ISS department is designated responsible for the oversight of permanently assigned laptops. A draft of a strengthened Laptop User Responsibility Agreement (URA) has been prepared for review and discussion with the Inventory Control Quality Improvement Team. In addition, the strengthened Inventory Control Policies and Procedures have been modified to make clear that all laptops loaned out, or permanently assigned, must have complete paperwork including signatures both at the point of sign out ***and*** return.

Physical Security and Environmental Protection

The College has made short term control improvements, i.e. installing a unique lock set for all IT related entrances, that could be implemented within this budget year with existing resources; and, have identified improvement actions that will be implemented next fiscal year when the new budget is implemented. In addition, the College has reinforced its policy requiring all classrooms, labs and facilities holding IT assets remain locked when not in use.

A list of employees with current access rights to the data center is being prepared and will be reviewed by Vice President of Data Management and the Executive Vice President for approval. The CIO will institute an entry and exit log for the remainder of this year to assure authorized personnel always sign in and sign out of the Data Center and that a record is always maintained of entries. The College is

investigating the options of more stringent controls including an ID card entry system for the Data Center that maintains a computerized record of those who enter and exit, and surveillance cameras.

Business Continuity and Contingency Planning

SunGard Collegis, Inc., serving as Mount Wachusett Community College's outsource IT management agent, prepared the College's Disaster Recovery Plan. During the audit, Collegis representatives were asked (November 2005) to provide the College with a proposal identifying action steps and services that could be provided by SunGard Availability Services to help the College develop a more comprehensive and complete College Disaster Response Plan. This request included 1) the conduct of a risk assessment as a vital first step in the plan development process; and, 2) a project plan incorporating professional facilitation/templates for use by an institutionally appointed Disaster Response Team comprised of key College personnel charged with developing essential business continuity plans.

The College will continue to pursue this project, formalizing a Scope of Work that incorporates the COBIT Standards and Guidelines, to ensure that the College's efforts also meet best practices as to IT Management criteria. The intention is to procure professional services to conduct a risk assessment and to provide facilitation to the members of the Disaster Response Plan Improvement Team. In addition, College ISS Management staff, upon the auditors' recommendation, is in the process of seeking an alternative back-up/restore processing site with other colleges and/or The Board of Higher Education.

In closing, I would like to thank you and your staff for considering our response in preparing your final report. I also appreciate the fact that this report can serve as a guide for further improvements in our IT operations. Our goal is to manage our IT operations in accordance with best practice criteria as outlined in the COBIT standards.

Please feel free to contact me if you have any questions or additional concerns regarding this issue.

Sincerely,

Daniel M. Asquino
President

Enclosure
copy: Frank Cintolo, Office of the State Auditor
Edward R. Terceiro, Jr., Executive Vice President, MWCC
Elaine Smith, VP of Data Management and Institutional Research, MWCC
Jane T. Gustowski, VP of Administrative Services, MWCC
File