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. 2005-0182-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE MASSACHUSETTS MARITIME ACADEMY

July 1, 2002 through March 10, 2005

OFFICIAL AUDIT REPORT

MAY 26, 2005

TABLE OF CONTENTS

INTRODUCTION

Massachusetts Maritime Academy (MMA), founded in 1891, is a four-year, undergraduate college that offers a curriculum leading to five degrees accredited by the New England Association of Schools and Colleges. The degree programs, which support career paths leading to job placements both at sea and ashore, are Bachelor of Science in Facilities and Environmental Engineering, International Maritime Business, Marine Engineering, Marine Safety and Environmental Protection, and Marine Transportation. Upon graduation, marine engineering and marine transportation students are qualified to take the U.S. Coast Guard Merchant Marine license examination for third-assistant engineer-steam and motor or third-mate oceans. In addition, the Academy offers part-time continuing education programs, such as training in the responsibilities and techniques of environmental protection and oil spill response management, fishery programs for pleasure and commercial fishermen, and a wide variety of community service courses. MMA is a member of the Massachusetts State College System and is regulated by Chapter 15A, Section 5, of the Massachusetts General Laws (MGL). In addition, a Board of Trustees provides oversight to the Academy's overall administrative activities which are under the direction of the Academy's President.

Massachusetts Maritime Academy's primary mission is to graduate educated men and women to serve the maritime industry as licensed officers or the transportation, engineering, environmental, and industrial interests of the Commonwealth and the Nation. The Academy supports national defense by the commissioning of officers in the U.S. Merchant Marine and the U.S. Armed Forces. The Academy is located in the town of Bourne on approximately 52 acres, adjacent to the Cape Cod Canal, where the Academy's training ship "Enterprise" is docked. The enrollment population for the 2003-2004 academic year was approximately 925 students registered in full-time day programs. At the time of our audit, the Academy employed 187 full-time and part-time faculty, administrators, and staff members and was supported by a budget of $9,758,080.

Massachusetts Maritime Academy's administrative and academic mission and operations are supported by automated services provided by the Academy's Technology Services Department. The Technology Services Department's role is to advance the mission of the Academy by providing innovation to the planning, design, and provision of high-quality information technology services to the campus. The Department is comprised of four sections: Academy Information Systems, Network Services, Support Services, and Simulator Systems. At the time of our audit, the Technology Services Department was staffed by six members, including a Director of Technology Services, who manage and provide assistance and guidance to administrative staff, faculty, and students regarding the use of IT resources including administrative computer services, Internet support, web hosting services, print servers and e-mail.

MMA's IT infrastructure consists of an administrative database server, web server, e-learning system server, staff e-mail server, staff file server, student e-mail/file server, and two servers for other network services. At the time of our audit, there were approximately 170 workstations for faculty and staff and 100 lab workstations for students on campus connecting to network services via a Local Area Network (LAN). The LAN configuration consists of a Cisco 3550 layer 3 switching core with fiber optics to all buildings feeding into a layer 2 switch. Outside network connectivity is provided through a Forerunner ATM switch combined with a Cisco 2601 router, which connects 4 T1 lines through the University of Massachusetts' Information Technology Services. MMA also connects to state-wide applications through the use of a virtual private network client server.

From an administrative perspective, IT-related systems are used to process the Academy's financial management, administrative, and student information activities. The primary application system used by MMA is the Datatel Colleague system. The Colleague application has two main modules, the student systems module and the financial module. These modules are comprised of an array of sub-modules. For example, the student system module includes recruitment and admissions management, curriculum management and registration modules, and the financial module includes purchasing, accounts payable, accounts receivable, and the general ledger. In addition, MMA's asset inventory is maintained in an application system called FoxPro, and the administrative functions are performed using Microsoft's Office Suite applications. Furthermore, the Academy utilizes the Massachusetts Management Accounting and Reporting System (MMARS) as well as the Human Resources Compensation Management System (HR/CMS) maintained by the Office of the State Comptroller.

The Office of the State Auditor's examination focused on a review of certain IT-related general controls over the Academy's computer operations.

AUDIT SCOPE, OBJECTIVES AND METHODOLOGY

Audit Scope

We performed an information technology (IT) general control examination of IT-related activities at the Massachusetts Maritime Academy (MMA) for the period of July 1, 2002 through March 10, 2005. The audit was conducted from October 14, 2004 through March 10, 2005. Our scope included an evaluation of IT-related controls pertaining to organization and management, physical security, environmental protection, system access security, inventory control over computer equipment, compliance with Chapter 647 regarding lost or stolen computer equipment, disaster recovery and business continuity planning, and on-site and off-site storage of backup copies of magnetic media.

Audit Objectives

Our primary objective was to determine whether adequate controls were in place and in effect for selected functions in the IT processing environment. We sought to determine whether the Academy's IT-related internal control framework, including policies, procedures, practices, and organizational structure, provided reasonable assurance that IT-related control objectives would be achieved to support business functions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to prevent unauthorized access, damage to, or loss of IT-related assets. Our objective regarding system access security was to determine whether adequate controls were in place to provide reasonable assurance that only authorized personnel had access to the Academy's automated systems. Further, we sought to determine whether the MMA was actively monitoring password administration.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that the Academy's computer equipment was properly recorded and accounted for and safeguarded against unauthorized use, theft, or damage. In addition, we determined whether the Academy was in compliance with Chapter 647 regarding lost or stolen computer equipment. Further, we determined whether the Academy had an effective business continuity plan that would provide reasonable assurance that mission-critical and essential IT-related operations could be regained within an acceptable period of time should a disaster render the computerized functions inoperable or inaccessible. In addition, we sought to determine whether MMA had adequate procedures for on-site and off-site storage of backup media to support system and data recovery objectives.

Audit Methodology

To determine the audit scope and objectives, we conducted pre-audit work that included obtaining and recording an understanding of relevant operations, performing a preliminary review and evaluation of certain IT-related internal controls, and interviewing senior Academy personnel. To obtain an understanding of the internal control environment, we reviewed the Academy's primary business functions, organizational structure, and documented IT policies and procedures. We performed a high-level IT-related risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities. Upon completion of our pre-audit work, we determined the scope and objectives of the audit.

Regarding our review of IT-related organization and management, we interviewed senior management, completed questionnaires, analyzed and reviewed the organizational structure and reporting lines of the MMA Technology Services Department. We also obtained and reviewed MMA's Technology Services job descriptions. In addition, we assessed the adequacy of documented IT policies, procedures, and IT strategic plans.

To determine whether computer equipment and backup copies of magnetic media stored on-site were adequately safeguarded from damage or loss, we reviewed physical security over the IT resources through observations and interviews with senior management and Campus Police. We conducted walk-throughs, observed and selectively tested security devices, and reviewed procedures to document and address security violations and/or incidents. We determined whether procedures were in place and in effect to help prevent unauthorized persons from gaining access to the data center, computer labs, and network communication closets. We reviewed control procedures for physical access, such as the authorization of staff to access the data center, and key management regarding door locks to the administrative offices, computer labs, and other areas housing IT equipment. We examined the existence of controls such as office door locks, remote cameras, and intrusion alarms. We determined whether individuals identified as being authorized to access the data center were current employees of the Academy and that controls were in place to restrict access to only Academy personnel.

To determine whether adequate environmental controls were in place to properly safeguard automated systems in the data center and areas housing workstations from loss or damage, we conducted walk-throughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., 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 reviewed the presence of appropriate dedicated air conditioning units in the data center. In addition, we reviewed environmental protection related to general housekeeping procedures in the data center, network communication closets, and areas housing computer workstations.

Our tests of system access security included a review of procedures used to authorize, activate, and deactivate access privileges to the network through the microcomputer workstations located at the Academy. To determine whether only authorized employees were accessing the Colleague system, we obtained a listing from MMA of individuals granted access privileges to the automated system and compared it to the Academy's current personnel listing. We performed the test by cross-referencing the Colleague users to the MMA personnel list to determine whether only current MMA employees had access to the automated systems. We reviewed control practices regarding logon ID and password administration by evaluating the extent of documented policies and guidance provided to the MMA personnel. We determined whether all employees authorized to access the automated system 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 MMA's computer equipment, we reviewed inventory control policies and procedures and requested and obtained the Academy's inventory system of record for computer equipment. We reviewed the current system of record to determine whether it contained appropriate data fields to identify, describe, and indicate the value, location, and condition of the IT-related fixed assets. To determine whether the system of record was current, accurate, and valid for computer equipment, we obtained a copy of the inventory of computer equipment dated January 11, 2005 and valued at $1,438,793. We used the random number generator to select a statistical sample of 73 items with an associated value of $67,115 out of a total population of 1,765 items. We verified the inventory tags of the hardware items listed on the inventory record to the actual tag numbers for the computer equipment on hand. In addition, to determine the validity of the system of record, we reviewed the physical location and the description of the hardware items selected in our test. Furthermore, we judgmentally selected an additional 18 items of computer equipment from multiple physical locations and traced them back to the system of record. In addition, we randomly selected 10 laptop computers valued at $19,531 out of a total population of 55 and verified the laptop hardware location. To further assess the degree of completeness of the system of record, we selected MMA's purchase orders pertaining to IT acquisitions made during fiscal year 2003 and 2004 and determined whether the equipment was properly recorded on the inventory record. Further, we reviewed the adequacy of procedures used by MMA to dispose of surplus equipment, and whether MMA was in compliance with Chapter 647 regarding lost or stolen computer equipment.

To assess the adequacy of disaster recovery and business continuity planning, we determined whether formal planning had been performed to provide for the timely resumption of computer operations in the event that the automated systems become inoperable or inaccessible. In addition, we determined whether MMA had assessed the criticality of application systems and whether risks and exposures to computer operations had been evaluated. We reviewed the status of management's efforts to designate a potential alternate processing site in case of a disruption of system availability.

As part of our review of the 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 storage of magnetic media. We interviewed the Director of Technology Services responsible for the automated full backup of the servers and Windows NT network, and reviewed the current back-up procedures in place for their adequacy and completeness. The review of the generation and storage of backup copies of magnetic media included provisions for the mission-critical, Colleague application system. We inspected the on-site daily backup copies of computer media to determine the provisions for storage, frequency of backup, and the adequacy of controls in place to protect backup media. In addition, we interviewed designated personnel to determine whether they had been formally trained in the procedures for generating backup copies and were aware of the procedures for on-site and off-site storage and the steps required to secure and protect the backup media. We further sought to determine whether designated personnel were aware of procedures required to restore systems via backup media that would be required under disaster or emergency circumstances. Although we did not review the off-site storage facility, we reviewed the contract for off-site storage and the register of backup copies stored off site, and confirmed that the Academy was using an established third-party vendor that that provides secure storage to other state agencies and private businesses.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States 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, we found that information technology-related controls in place at Massachusetts Maritime Academy provided reasonable assurance that control objectives regarding IT organization and management, physical security, environmental protection, business continuity planning, and the generation and storage of on-site and off-site backup media would be met. However, we found that controls needed to be enhanced to provide reasonable assurance that IT resources were properly accounted for in the inventory system of record and that only authorized users could gain access to MMA's Colleague application system.

We found that MMA had a defined organizational structure for the Academy, an established chain of command, clearly delineated reporting responsibilities, and documented job descriptions for information technology staff. The Academy had also documented IT strategic and tactical plans. With respect to appropriate use and the safeguarding of information technology, we determined that formal policies and procedures were in existence, but needed to be strengthened for the management of keys in area of physical security, inventory control over IT-related resources, and system access security. The absence of sufficiently documented controls increases the risk that desired control practices will not be adequately communicated, administered, or enforced. When controls are not documented, the nature and extent of operation controls cannot be referred to or reviewed. We recommend improving the degree of documentation for control procedures with respect to IT security and operations.

Our review of areas housing IT resources indicated that the data center is subject to a keypad lock and is alarmed when unattended. We found that all visitors are escorted when accessing the data center. Our review of other areas housing microcomputer workstations disclosed that on-site Campus Police make periodic rounds nightly to verify that all office doors are locked and that all areas are secure. In addition, Campus Police had written policies and procedures regarding the securing of all campus buildings, and that the entrance gate to the campus is locked and guarded on a nightly basis. However, our audit disclosed that although physical security controls existed, controls over the management of keys should be strengthened by maintaining an up-to-date listing of keyholders and periodically reconciling the list to current employees and required access.

We found that adequate environmental protection, such as fire prevention and detection controls, smoke detectors and alarms, and fire suppression systems such as sprinklers and fire extinguishers, were in place throughout the MMA Campus. In addition, we found that an emergency generator and an uninterruptible power supply were in place for the areas housing the IT resources to help prevent damage to, or loss of the equipment. Our audit disclosed that the data center was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. To improve environmental controls, we recommend that the Academy post evacuation and emergency procedures in the Campus buildings and that staff be trained in their use.

Regarding availability of systems, we determined that control practices were in place to provide reasonable assurance that normal business operations could be resumed at the Academy in a timely manner should the LAN file servers and microcomputer workstations be unavailable for an extended period. Our audit disclosed that MMA had a documented disaster recovery and business continuity plan that was updated periodically. The disaster recovery plan incorporated a disaster preparedness section which included data recovery, data center and server recovery, network and telecommunication recovery, application recovery, and desktop equipment recovery information. In addition, MMA's mission-critical and essential IT systems had been identified in the plan. Our review of the generation and storage of on-site and off-site backup copies of magnetic media disclosed that MMA utilized Live Vault (Iron Mountain) online backup and recovery service. The intent of the Live Vault service is to ensure that data is continuously stored off site at a secure, remote IBM eHosting facility. In addition MMA uses an off-site facility for a warm recovery site in which two servers are housed, one dedicated to the Colleague application and one dedicated to messaging and web services. LiveVault backup data is restored to the warm recovery site each day ensuring the Academy can recover application systems to the previous day's state. In addition, MMA also had a cold site located in a campus building other than where the data center is located. We also found that on-site backup copies of magnetic media were maintained. The backup tapes are bar coded and indexed according to the information that has been copied. However, MMA's business continuity strategy could be strengthened by formally testing the recovery and business continuity plan.

With respect to system access security, our audit disclosed that control practices need to be strengthened to provide reasonable assurance that only authorized users have access to the Colleague application. Certain system access security controls were in place, such as a written responsible use policy, a detailed control process for authorizing access, and a single point of accountability for access security through a Security Administrator. Our test revealed that all Colleague users were current employees. We determined that MMA had implemented certain informal procedures regarding deactivation of logon ID's and passwords. However, documentation of stated control practices with respect to policies and procedures for monitoring user privileges, and password administration and configuration needed to be implemented.

Our audit revealed that MMA could not provide reasonable assurance that the system of record for computer equipment, with a listed value of $1,438,793, could be relied upon, since adequate data integrity controls were not in place and that an annual physical inventory and reconciliation were not being performed to assist in verifying the accuracy and completeness of the inventory record. Although we found IT purchases made during fiscal years 2003 and 2004 were included in the inventory system of record, our audit tests detected missing or incorrect information regarding IT equipment. Our data analysis of the entire population of 1,765 IT hardware items indicated that there were data deficiencies with respect to location, receiving date, model and serial number, and value. In addition, our inventory test of 73 items indicated 29 pieces of computer equipment could not be located, that six additional items were found in different locations than that listed on the inventory, and that two items had been disposed of, but not properly accounted for. Furthermore, an inventory test of ten laptop computers indicated that two laptops could not be found. In addition, our test of 18 hardware items traced from multiple physical locations back to the inventory listing indicated that all 18 were on the inventory list, but the location fields for four items were incorrectly listed. Our audit revealed that although MMA was aware of the OSD policy on surplus property and equipment, the Academy was not in full compliance. Our audit test of 70 surplus items disclosed that none had been submitted to OSD for approval, and that four of the 70 surplus items tested were still on the inventory listing. Furthermore, we found that MMA's Internal Control policies did not include control and reporting requirements set forth in Chapter 647 of the Acts of 1989. During the course of our audit, we determined that the Academy did not report to our Office any computer equipment that had been lost or stolen, as required by Chapter 647.

AUDIT RESULTS

1. Inventory Control over IT Resources

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 the Academy's system of record for property and equipment. We determined that adequate controls were not in effect to ensure that a current, accurate, and complete perpetual inventory record of computer equipment was being maintained. 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, inventory records did not appear to be adequately reviewed for accuracy and completeness, and an appropriate level of reconciliation was not in place. As a result, the integrity of inventory system of record for computer equipment could not be adequately assured. The absence of a sufficiently reliable inventory of computer equipment hinders the Academy'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 Academy had documented internal controls regarding the purchasing and receiving of IT resources, we found that documented policies and procedures were not in place regarding the recording, maintenance, compliance monitoring, and reconciliation of the system of record for IT resources. Additionally, although documented procedures were in place requiring capital asset inventory (GAAP) verification and stock inventory (Non GAAP) verifications be conducted, MMA's internal control document states that "due to limited manpower, we only conduct secondary inventory every three years." In addition, although the Academy had an adequate policy and procedure for the disposal of surplus property, it was not being followed. Furthermore, our review of the receiving, tagging, and recording of the IT resources revealed that all of these duties were being performed by one employee without supervisory oversight, thereby increasing the risk of undetected data errors, unrecorded items, and the potential loss of IT resources.

Massachusetts Maritime Academy provided us with a master inventory system of record that listed IT resources as of January 15, 2005 with a total value of $ 1,438,793. Our audit tests of the inventory of computer equipment indicated that inventory control procedures required strengthening to ensure that inventory records were accurate and complete.

Our data analysis of the system of record identified errors in the proper location of certain computer hardware items. Assuming that the location of equipment is properly recorded at initial installation, the failure to maintain accurate information on location may be the result of inadequate procedures to notify the person responsible for the inventory record when equipment is relocated. There were no formal notification procedures or records in place to ensure that prompt notification would be made to require updating the location field when equipment is moved. In addition, our review of the inventory of computer equipment indicated that a significant portion of the data fields did not include any information. Although we found that complete information was provided for item description and bar code, the extent of missing information for the remaining fields, excluding division code and employee number, averaged 12.2%. The error rate of 12.2% applied to essential data elements such as value, date received, condition, location, and serial number in the Academy's inventory system of record.

We determined that, contrary to the requirements of the Office of the State Comptroller's (OSC) "MMARS Fixed Asset Subsystem Policy Manual and User Guide," MMA had not consistently maintained and accounted for all fixed-asset transactions, including the proper recording and reconciliation of Non-Generally Accepted Accounting Principles (non-GAAP) Fixed Assets. Non-GAAP Fixed Assets are defined as assets, including computer software and electrical and computer components with a historical cost between $1,000 and $49,999. Our audit tests comparing information pertaining to 18 IT-related items selected from their actual location to data contained in the inventory list disclosed that although accurate and complete records were maintained for 14 items, four microcomputer systems (22% of the sample) could not be traced back from their physical location to the listed location in the master inventory listing.

Based on a statistical sample of 73 items with a value of $67,115, we determined that 29 items (40% error rate) valued at $28,207 could not be located at the Academy and six additional items, valued at $5,243, were found in locations other than those stated on the inventory record. We found that two of the sample items drawn from the system of record had been disposed of. With respect to these items, there was no documentation available supporting whether the equipment was properly disposed of as outlined in OSD's Surplus Property policies and procedures. An audit test of 70 surplus IT items disclosed that no documentation to support the surplus had been submitted to OSD for approval, and that four out of the 70 surplus items tested were still on the inventory listing. Based on a judgmental sample of 10 laptop computers, valued at $19,531, we determined that two of the laptops valued at $3,200 could not be located.

We determined that an annual physical inventory and reconciliation of all IT resources was not being performed on a periodic basis in order to assist in verifying the accuracy and completeness of the master inventory record. A lack of monitoring inventory procedures to ensure the timely recording of the relocation or disposal of IT equipment on a perpetual basis and accurate and complete records of individual items resulted in the system of record not being properly maintained, and therefore not reflecting a proper total inventory valuation. As a result, there was limited assurance that the Academy's hardware inventory was being properly recorded and reported, and that sufficient controls were in effect to identify missing equipment, thereby mitigating the risk of lost or stolen hardware. Control measures should be in place to ensure that Academy personnel are aware of and understand the guidelines for hardware inventory. In addition, the Academy should implement inventory-related policies and procedures to continually monitor and periodically evaluate the IT inventory system of record. In addition to properly recording IT resources, IT configuration management will be supported by strengthening the integrity of the IT inventory.

Generally accepted industry standards and good management 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 Office of the State Comptroller's (OSC) "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 the Academy's inventory system of record. During the course of our audit, we determined that the Academy did not report to our Office any computer equipment that had been lost or stolen, as required by Chapter 647.

<u>Recommendation:</u>

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

We recommend that MMA review the assigned responsibility for the recording and accounting of IT-related resources to ensure that adequate segregation of duties, oversight, and accountability are addressed. We recommend that the Academy perform an annual physical inventory and reconciliation of its IT resources to ensure that an accurate, complete and valid 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 hardware, acquisition, and disposal records. To maintain proper internal control, the periodic reconciliation should be performed by staff who are not responsible for maintaining the inventory system of record. We also recommend that MMA refer to the policies and procedures outlined in the Office of the State Comptroller's "Internal Control Guide" to help achieve the goal of ensuring the integrity of the inventory record and enhancing knowledge of the IT infrastructure.

We recommend 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. The Academy should consider the use of the inventory/asset management module in the integrated accounting information system that is currently installed. In addition, we recommend that the inventory responsibilities for recording, maintenance, disposition, and reconciliation of the inventory and configuration information be defined to provide appropriate segregation of duties and management review and oversight. We believe that it would benefit the Academy to use a single inventory system to support inventory and IT configuration management requirements.

We recommend that the Academy management strengthen their understanding of the Internal Control Act, Chapter 647 of the Acts of 1989, and that management control practices and procedures required by the Office of the State Comptroller (OSC) be used as a guide for establishing inventory controls regarding the safeguarding of, accounting for, and reporting on IT-related resources. The Academy should formalize a process for notifying the appropriate individual responsible for maintaining the IT system of record of any lost, stolen, or missing items.

Auditee's Response:

> *In response to the "Inventory Control over IT Resources" audit result, Massachusetts Maritime Academy has embarked on an overhaul to the current Asset Management system. We have presidential authorization to modify our current procedures to comply with OSC guidelines for fixed asset management and internal controls. We have also purchased a Fixed Asset/Property Management software system that will be integrated with our current Administrative database system (Datatel Colleague). The procedural and system changes will be in place by the fall 2005.*

Auditor's Reply:

We are pleased that MMA is taking steps to strengthen the integrity of the fixed-asset inventory record. We believe a single comprehensive inventory control system for all fixed assets, including IT resources, is an important ingredient for your overall internal control structure. Strengthening inventory control procedures will improve the integrity of the inventory system of record and enhance knowledge of the IT infrastructure management capabilities.

We believe that controls to ensure adequate accounting of fixed assets 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 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 surplused equipment. In addition, these efforts should help minimize the risk of lost or stolen equipment and improve the identification of the status of equipment for configuration management purposes.

2. System Access Security

Our audit disclosed that although certain system access security controls were in place, other control practices needed to be enhanced to provide reasonable assurance that only authorized users have access to the Colleague application. We found that control practices needed to be implemented or strengthened regarding the degree of documented access security policies and procedures, deactivation/deletion of logon IDs and passwords, password configuration, and required periodic changes of passwords.

Regarding authorization, we determined that control procedures granting users access to the Colleague application system were generally adequate. We found that MMA had an established process for authorizing new employees with access to the network and Colleague application. The documented procedures stated that Technology Services would be notified of new employee hires by the Human Resources Department together with information regarding the individual’s position and assigned department. Based on this input, which is deemed as authorization for system access, Technology Services establishes e-mail and log in accounts for the new users. If the new employee were a Colleague application user, Technology Services would assess the user’s system needs, assign a security class, and configure an appropriate level of access to the Colleague application system.

With respect to procedures to deactivate access privileges, our audit revealed that although MMA had no written policies and procedures in place to provide reasonable assurance that access privileges would be deactivated for users no longer authorized or needing access to the Colleague application system, our tests revealed that all users were current employees of the Academy and that no logon IDs and passwords remained active for individuals no longer authorized or needing access. However, we determined that MMA management had not established a mandatory timeframe for changing passwords nor had password configuration rules been established or communicated to users. Further, there were no formally documented policies and procedures for terminating user accounts and access privileges.

Generally accepted computer industry standards dictate that IT resources be made available to only authorized users and that the resources be used for only authorized purposes. To help ensure that only authorized users have access to IT resources, appropriate controls also need to be implemented to prevent and detect unauthorized access by individuals, or other systems, not granted access to the resources. 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. Control practices should include formal procedures to ensure that users granted access privileges to automated systems are properly authorized, assigned logon IDs and passwords, and that access privileges are modified or deactivated when employee status changes. 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 the technological environment, including the Internet.

Recommendation:

We recommend that MMA evaluate the required frequency of password changes and implement a required schedule for users to change passwords periodically. We recommend that for administrative users the Academy consider requiring password changes not to exceed 60 days and that at least ten prior passwords not be available for use for each employee. In addition, to reinforce user responsibilities regarding access privileges, we recommend that the MMA require all users to sign a formal statement acknowledging the confidentiality of their passwords and commitment to protect the password from unauthorized use and/or disclosure. With respect to authorization of users to access automated systems, we recommend that MMA review all persons currently granted access to the network and Colleague application system and ensure that all users have been properly authorized. In addition, we recommend that MMA monitor users with active access privileges to the Colleague application and the network.

To strengthen deactivation procedures of logon IDs and passwords, we recommend that MMA coordinate notification by department managers and the Human Resources Department to the Technology Services personnel responsible for access security administration of changes in employee status, such as terminations, extended leaves of absence, or employee transfers. Documented control practices should also help ensure that the Technology Services staff are notified in a timely manner. Once notified of the change in employment status, Technology Services staff should deactivate and/or delete the logon ID and password in a timely manner. Appropriate staff should be instructed regarding compliance with these policies and procedures.

We recommend that documented control practices regarding logon ID and password administration, including authorization and activation of access privileges be included in the Academy's internal control plan. Policies and procedures should also include procedures for deactivation and deletion of logon IDs and passwords. We also recommend that the internal control plan address security violations, monitoring and reporting of access attempts, and follow-up procedures for violations and violation attempts.

Auditee's Response:

> *In response to the "System Access Security" audit result, the Technology Services department at the Academy is undergoing the implementation of the audit recommendations for password frequency change and the ability to use prior passwords. We have also implemented an internal*

> *security class audit for the administrative database system. The audit will be accomplished twice a year for all of the administrative users. Although the Academy has documented procedures for the creation of system users and security classes for incoming employees, deactivation of system users for reasons of termination, extended leave, and transfer has not been formally documented. Technology Services is working with Human Resources to document this procedure for presidential approval. The system and policy documentation will be in place by fall 2005.*

Auditor's Reply:

We are pleased that MMA is taking steps to strengthen security to its systems by implementing procedures for user account and password administration as well as a schedule for users to change passwords periodically. In addition, documenting formal policies and procedures to notify the network security administrator of any change in job requirements, transfers, active/inactive status, or termination of employees will enhance system security for the administrative database system.