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. 2006-0456-4T

OFFICE OF THE STATE AUDITOR'S REPORT ON THE EXAMINATION OF INFORMATION TECHNOLOGY–RELATED CONTROLS AT THE MASSACHUSETTS DEPARTMENT OF ENVIRONMENTAL PROTECTION

July 1, 2004 through March 1, 2007

OFFICIAL AUDIT REPORT

SEPTEMBER 13, 2007

TABLE OF CONTENTS

INTRODUCTION

The Massachusetts Department of Environmental Protection (DEP) was established under the provisions of Chapter 21A, of the Massachusetts General Laws (MGL). The Executive Office of Environmental Affairs (EOEA) provides administrative oversight as well as strategic and tactical planning to DEP's IT operations. The DEP's primary mission is to monitor hazardous-emission levels in the air and pollution levels in the water, safe management and disposal of solid and hazardous wastes, timely cleanup of hazardous waste sites and spills, and the preservation of wetlands and coastal resources. The DEP operates from a central office located in Boston, four regional offices in Springfield, Worcester, Wilmington, and Lakeville, and a state laboratory in Lawrence. At the time of our audit, the DEP had 971 employees working in conjunction with local communities to protect the environment. The DEP received an appropriation of $53,084,756 in state funds for fiscal year 2006 and an appropriation of $56,479,040 in state funds for fiscal year 2007.

The DEP's Information Technology Office (ITO) is responsible for managing all network operations. The DEP IT operations are supported through a local area network (LAN) consisting of 100 file servers, 1,058 microcomputer workstations, and 122 notebook computers located throughout DEP's central office and regional sites. The local area network provides connectivity to the Commonwealth's wide area network allowing users to access the Massachusetts Management Accounting and Reporting System (MMARS), and the Human Resources/Compensation Management System (HR/CMS) systems. The ITO is responsible for managing all of the DEP's file servers, routers and switches to support local area and wide area network access and manages data file exchanges with various state and federal environmental agencies. Furthermore, the ITO provides a help desk function and a field staff to provide technical services to all application users.

The DEP utilizes over 25 application systems to support its business functions. The main application system is a customized product, which is called the Environmental Protection Integrated Computer System (EPICS). The EPICS application database was deployed at the Boston Central Office in 1988 and has served as the primary application system throughout the DEP. The EPICS is an Oracle database application that contains information regarding regulated facilities, water supplies, waste sites and some DEP compliance and enforcement activities. The EPICS application tracks environmental discharges and spills as well as the issuance of permits, and compliance inspection reports.

The Office of the State Auditor's internal control examination was limited to a review of certain IT general controls over and within the DEP's IT environment.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From June 6, 2006 through March 1, 2007, we performed an audit of selected information technology (IT) related controls at the Massachusetts Department of Environmental Protection (DEP) for the period covering July 1, 2004 through March 1, 2007. The scope of our audit included an evaluation of IT-related controls pertaining to organization and management, physical security, environmental protection, system access security, inventory control over computer equipment, disaster recovery and business continuity planning, on-site and off-site magnetic media storage.

Our audit also included an examination of controls over data integrity for selected acute contaminant information in the Water Quality Testing System (WQTS) for validity, completeness and accuracy. The WQTS is an application module within the Environmental Protection Integrated Computer System (EPICS).

Audit Objectives

Our primary audit objective regarding the examination of IT-related controls was to determine whether the IT environment was sufficiently controlled to support automated systems and to safeguard IT-related assets. We sought to determine whether the control environment, including policies, procedures, and the organizational management structure provided reasonable assurance that IT-related control objectives would be achieved. 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 ensure that only authorized personnel had access to the automated systems and IT resources. We sought to determine whether passwords were being properly controlled and monitored. In addition, we determined whether data was sufficiently protected against unauthorized disclosure, change, or deletion.

We sought to determine whether adequate controls were in place and in effect to provide reasonable assurance that computer equipment was properly accounted for and safeguarded against unauthorized use, theft, or damage. We sought to determine whether business continuity and user area plans were in place for use in disaster recovery efforts to regain business operations supported by technology. In addition, we sought to determine whether continuity plans included recovery strategies should IT resources be lost or damaged. We also sought to determine whether there were adequate procedures for on-site and off-site storage of backup media to regain business operations should IT systems become inoperable or inaccessible. A further objective was to determine the integrity of acute contaminant data within the

EPICS water quality module, which is used to report information to the Environmental Protection Agency (EPA) regarding water quality.

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 management. To obtain an understanding of the internal control environment, we reviewed the DEP's organizational structure, primary business functions, and relevant policies and procedures. We performed a high-level risk analysis and assessed the strengths and weaknesses of the internal control system for selected activities.

Regarding our review of organization and management, we interviewed senior management and reviewed, analyzed, and assessed relevant IT-related internal control documentation. We also reviewed the organizational structure and reporting lines of DEP's Information Technology Office. For the areas under review, we determined whether policies and procedures were in place, in effect, and communicated to appropriate staff. We also reviewed DEP's strategic planning initiatives. To determine whether IT-related job descriptions and job specifications were up-to-date and reflected current responsibilities, we obtained a current list of the personnel employed by the ITO, including their duties and job descriptions, and compared the staff list to the ITO organizational chart and each employee's stated day-to-day responsibilities.

We interviewed management to discuss internal controls regarding physical security over and within the file server room, the business offices where microcomputer workstations are located, and the on-site and off-site areas for mission-critical and essential magnetic media storage. To evaluate physical security, we interviewed senior management and security personnel, conducted physical inspections, observed security devices, and reviewed procedures to document and address security violations and/or incidents. Through observation, we determined the adequacy of physical security controls over areas housing IT equipment. We examined controls such as office door locks, security personnel on duty, locked entrance and exit doors, the presence of personnel at entry points, whether sign-in/sign-out logs were required for visitors, and whether the facility was equipped with an intrusion alarm. We reviewed key management policies and procedures regarding key management. We requested and obtained a list of master key holders to the file server room and determined whether individuals identified as being authorized to access areas housing computer equipment were current employees.

To determine whether adequate environmental controls were in place to properly safeguard areas housing computer equipment from loss or damage, we conducted walkthroughs and checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (i.e., sprinklers and fire extinguishers), an uninterruptible power supply (UPS), and emergency power generators and lighting. To determine whether proper temperature and humidity controls were in place, we inspected the file server room to ensure the presence of appropriate dedicated air conditioning units and/or Heating, Ventilation and Cooling systems (HVAC). In addition, we reviewed environmental protection controls related to general housekeeping procedures in the file server room, as well as selected areas housing computer equipment. Audit evidence was obtained through interviews, observation, and review of relevant documentation.

Our tests of system access security included a review of policies and procedures to authorize, activate, and deactivate access privileges to system applications residing on DEP file servers through the microcomputer workstations located at the DEP's Central office and regional facilities. We reviewed control practices regarding logon ID and password administration and password composition by evaluating the appropriateness of documented policies and guidance provided to personnel. We determined whether all individuals authorized to access system applications were required to change their passwords periodically, and, if so, the frequency of the changes. In order to verify that all users of the automated systems were either current DEP employees or current DEP contract employees, we obtained a system generated user list containing 1,335 user accounts as of August 8, 2006. We compared this list to a DEP employee and contractor listing dated July 10, 2006. We determined whether there were any changes in employment status between July 10, 2006 and August 8, 2006. The employee listing consisted of 971 full-time employees and 55 contract employees. We determined that out of a total of 1,026 full-time and contract employees, 1,005 were considered by DEP to be authorized users. We developed an exception list from which we were able to identify those user accounts no longer requiring access privileges to the automated systems. Our audit did not include an examination of controls over network security**.**

To determine whether adequate controls were in place and in effect to properly safeguard and account for computer equipment, we initially reviewed inventory control policies and procedures and obtained an inventory of computer equipment. We examined the computer inventory record for identification tag numbers, locations, descriptions, acquisition dates, and historical cost. We obtained the master fixed asset inventory record dated June 2006. We conducted an inventory test applying ACL audit software, selecting a sample of 80 out of a population of 1,282 hardware items listed on the inventory. In addition, we judgmentally selected 63 items and traced the equipment from the physical location to the master list. Subsequent to our initial inventory test, we obtained a secondary inventory list dated July 2006 consisting of 28 notebook computers not included in the master inventory. We judgmentally selected eight of the 28 notebook computers and traced the items to their physical location. We also selected 50 out of a population of 150 leased microcomputers for fiscal years 2005 and 2006, and verified the leased documentation to the individual items. We then physically located each item and traced the item back to the current master inventory record.

To assess the adequacy of business continuity planning, we identified the extent to which DEP management had reviewed the impact of a loss of processing capabilities to its automated systems. We examined whether the DEP had performed a formal risk assessment in order to determine the degree to which formal planning had been developed to address the impact should processing capabilities be disrupted for an extended period of time. With respect to business continuity planning, we reviewed DEP’s continuity of operations plan, and the business continuity plan. We interviewed management to determine whether a written, tested business continuity plan was in place, whether the criticality of application systems used by the DEP had been assessed, and whether risks and exposures to computer operations had been evaluated. In addition, to evaluate the adequacy of controls to protect and ensure the availability of electronic documents and data files, we interviewed DEP staff regarding the generation of backup copies of computer-related media. We also reviewed the frequency and types of backup procedures as well as physical and environmental controls for on-site and off-site storage. In addition, we also reviewed physical security and environmental controls for on-site and off-site magnetic media storage at DEP’s four regional offices and the laboratory location.

Our tests of data integrity over the EPICS Water Quality Testing System (WQTS) included a review of policies and procedures over data preparation, maintenance, and compliance reporting. To determine whether DEP had adequate controls over data entry for the EPICS database, we judgmentally selected data elements related to water quality samples for bacteria, nitrates, and nitrite contaminants from the WQTS for the period January 2006 through December 2006. We conducted a data integrity test applying ACL audit software, selecting a random sample of 61 out of a population of 1,732 public and private water suppliers throughout the Commonwealth. We tested the sample items to determine whether acute bacterial contaminant information documented on the WQTS source documents was properly and completely recorded in the EPICS database.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) issued by the Comptroller General of the United States through the U.S. Government Accountability Office and generally accepted industry practices. Audit criteria used in the audit included management policies, 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 Department of Environmental Protection (DEP), we determined that internal controls in place provided reasonable assurance that IT-related control objectives pertaining to organization and management, physical security, and environmental protection would be met. However, our audit revealed that controls pertaining to system access security, inventory control over computer equipment, on-site and off-site storage of backup copies of magnetic media, disaster recovery and business continuity planning, and data integrity concerning certain data elements in the EPICS Water Quality Testing System (WQTS) needed to be strengthened.

Our examination of organization and management controls revealed that there was an established chain of command, adequate level of oversight, segregation of duties and clear points of accountability regarding IT functions. We found that management and staff were well aware of their responsibilities, and that job descriptions and job specifications reflected current responsibilities. Our review of IT internal controls found that the DEP, in conjunction with EOEA, had developed and documented policies and procedures for IT-related functions and appropriate strategic planning initiatives.

Our audit revealed that physical security and environmental protection controls at the Boston central office and regional offices were in place and in effect to provide reasonable assurance that IT resources would be protected and were operating in a controlled environment. Our examination of physical security controls revealed that a security guard was posted in the main lobby during business hours and that entry doors were equipped with intrusion alarms. We found that employees were required to wear identification cards during business hours and visitors were required to be escorted through the office during their visit. We found that the file server room was locked and that access was limited to designated IT personnel. Furthermore, we found that DEP management maintained a master key list to the file server room.

Our audit test of environmental protection controls over the office areas and file server room indicated that policies, procedures, and appropriate control mechanisms were in place and in effect over the processing environment. Specifically, we found that control objectives related to general housekeeping, air conditioning, fire prevention and detection, emergency power and lighting, and emergency shut down would be met. We observed that the file server room was well planned and organized and had strong environmental controls to protect personnel and equipment. The areas housing IT resources were found to be clean and environmentally protected. We observed the presence of hand-held fire suppression devices and an automatic fire suppression system throughout the office areas.

Although we found certain access security controls to be in place, our audit indicated that access security controls needed to be strengthened for DEP’s automated systems. We found that appropriate policies and procedures were documented, security administration had been assigned, appropriate rules for user access activation and deactivation and password length and composition were in place. We found that employees were required to change passwords every 42 days. However, our tests of authorized users of DEP's network system revealed that 60 (4.5%) out of 1,335 user accounts could not be identified on the July 2006 official personnel record containing both current employees and contract employees. Our review indicated that termination dates for system user accounts for individuals no longer employed or contracted to the DEP, dated back to early July 2003. Our audit also identified 270 user accounts that contained generic accounts, user accounts for individuals with name changes and new hires. We recommend that DEP adhere to existing policies and procedures requiring department supervisors and the Workforce Services Division to notify the security administrator of changes to either an employee or contract employee's status that may warrant changes to, or removal of their user account.

Although we found certain inventory control policies and procedures in place, inventory controls for computer equipment needed to be enhanced to ensure that computer equipment is properly accounted for and recorded in the inventory system of record. Our audit tests of DEP's master inventory record indicated that all items were located, properly accounted for, and tagged. However, we found that the inventory record did not contain appropriate data fields including historical costs, location, and condition of the equipment. We also found seven microcomputers on the inventory record without serial numbers and three laptop computers with duplicate serial numbers. Furthermore, our audit disclosed that although written policies and procedures were in place for the reporting of lost or stolen equipment, DEP management failed to report two missing laptops with a total estimated value of $2,600 to the Office of the State Auditor and State Police as required by Chapter 647 of the General Laws.

We found that adequate controls were in place over on-site and off-site storage for computer media systems and data files. Our audit revealed that DEP has a designated alternate processing site to continue business-processing operations for the central and regional offices. We found that the business continuity plan had sufficient details for comprehensive instructions, including identifying key personnel, designating specific tasks and listing telephone numbers. Our audit disclosed that there was a written business continuity plan in place for the timely restoration of computer operations with regard to the EPICS system. Even though DEP had designated an alternate processing site to ensure timely restoration of business functions and applications operating on the LAN and standalone microcomputer systems, we found no evidence that DEP had conducted formal recovery exercises since the Year 2000 initiative of their business continuity plan. These types of exercises are crucial to ensure efficient and complete continuity processes and procedures. Therefore, DEP may be vulnerable to the loss of business and computer functions should a significant and disruptive event occur and recovery processing from such an event may be considerably hampered. Our review of on-site and off-site magnetic media storage at

DEP's four regional offices and the laboratory location revealed that adequate controls were in place and in effect.

Our limited examination of the data integrity controls over the Water Quality Testing System application module revealed that there were established policies and procedures to comply with regulatory reporting requirements, but monitoring procedures to ensure accurate and complete information needed to be enhanced. Our limited audit tests revealed that DEP did not monitor data entry activities relating to the proper and complete recording of information in the EPICS database on a consistent basis. Our examination of data integrity controls revealed that information in the EPICS database for acute contaminants in the WQTS system did not reflect the actual information recorded on the source documentation for our test sample. Our audit tests revealed that acute contaminant data, for 10 of the 61 (16.39%) public and private water suppliers sampled contained missing or erroneous information. Since DEP relies on information in the EPICS database to comply with reporting requirements to federal agencies and to provide statistical information on water quality, incorrect or missing data may have resulted in inaccurate reporting**.**

.

AUDIT RESULTS

1. User Account Management

Our audit revealed that system access security over the Department of Environmental Protection's (DEP) automated systems needed to be strengthened to ensure that only authorized users have access to the system. We found that appropriate policies and procedures were documented, security administration had been assigned, and appropriate rules for user access activation, password length, and composition were in place. We also found that employees were required to change passwords every 42 days. However, we found that, although there were written procedures in place requiring that DEP's Workforce Services Division inform the Information Technology Office (ITO) when an employee terminates employment, our audit revealed instances where no action was taken to remove expired, terminated or suspended user accounts from the DEP's network.

Our tests of system access security for DEP's network indicated that, contrary to sound access security practices and DEP's security policies, there were inactive user accounts that had not been deleted for individuals who were no longer employed or contracted by the DEP. Our tests of the network system indicated that 60 (4.5%) out of 1,335 user accounts were not identified on the July 2006 employee and contractor listing. Our audit disclosed that a DEP contract employee whose contract had expired in July 2003 remained on the user account list as of August 2006. We also determined that there were two duplicate accounts for active users on the DEP user list. In addition, our audit identified 270 user accounts that contained generic accounts or user accounts for individuals with name changes and new hires.

The DEP's security policy titled Standard Operating Procedure For Accessing Computer Systems And For Assigning User Roles states: *Whenever a staff member terminates his/her employment with the DEP, the BAS Workforce Services Division notifies the DEP Security Administrator and the DEP ITO Help Desk via an e-mail. The UAID must be deleted immediately*.

The DEP had not consistently exercised their monitoring procedures concerning compliance with the access security policy addressing controls over the deletion of user accounts. To ensure that only authorized access privileges are maintained, timely notification should be made to the security administrator of any changes in user status that would impact their level of authorization. The failure to delete user accounts in a timely manner may place the DEP at risk of unauthorized access or use of established privileges (using another individual's user account having higher access privileges). As a result, certain information residing on the DEP network could have been vulnerable to unauthorized access.

Computer industry standards advocate that policies and procedures for system access security be documented and approved to provide a basis for proper protection of information assets. The policies and procedures should address authorization for system users, activation and deactivation of user accounts, notification of changes in user status, maintenance of authentication mechanisms, and procedures to be followed in the event of an unauthorized access attempt or unauthorized access.

Recommendation:

We recommend a review of the status of all active users of DEP's application systems and removal of all access privileges and user accounts for those individuals who no longer require access. We recommend that DEP management adhere to its own established policies regarding the timely notification to the ITO to de-activate user accounts. We further recommend that the policy be expanded to include not only staff members, but also contract employees. We recommend more vigilant monitoring of access accounts for DEP employees, as well as outside contractors providing services, to ensure that access privileges be terminated and deleted from the user access list in a timely manner when individuals no longer require access to application systems.

We further recommend that DEP management consider implementing elements of CobiT (Control Objectives for Information and Related Technology). CobiT, issued by the Information Systems Audit and Control Foundation, is a generally applicable and accepted standard for IT security and control that provides a control framework for management, business process owners, IT functions, users, and auditors. In particular, the CobiT User Account Management Control for Data Security recommends: *"Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts. A formal approval procedure outlining the data or system owner granting the access privileges should be included. The security of third-party access should be defined contractually and address administration and non-disclosure requirements. Outsourcing arrangements should address the risks, security controls and procedures for information systems and networks in the contract between the parties. Management should have a control process in place to review and confirm access rights periodically. Periodic comparison of resources with recorded accountability should be made to help reduce the risk of errors, fraud, misuse or unauthorized alteration."*

Auditee's Response:

> *MassDEP believes that the draft report overstates the extent of this problem and implies a more serious risk than actually exists. However, after conferring with the Audit team, MassDEP has developed and put into practice new procedures to bolster user account management in areas that were weak.*
>
> *To fortify MassDEP's user account management, the agency has instituted new procedures governing staff "transactions". Staff includes regular employees, personal*

> *service contractors, interns, seasonal staff, and third party contract personnel such as temporary workers, staff augmentation employees, and short-term contractors. Transactions include hiring, terminating, transferring, moving, or even just changing network access, telephone numbers, or cubicles.*
>
> *The development of this new procedure included participation from each MassDEP Bureau, Region, and Office. Department managers have signed off on the procedure and it has been in use since March 2007. The new process addresses updating user account information associated with any and all job changes. Supervisors complete a form on the MassDEP Intranet site and send it to a distribution list, DEP-DL - Staff Changes. The distribution list is comprised of staff with responsibilities for Information Technology, Human Resources, Employee Relations, Facilities, Telephones, and Security Operations.*
>
> *In addition, a network domain manager reviews all accounts quarterly to identify accounts that are disabled due to contract completion, administrative leaves, etc. Where appropriate, the network domain manager contacts program staff/supervisors to confirm that the account is still needed or to arrange for the account termination. Special reviews will be conducted to coincide with peak periods of activity. For example, although a quarterly review will be completed at the end of June, another review will be completed late in July and again in September to focus on network accounts held by direct personal service contractors, summer interns, and seasonal employees, since many personal service contracts end on June 30th and interns and seasonal staff leave around September 1st.*
>
> *Lastly, MassDEP IT staff has tightened the process to justify generic accounts. All requests and justifications for generic accounts must be put in writing and approved by the program manager. When the request is submitted, IT staff meet with program personnel to discuss alternatives that may be available to meet the business need rather than using a generic account. This process has been in effect since March 2007.*

Auditor's Reply:

We believe system access security in DEP's IT environment is critical and commend the actions taken to improve controls in this area. We acknowledge DEP's efforts to enhance policies and procedures for access security based on our audit recommendations. We believe DEP should continue to ensure that user privileges be clearly specified and documented for every active user account and constantly monitored and evaluated to ensure that only authorized users are allowed access to network application systems and data.

2. Inventory Control Over Computer Equipment

Our audit disclosed that inventory control over computer equipment needed to be strengthened. Although we determined that the DEP had documented internal controls regarding the purchasing, receiving and leasing of IT resources, we found that documented policies and procedures needed to be enhanced regarding the recording, maintenance, compliance monitoring, and reconciliation of the system of record for IT resources. 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, we found the DEP maintained a master inventory record as well as secondary listing of notebook computers not listed on the master inventory record. We also found both inventory records were not adequately reconciled for accuracy and completeness. As a result, the integrity of the inventory system of record for computer equipment could not be adequately determined.

Our audit tests revealed that DEP did not comply with the reporting requirements in Chapter 647 of the Acts of 1989, of the General Laws "An Act Relative to Improving the Internal Controls Within State Agencies." Our audit revealed that incident reports over the audit period for two missing or stolen notebook computers had not been filed with the Office of the State Auditor (OSA) as required by Chapter 647. According to DEP management, the two missing notebook computers had a total estimated value of $2,600.

Our audit tests of DEP's master inventory record indicated that all items were located, properly accounted for and tagged. However we found seven microcomputers on the inventory record without serial numbers and three notebook computers with duplicate serial numbers. We also found that the inventory record did not contain appropriate data fields including historical costs, location and condition of the equipment. We believe that having one inventory system of record for all computer equipment would enhance the inventory record.

Generally accepted industry standards and sound 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, "the agency shall be responsible for maintaining accountability for the custody and use of resources and [shall] assign qualified individuals for that purpose, and [that] periodic comparison should be made between the resources and the recorded accountability of the resources to reduce the risk of unauthorized use or loss and protect against waste and wrongful acts." Moreover, the OSC's "Internal Control Guide for Departments," promulgated under Chapter 647 of the Acts of 1989, notes that fixed assets should be accounted for in compliance with 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 DEP's inventory system of record. During the course of our audit, we determined that the DEP did subsequently report to the Office of the State Auditor the computer equipment that had been missing.

Recommendation:

The DEP should establish and maintain a comprehensive list of computer equipment. The list should be maintained on a perpetual basis, and any changes to the list should reconcile to the master system of record. We recommend that control procedures be implemented to ensure that the inventory records are maintained in an accurate, complete, and timely manner. DEP's inventory records should reflect any changes to computer hardware items, including location or status, for both deployed equipment and items held in storage.

We further recommend that DEP's system of record for IT inventory be expanded to include data fields containing information relative to cost, condition, acquisition and installation date, and status of the IT resource. The recommended control procedures should provide increased assurance that all IT-related equipment is properly recorded and accounted for and enable the development of a complete record, maintained on a perpetual basis, of all IT-related equipment at the DEP.

We recommend that the DEP's 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 the DEP maintain a single master inventory record for all computer equipment.

The DEP should maintain policies and procedures that will comply with Chapter 647 of the Acts of 1989 and immediately report all instances of unaccounted for variances, losses, and thefts of funds or property to the OSA. The DEP should communicate requirements for all internal and external notifications of thefts to a designated staff member. Furthermore, the DEP should investigate how these notebook computers were either lost or stolen and try to establish controls to minimize the risk of reoccurrence.

Auditee's Response:

> *MassDEP has established a comprehensive list of equipment, instead of relying on separate inventory lists for computers and laptops/tablets. Also, MassDEP now maintains active and inactive computer devices on the network. Systems that are removed from the network remain in the same inventory, in a section labeled inactive. This section includes workstations that are on hold for a specific purpose and workstations that are being prepared for redistribution. Hold and Ready folders are used for the inactive PCs. The use of a notes feature in the inventory helps identify specific issues for a PC or Laptop such as why it is in Hold folder.*
>
> *To address the audit issue with the location field, new data standards have been adopted to clarify location so that it will be more exact, such as Fabrication Room, Server Room, or Storage cabinet, instead of ITO.*
>
> *To ensure that the inventory is accurate on a perpetual and periodic basis, MassDEP has implemented new procedures. On a monthly basis a senior IT staff member now retrieves a report from the inventory and reviews the report for completeness and identifies workstations that need to be updated. Data elements that sometimes need to be updated include Program Unit, location, lease information, and problems with the beaconing application.*

> *In order to include data fields containing information relative to cost, condition, acquisition and installation date, and status of the IT resource, MassDEP will merge information from databases that store the physical inventory and fiscal information. MassDEP utilizes an electronic inventory system that enables it to track the location from which the laptop/computer is operating. MassDEP leases equipment so that the turnover period is three years for nearly all PCs, Laptops, and Tablets. Since the condition of the equipment does not vary much from model to model, MassDEP will use the active/inactive terminology with notes to explain whether or not a device is functioning. Within the Fiscal store of data, the lease contract information includes the serial number, lease cost, receipt date, term of lease, and initial date of installation. This information will be aligned with the electronic inventory system using the serial number as a key identifier.*
>
> *MassDEP has policies and procedures that comply with Chapter 647 of the Acts of 1989 and will ensure that in the future agency staff will immediately report all instances of unaccounted for variances, losses, and thefts of funds or property to the OSA.*

Auditor's Reply:

We are pleased that DEP is developing a single comprehensive system of record that will incorporate additional data fields and include all IT resources. Although DEP had documented policies and procedures, we are pleased to note that inventory controls are being enhanced and monitoring procedures are being improved to evaluate compliance with established guidelines and to ensure proper accounting and recording of IT resources. We commend DEP's efforts to maintain and monitor the system of record on a perpetual basis. Once DEP's inventory system of record is fully developed it should be reconciled annually to physical resources and inventory-related records regarding the acquisition, maintenance and disposition of IT resources.

3. Business Continuity Planning and Off-Site Storage of Computer Media

Our audit revealed that the DEP, in conjunction with the Executive Office of Environmental Affairs (EOEA), had developed a disaster recovery and business continuity plan for restoring processing functions in the event that automated systems were rendered inoperable or inaccessible. However, while we acknowledge the existence of a documented business continuity plan, we found no evidence that DEP had conducted any recovery tests of the plan. According to management, DEP's active participation supporting the Massachusetts Emergency Management Agency's (MEMA) project to comply with Massachusetts Executive Order No. 144 directing all state executive agencies to prepare for emergencies and disasters took priority over further development, including testing of the business continuity plan.

The lack of a formally tested plan to address the resumption of processing capabilities may significantly impact DEP's recovery efforts to properly restore mission-critical, essential, and confidential data. Without a formal, tested recovery strategy, DEP might experience delays in re-establishing mission-critical functions, such as processing of WQTS data for the EPICS application and performing the monitoring of hazardous-emission levels in the air and pollution levels in the water, safe management and disposal of solid and hazardous wastes, timely cleanup of hazardous waste sites and spills, and the preservation of wetlands and coastal resources. Recovery tests are a key component of a formal business continuity plan.

The objective of business continuity planning is to help ensure timely recovery of mission-critical functions, should a disaster cause significant disruption to business or computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted business practices and industry standards for computer operations support the need for the DEP and the EOEA to have an ongoing business continuity planning process that assesses the relative criticality of information systems, maintains appropriate contingency and recovery plans, and conducts recovery tests to provide assurance of the viability of the business continuity plans. To that end, DEP, in conjunction with the EOEA, should assess the extent to which it is dependent upon the continued availability of information systems for all required processing or operational needs and conduct tests for its recovery plans based on the critical aspects of its information systems.

Regarding our examination of backup computer media, we found that controls were in place to provide reasonable assurance that control objectives relating to the physical security over the storage of computer media would be met. However, our audit revealed weaknesses in the timeliness of storing backup copies of magnetic media off-site.

We found that each DEP location conducted system backups on a daily basis and the backup tapes were kept at secure on-site locations. Our examination also revealed that weekly backups were being performed at the end of each weekend and stored off-site at a designated regional office. However, we found that the central office located in Boston retains the most current copy of its backup for the following week to accommodate various requests for file and data restorations, while transporting the previous weekly backup to a regional office. Therefore, the backup copies of information being stored off-site is never less than one week old and can extend to two weeks, which could result in significant delays to recovery efforts should DEP experience a loss or disruption to their automated systems. Because the backup copies used to recover the system would not contain the timeliest data available, we believe that the scheduling of off-site storage could result in an impediment to recovery efforts to restore system and electronically processed information.

Recommendation:

We acknowledge DEP's efforts to actively support MEMA's Continuity Of Operations project to comply with Massachusetts Executive Order No. 144; however, we recommend that DEP enhance their efforts to develop and maintain a formal business continuity plan for the timely restoration of mission critical and essential business functions.

We recommend that DEP formally test their disaster recovery plans to assess the viability of the plans and thereby reduce restoration time, minimize the risk of errors or omissions of necessary processes and procedures, and mitigate any negative impact to the recovery of its business functions.

Regarding controls over off-site storage, we recommend that DEP modify the scheduling of transporting backup copies of electronic media to ensure that more timely backup copies are stored off site. To ensure storage of the most recent weekly data, we recommend that DEP devise a method whereby off-site storage contains information immediately preceding the current week.

Auditee's Response:

> *MassDEP did not provide formal evidence of recovery tests of the plan since such information is captured in eMail messages and meeting minutes. Going forward, such data will be attached to the COOP plan and/or the Disaster Recovery plan with a summary of changes. MassDEP conducts tabletop exercises and as a result has modified the COOP plan. Actual events, (sudden power outage, server failure, accidental deletion of critical files, virus infection), have triggered actual recovery of data on a number of occasions. After each event IT staff have conducted a post-mortem, developed lessons learned, and updated the disaster recovery plan to reflect the lessons learned. Written summaries of the tabletop exercises and actual events will be attached to the COOP a/o Disaster Recovery plan. Additionally, MassDEP will conduct physical exercises to better assess the risks of the current COOP plan in the future.*
>
> *MassDEP agrees with the audit recommendation and the Department will continue to pursue additional funding for such measures. MassDEP requires additional storage capacity and the installation of more bandwidth to implement a full offsite backup plan. Since EPICS is the agency's primary repository for environmental data, MassDEP now exports a copy of the EPICS data nightly to a database server in the Lawrence office. This effort was implemented during the audit.*

Auditor's Reply:

We acknowledge DEP's efforts to enhance and test the COOP plan as a necessary first step in developing a comprehensive and formalized business continuity plan; however, the COOP plan does not provide sufficiently detailed recovery strategies to restore the IT processing environment and automated systems to support DEP's business objectives. We encourage DEP management to evaluate, continue to test, and approve and finalize a comprehensive business continuity strategy. Once developed, the business continuity plan should be reviewed and updated annually, or whenever there are significant changes to processing requirements, risks, or the Department's IT infrastructure.

4. Data Integrity of the Water Quality Testing System (WQTS) - Environmental Protection Integrated Computer System (EPICS)

Our audit revealed that data integrity controls over the DEP's Water Quality Testing System module needed to be strengthened to ensure that monitoring of acute contaminant data (bacteria, nitrate and nitrite) is performed on a consistent basis. We determined that DEP program management did not consistently adhere to current policies and procedures associated with management review of data entered into the WQTS database. We focused our review on data integrity controls for DEP's acute water contaminant results for bacteria, nitrate and nitrite information processed by DEP's water quality program.

Our audit revealed that data entry errors occurred in the WQTS module during the period of January 2006 to December 2006. Our audit tests identified missing acute contaminant information and data entry errors for 10 of the 61 cities and towns sampled (16.39% error rate). We found examples in the WQTS module of nitrates and nitrite information that did not conform to the hard copy documentation submitted by DEP's regional offices. Our tests of information on bacterial results entered into the WQTS module revealed examples of incorrect data. We also found some examples of bacteria data not entered into the WQTS database at the end of each month as required by DEP's procedures regarding quality assurance and control. We believe that lack of supervisory monitoring, from both the regional offices and the central office, contributed to this error rate.

Computer industry standards advocate that policies and procedures for data integrity controls be documented and approved to provide a basis for the proper validity and availability of data. Our audit revealed that DEP policies and procedures regarding data integrity controls and quality assurance require that "…data entry deadlines for bacterial information at the end of each month, and 30 days after the end of the quarter for other monitoring data." In addition the policy states that the program coordinator "will review the quality assurance report for any obvious data anomalies and duplicate records and audit approximately 10% of the records by comparing the WQTS data with the hard copy. The program coordinator will be responsible for ensuring that all data corrections are made to WQTS."

DEP relies on information within the EPICS WQTS database to comply with reporting requirements to local, state and federal agencies. Incorrect or missing data may result in inaccurate statistical information in the EPICS database.

Recommendation:

We recommend that DEP strengthen their data integrity controls to ensure that test results are entered into the system in a more timely manner. We further recommend that data that has been entered into the system be subject to review to ensure an adequate level of data accuracy and completeness. DEP management should enhance and adhere to DEP policies and procedures for the monitoring of data entry and reconcile water quality test results from source documentation to information contained in the EPICS WQTS module.

Auditee's Response:

> *It is important to emphasize that public health and the environmental compliance determinations that form the basis of MassDEP's drinking water oversight are in no way compromised by problems with the manual data entry of water quality results into the Water Quality Testing System. Additionally, the acute contaminant data in EPICS is not part of the subset of state data that is reported to the EPA.*
>
> *The report characterizes our monitoring activities "to ensure accurate and complete information" as inconsistent and in need of enhancement. On the surface MassDEP agrees with this statement in as much as it applies to the complete data set within WQTS and reflects historical decisions about the application of limited staff resources. However, MassDEP believes that all of the recommendations for improving the timeliness, accuracy and completeness of water quality data entry, including acute contaminant data, will be addressed as hardcopy submissions are replaced by electronic reporting. The Department's electronic bulk upload process enables laboratories and Public Water Suppliers to directly submit reports via our online system (eDEP). Data submitted via eDEP that has passed the validation routines and is deemed acceptable is automatically passed into WQTS thereby eliminating the manual data entry process being scrutinized here.*

Auditor's Reply:

The audit report does not imply that water quality or public health would be jeopardized by missing or incorrect data recorded in the EPICS WQTS module database, since the Regional Offices did have original source documentation for which not all information had been entered into the database. Our tests indicated that not all test result information existing at the Regional Offices at the time of our audit had been recorded in the EPICS WQTS database in a timely manner. Further, the audit tests indicated that contrary to DEP policies and procedures, monitoring of the information recorded in the WQTS database had not been consistently exercised. We agree with management's decision that the use of the electronic reporting on-line system will enhance monitoring activities over information in the WQTS database.