# 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. 2001-0506-4F**

## OFFICE OF THE STATE AUDITOR'S REPORT ON EXAMINATION OF INFORMATION TECHNOLOGY-RELATED CONTROLS AT THE MASSACHUSETTS HIGHWAY DEPARTMENT JULY 1, 1999 TO MAY 31, 2001

**OFFICIAL AUDIT REPORT**

**MARCH 22, 2001**

2001-0506-4F

TABLE OF CONTENTS

## INTRODUCTION

The Massachusetts Highway Department (MHD) was originally organized as the Department of Public Works under Chapter 16, Sections 1 through 5, of the Massachusetts General Laws, as amended, and is within the purview of the Executive Office of Transportation and Construction (EOTC). Chapter 286, Section 59, of the Acts of 1992, changed the name of the Department of Public Works to the Massachusetts Highway Department. Currently, the Department operates with a staff of 2,135 employees and is overseen by a five-member Board of Commissioners that is chaired by the Department's Commissioner. The Board of Commissioners, which is appointed by the Governor, reviews and approves all Department contracts and major initiatives.

The Department's Chief Engineer is responsible for all operational activities, including construction projects, environmental compliance activities, highway operations, highway engineering, and the supervision of the five district offices. Administrative Services, which includes the Information Technology (IT) section, provides administrative, financial, and technological support to MHD operations. The MHD also contracts with third-party contractors and vendors to obtain specialized professional services, such as those for software development, computer operations, road plowing, and design and construction. The MHD's Deputy Commissioner is responsible for and oversees other Departmental functions, including communications via the Public Affairs section and legal activities via the Chief Counsel section. The MHD operates from a central office in Boston and five district offices, located in Lenox, Northampton, Worcester, Arlington, and Taunton.

The MHD's primary mission is to provide for the planning, design, construction, operation, and maintenance of 12,600 lane-miles of state highway and 2,900 bridges. In addition, the MHD supervises over $600 million of statewide construction projects, exclusive of the Central Artery/Third Harbor Tunnel Project.

The MHD received approximately $143.4 million of state funds and approximately $500 million of federal reimbursements for fiscal year 2000. In addition, the MHD generated revenue of approximately $7.4 million for fiscal year 2000 from sources such as outdoor advertising, reimbursable fuel, signs, access permits fees, load permits, highway inspections, and rentals. MHD processes and reports revenues and expenditures using the Massachusetts Management Accounting and Reporting System (MMARS). In addition, the Department reports Generally Accepted Accounting Principles (GAAP) fixed assets, including those of the Central Artery/Third

Harbor Tunnel Project, to the Office of the State Comptroller for inclusion in the Commonwealth's Comprehensive Annual Financial Report.

At the time of our audit, MHD's computer operations were supported by local area networks (LANs) installed at the central office and the five district offices. MHD processes its business transactions using a number of software applications. Two primary applications include Projis, which is software that tracks projects from inception through the securing of required environmental permits and completion of highway design, and the Administrative/Engineering application, which is software that performs bid processing, tracks construction projects, and generates MMARS payment vouchers related to construction projects. Additional software applications include Permits Management, which is software that records approved permits for road use and records revenue from the issuance of the permits; Fuel Management, which is an application that collects fuel usage data for setting charges for state agencies for highway operations; Accident Records, which is software that collects vehicle crash data for reporting purposes; Maintenance Management System, which is software that tracks employee and equipment usage; and Snow and Ice Billing, which is software that produces voucher payments for third-party contractors who remove snow and ice.

The Office of the State Auditor's examination of IT control practices for this segment of the follow-up IT audit focused on logical access security and business continuity planning.

## AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

### Audit Scope

We performed an information technology (IT) audit at the Massachusetts Highway Department for the period July 1, 1999 through May 31, 2001. The audit was conducted from February 15, 2001 to May 31, 2001. Our audit included a review of the status of audit results and recommendations regarding logical access security and business continuity planning noted in our prior IT audit report (No. 93-0506-4C), issued June 30, 1993.

On March 30, 2001, we issued an interim IT audit report (No. 2000-0506-4F), which covered inventory control over IT-related assets and physical security and environmental protection over IT-related assets and other resources. The current report represents the final segment of the follow-up IT audit.

### Audit Objectives

The primary objective of our audit was to determine whether the issues and recommendations regarding logical access security and business continuity planning from our prior IT audit report (No. 93-0506-4C) had been addressed. In conjunction with our examination of the Department's control practices, we determined whether written and approved policies and procedures regarding logical access security and business continuity planning had been developed and implemented by the MHD central office. We reviewed logical access security procedures used to prevent, detect, and potentially correct unauthorized access or attempts to access MHD files and software installed on various MHD systems. We also sought to determine whether business continuity plans would provide reasonable assurance that mission-critical and essential computer operations could be regained within an acceptable period of time should a disaster render computer systems inoperable or otherwise inaccessible.

Audit Methodology

To determine the scope of the audit, we performed a pre-audit of MHD's IT environment. The pre-audit included interviews with senior management; a review of policies, procedures, and other internal control documentation; and observation of IT-related areas. To obtain an understanding of the Department's activities and internal control environment, our pre-audit also included a review of MHD's mission, organizational structure, and primary business functions. Upon completion of our pre-audit work, we assessed the strengths and weaknesses of the internal control system for selected IT-related activities and determined the scope and objectives of the audit.

To obtain an understanding of, and to evaluate the organization and management of IT operations, we reviewed the Department's organizational structure with respect to IT operations and evaluated reporting lines, job descriptions, and oversight mechanisms. We reviewed IT-related policies and procedures to determine the level of documentation regarding the IT general control areas related to our audit.

To evaluate the adequacy of logical access security controls, we reviewed the Department's policies and procedures regarding the activation and deactivation of access privileges to automated systems and security administration. We reviewed the requirements for logical access security and the means by which the department addressed these requirements. We reviewed MHD's logical access security policies and procedures to prevent, detect, and possibly correct unauthorized access and access attempts to the MHD data files and software installed on ITD's mainframe, MHD's WAN, LAN, and the microcomputer systems. We examined the security procedures in effect with the Systems Director, the LAN Manager, and the Security Officer who were responsible for controlling MHD's access to ITD's mainframe, the Massachusetts Management Accounting and Reporting System (MMARS), Human Resources/Compensation Management System (HR/CMS) and the microcomputer systems. We reviewed the access privileges of those staff who were authorized to access applications residing on ITD's mainframe, the MMARS system, HR/CMS and the microcomputer systems. Subsequently, we determined whether all system users authorized to access the automated systems were required to change their passwords periodically and, if so, the frequency of the changes. Further, we determined whether users were restricted to only the application programs and data files to which they had been authorized. To determine whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed procedures for authorizing access to MHD's data and system resources on ITD's mainframe, the system, and the microcomputer systems. On two separate occasions, we compared the list of individuals authorized to access the automated systems

to the MHD's payroll roster to determine whether they were current employees. We also traced the forms used to grant access to the local area network. To determine whether all access privileges for former staff and consultants were removed from the system, we obtained and compared a list all staff terminations that had occurred from July 1, 1999 to March 31, 2001, including employees and consultants, to those persons with then current access privileges. To document the process of notification of employee termination from Personnel to MHD's IT section, we verified written communications from Personnel to the appropriate IT staff responsible for deactivation of former users of the system.

To assess the adequacy of business continuity planning, we reviewed the extent to which risk management had been performed and recovery steps had been planned and outlined in order to resume computer operations if the mainframes or microcomputer systems were rendered inoperable or inaccessible. We interviewed MHD management to determine whether the criticality of application systems had been assessed; whether risks, threats, and vulnerabilities to computer operations had been evaluated; and whether a written business continuity plan was in place. We also evaluated the adequacy of controls to ensure that data files and software would be available from on-site or off-site locations to support the recovery of automated systems.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted industry auditing practices. The criteria used in the audit came from sources such as the MHD's policies and procedures and from the Information Systems Audit and Control Association's Control Objectives for Information and related Technology (CobiT) control guidelines, which have been developed as a generally applicable and accepted standard for sound IT security and control practices.

## AUDIT SUMMARY

Based upon our examination of general controls, we found that internal control practices needed to be strengthened to provide reasonable assurance that only authorized users would have access to IT resources and that mission-critical and essential functions supported by technology can be recovered within an acceptable period of time.

Although certain access security controls over the Department's automated systems were found to be in place, logical access security controls needed to be strengthened to prevent unauthorized system access and to provide for corrective action if violations were detected. Specifically, controls needed to be strengthened to ensure that user IDs and passwords would be active for only authorized personnel and that access privileges would be deactivated in a timely manner for users no longer needing or authorized to have access. Without proper system access restrictions, persons could gain unauthorized access to system data, and/or programs, thereby placing the MHD at risk of unauthorized use, which could lead to modifications to, and deletions or disclosure of critical or confidential data. We acknowledge that the MHD strengthened its control practices regarding notification to security administrators of users no longer requiring access to automated systems, thereby improving deactivation procedures.

Disaster recovery procedures and business continuity planning for the MHD were not in place at the beginning of the audit, although by the end of our audit field work, the Department had initiated an effort to develop appropriate business continuity plans. Until the recovery and contingency plans are fully developed and tested, we believe that the MHD may be unable to regain processing within an acceptable period of time should the MHD's systems be rendered inoperable or inaccessible. The inability to restore mission-critical and essential systems could have a serious or adverse impact on system users or functional operations.

## AUDIT RESULTS

1. Logical Access Security

Our audit revealed that system access security over the MHD's local area network needed to be strengthened to ensure that access to systems, data, and programs is restricted to only authorized users and to safeguard information against unauthorized use, disclosure, or modification. Procedures needed to be enhanced to ensure that user accounts are documented and to ensure timely action related to suspending and/or closing user accounts.

Although there were written policies and procedures in place to inform the security administrators when an employee or consultant/contractor terminated employment, notification was not always provided to the system security administrator. Further, the procedures for establishing an audit trail of activating and deactivating user accounts needed to be strengthened to provide adequate documentation. Our tests of access security for the WAN and LAN indicated that, contrary to the requirements of the MHD's "Internal Control Manual" and sound access security practices, there were active user IDs for individuals who were no longer employed by the Department. Our tests of the WAN and LAN indicated that 70 (or 6%) out of 1,190 users were not employees or contractor personnel as of February 24, 2001. Upon our request for further explanation, MHD described 20 of the 70 active user IDs as "unknown" and the remainder as former Departmental employees or consultants.

Our review of the forms used by the MHD to grant access to the WAN and LAN revealed that not all employees at MHD had an access authorization form on file. Without such forms, MHD could not readily verify or confirm levels of access privileges granted. We tested a sample of 17 from the above 70 unknown or former employee user IDs to determine whether MHD had on file access authorization forms for these users. MHD was able to provide only three of the 17 requested LAN access authorization forms.

During the review of the Microsoft NT operating system used by MHD to control access to its WAN and LAN, we determined that not all the security features of NT were being utilized. Specifically, when a user ID is established, the Microsoft NT operating system allows the system administrator the option of specifying a start and end date for an ID. This feature is used for temporary employees or consultants who have contracts with start and end dates, rather than for employees for whom an end date is unknown. If one were to assume that many of the 20 "unknown" user IDs alluded to above were consultants, then the use of this access security "start

and end date" feature could have reduced the risk of active and unauthorized system access privileges for consultants under contract.

Recommendation:

In order to improve system security at MHD, the following steps, at a minimum, should be performed:

- Remove, as soon as possible, user IDs of those individuals identified as no longer current staff or contractors.
- Notify security administration of terminations or leave of absences of all appropriate staff in order to further decrease the chance of an account remaining active following the separation of an employee from MHD. A copy of the e-mail notifying termination should be maintained in the Director of Benefits and Employee Programs files and the district support specialist files. By maintaining these records, the Department will have established an audit trail to assist in performing reviews of active system users.
- Based upon MHD's assessment of risk and established level of assurance that access security control objectives are being addressed, MHD management should determine the frequency of required reviews of user IDs to the list of authorized users. We suggest that the review of user IDs be performed at least semi-annually.
- When IT services upgrades from Windows NT to Windows 2000, MHD should:
    - Re-issue the Network Access form, have the forms pre-numbered, have one copy maintained by Human Resources and one copy maintained by IT and have the forms used as part of the semi-annual review.
    - Provide for a unique user number incorporated in to the user profile so that the number can be cross-referenced to HR/CMS and MMARS for future reconciliation.
    - Have the all contractor users' logon privileges secured with a start date and an end date and synchronize these dates with the start and end dates of the associated contract.

Auditee's Response:

*We are in agreement with your recommendations and will take the following action:*

- *All user accounts that are no longer valid (identified during the audit), have been disabled.*

- *IT Services has developed a process with the Director of Employee Programs that provides for proper and timely notifications of terminations through e-mail. The Director of Employee Programs and the Network Manager will keep a hard copy of these notifications on file. This will provide an audit trail for performing reviews of active system users.*
- *IT Services will cross reference active user accounts with the payroll department on a semi-annual basis and disable any anomalies.*
- *IT Services is investigating the impact of reissuing LAN Access Forms to all users as part of the Windows 2000 PC rollout scheduled to commence in August 2001.*
- *The addition of a unique identifier will be made part of the Windows 2000 Server and Active Directory migration project.*
- *Contractor users' logon privileges will be secured with a start and an end date that is associated with the appropriate contract.*

Auditor's Reply:

We are pleased that MHD is taking immediate action to address system access security concerns. During our next IT audit, we will review the MHD's system access security controls and the process by which system access security is managed and monitored.

2. Business Continuity Planning

We determined that, as of the start of our audit, the Department did not have a documented business continuity plan to provide for the timely restoration of mission-critical and essential business functions should systems that are processed through an ITD mainframe or MHD's WAN be rendered inoperable. We acknowledge that by the end of our fieldwork, the Department had started to develop a written business continuity plan.

Although we found that MHD was performing backup procedures for applications residing on its WAN, and ITD was backing up MHD data files at the Chelsea data center, MHD had not designated or tested an alternate processing site to be used in the event that a disaster rendered MHD's offices inaccessible or systems inoperable. The absence of a tested business continuity plan, which designates an alternate processing site, places at risk the Department's ability to regain mission-critical and essential data processing operations that support administrative functions within an acceptable time period.

Because IT operations supporting the Department are located at ITD and at the Department's Boston and five district offices, the business continuity plan should take into account recovery strategies to address various scenarios, including the of loss of IT components for each on of the processing sites. The Department's and ITD's efforts to ensure that backup copies of data files and

programs are being stored both on and off site is a good step toward addressing a necessary requirement for viable recovery plans. While some of the risks to IT operations were being mitigated by good physical security and environmental protection at MHD and at the ITD facility, to help ensure that all potential risks are addressed and to obtain assurance regarding the practicality and viability of the recovery plans, recovery strategies should be documented and tested. Without a formal, comprehensive recovery and contingency plan that includes required user area plans and network communication components and has been sufficiently tested, the Department could be inhibited from accessing information related to the MMARS, PARS, and HR/CMS systems residing on an ITD mainframe, or to WAN or microcomputer-based applications residing at MHD and its district offices. As a result, MHD would be hindered from obtaining information needed for administrative functions or for information related to planning, designing, constructing, operating, and maintaining the state's highways and bridges.

The objective of business continuity planning is to help ensure the continuation of mission-critical and essential functions should a disaster cause significant disruption to computer operations. Business continuity planning for information services is part of business continuity planning for the entire organization. Generally accepted practices and industry standards for computer operations support the need for MHD to have an ongoing business continuity planning process that assesses the relative criticality of information systems and develops appropriate contingency and recovery plans, if required. To that end, MHD should assess the extent to which they are dependent upon the continued availability of information systems for all required processing or operational needs and develop its recovery plans based on the critical requirements of its information systems.

The assignment of impact should identify the extent to which departmental business objectives and functions are affected over various time frames of the loss of processing capabilities. The assessment of criticality and impact of loss of processing should assist the Department in triaging its business continuity planning and recovery efforts.

The MHD, in conjunction with ITD, should perform a risk analysis of the IT systems supporting the Department to more clearly identify the impact of lost or reduced processing capabilities. The risk analysis should identify the relevant threats that could damage or preclude the use of the systems and the likelihood and potential frequency of each threat. The success of the business continuity planning process requires management commitment. Senior management and system users should be closely involved in business continuity planning to help ensure that there is a clear understanding of the entity's information system environment, that determinations of system criticality and the risks and exposures associated with the systems are correct, that appropriate data processing and user area plans are developed based on the relative critical character and importance

of systems, and that adequate resources are available. The recovery strategies should address potential scenarios of loss of IT operations and should be based upon the results of risk analysis and an assessment of processing requirements.

Recommendation:

The MHD should establish a business continuity planning framework that incorporates critical and impact assessments, business continuity plan development, risk management, recovery plan testing and maintenance, training, and communication. Disaster recovery procedures should be developed to ensure that the relative importance of the Department's systems is evaluated on an annual basis, or upon major changes to user requirements. The MHD should also conduct a formal risk analysis of its IT-related components, including outsourced services provided by ITD, on an annual basis, or upon major changes to the relevant IT infrastructure or to business operations or priorities. Based on the results of the risk analysis and criticality assessment, MHD should confirm its understanding of business continuity requirements and, if necessary, amend recovery plans to address mission-critical and essential IT-supported business functions.

The MHD should ensure that the business continuity plan provides recovery strategies with respect to all potential disaster scenarios. The recovery plan should contain all pertinent information needed to effectively and efficiently recover mission-critical and essential operations within the needed time frames. In addition, the MHD should ensure that appropriate user area plans are in place and sufficiently understood by administrative and operational management, as well as staff, to enable business areas to continue their operations should automated processing be lost for an extended period of time. The user area plans should take into account unavailable processing due to a loss of mainframe, WAN or microcomputer-based system operations.

We recommend that the business continuity plan identify alternative sites for business operations and data processing. We further recommend that the business continuity plan be tested and formally reviewed and approved. The plan should be periodically reviewed and updated when necessary to ensure that it remains appropriate to recovery needs. The MHD should ensure that management and staff are adequately trained in the execution of the plan. The completed plan should be distributed to appropriate management and staff members, and a copy should be stored in a secure off-site location. Since recovery actions to be taken may need to be made in concert with ITD, or other third parties, we recommend that recovery tests be coordinated with ITD and any other required third parties and that a copy of the plan be available to appropriate ITD and third-party personnel.

Auditee's Response:

*As acknowledged in the Auditor's report, the Department has started to develop a written Business Continuity Plan/Disaster Recovery Plan. The Department's current plans provide for vendor response service contracts, back-ups, manual paper based fall backs and redundant connections to ITD. The Department acknowledges the necessity to develop a more detailed plan that includes:*

- *A plan for multiple disaster or disruption scenarios. Each scenario will include a flow chart for both IT and business processes and a contact list with current phone numbers.*
- *An alternate processing site will be identified for each major location (e.g., Districts 1 - 5 and Ten Park Plaza).*
- *All continuity plans and alternate processing information will be detailed in the Internal Control Manual and kept in both electronic and paper format at all major locations.*
- *The Business Continuity plans will be reviewed and approved by appropriate management personnel and where applicable will become part of our Standard Operating Procedures.*

*IT services appreciates your recommendations and will make every effort to follow through accordingly in an effort to make improvements in our Business Continuity Plans and tightening controls in our Access Security.*

Auditor's Reply:

We reiterate the need to maintain, test, and review and approve business continuity plans and establish a framework for business continuity planning with procedures requiring risk management, recovery, contingency plan testing, business continuity plan maintenance, and appropriate training for assigned business continuity responsibilities. The plan should also include reference to the staff assigned the responsibility for its on-going maintenance and procedures should ensure that the business continuity plan be reviewed and approved upon update to ensure that it accurately reflects the most current information.