A. JOSEPH DeNUCCI
AUDITOR

The Commonwealth of Massachusetts

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

NO. 2004-0307-4T

OFFICE OF THE STATE AUDITOR'S
REPORT ON THE EXAMINATION OF
INFORMATION TECHNOLOGY-RELATED CONTROLS AT
THE DEPARTMENT OF TELECOMMUNICATIONS AND ENERGY

JULY 1, 2001 through APRIL 30, 2004

OFFICIAL AUDIT REPORT
JULY 6, 2004

TABLE OF CONTENTS

INTRODUCTION

The Department of Telecommunications and Energy (hereinafter referred to as DTE) was created in 1919 and is organized under Chapter 25 of the Massachusetts General Laws (MGL) and operates within the purview of the Office of Consumer Affairs and Business Regulation (OCABR) under Chapter 24, Section A of the MGL. Until 1998, DTE was known as the Department of Public Utilities. A five-member Commission appointed by the Governor oversees the DTE. The Governor designates one of the commissioners as the chairman. At the time of our audit, DTE was comprised of an Executive Director, a Deputy Director, and 157 staff, including a legal counsel, an MIS Director, and nine additional division directors. For the 2004 fiscal year, DTE's appropriation was $7,443,364, including a budgetary appropriation of $6,910,413 and funding for the Transportation Division of $532,951. DTE's budget was funded, to a large extent, by assessments against electric, gas, telecommunications, and cable companies. DTE received $3,270,321 from assessments on electric power companies for Department activities performed under the aegis of the Electric Restructuring Act, Chapter 164 of the Acts of 1997. The Restructuring Act required the Department to monitor the developing competitive market for natural gas and electric power. In addition, DTE received $466,132 federal grant money, including $456,411 for Pipeline Security, $2,803 for Motor Carrier Safety Assistance, and $6,918 for "Dig Safe" activities. DTE's administrative office is located in Boston.

The DTE's primary mission is "to ensure that utility customers are provided the most reliable service at the lowest possible cost as determined by its orders; to protect the public safety from transportation and gas pipeline related accidents; to oversee the energy facilities siting process; and to ensure that residential ratepayers' rights are protected under regulations." According to DTE documents, the Department has "regulatory authority over a significant portion of the Commonwealth's economy."

The Department is comprised of eleven divisions, including the Executive Division, Legal Division, and nine operating divisions. The nine divisions were responsible for a wide range of activities from ensuring public safety to setting rates and ensuring service quality for businesses, such as investor-owned electric power, natural gas, telecommunication, transportation, and cable industries. DTE earned revenue of approximately $5,364,879 from business operations and services for the 2003 fiscal year. (See Appendix A, page 16 for a description of the Division's business functions and revenue earned for the 2003 fiscal year)

At the time of our audit, DTE's computer operations were supported by nine file servers and approximately 215 microcomputer workstations configured in a local area network. Two additional servers were used by Management Information Systems (MIS) for testing. The file servers were connected through a wide area network (WAN) to the Executive Office for Administration and Finance's Information Technology Division (ITD) mainframe, which provides connectivity for access to the web-based Human Resources Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS), the Commonwealth's accounting system. The primary software used by DTE to support its business functions was business-related applications, such as word processing and Access databases. In addition, a Disk Operating System (DOS) database application, operating on a microcomputer workstation, was used to report statistical information to the federal government regarding the Single State Registration Program (SSRS).

Our examination focused on selected general controls, such as physical security and environmental protection, system access security, inventory control over IT-related resources, and business continuity planning, including on-site and off-site storage of magnetic media. In addition, we reviewed control practices regarding the issuance of school bus driver certificates and identification decals under the SSRS.

AUDIT SCOPE, OBJECTIVES, AND METHODOLOGY

Audit Scope

From August 18, 2003 to April 30, 2004 we performed an audit of selected information technology (IT) related controls at the Department of Telecommunications and Energy (DTE) for the period of July 1, 2001 through April 30, 2004. The scope of our audit included an examination of control practices, procedures, and devices regarding physical security and environmental protection over and within the administrative office and the data center housing the file servers at DTE. We reviewed DTE's awareness of and compliance with the Executive Office for Administration and Finance's Information Technology Division's (ITD) "Enterprise Information Security Policy." We reviewed and evaluated system access security to DTE's automated systems, including file servers and microcomputer workstations. In conjunction with our review of system access security, we reviewed and evaluated selected control practices regarding DTE's security over its network configuration. In addition, we examined inventory control practices for computer equipment and software. In conjunction with our audit, we reviewed formal IT-related policies and procedures.

Regarding system availability, we reviewed business continuity planning for the daily administrative and financial operations processed through the automated systems. With respect to normal business functions, we reviewed the adequacy of formal policies and procedures regarding business continuity planning, including the provisions for on-site and off-site storage of backup copies of magnetic media. We reviewed procedures for generating and transferring backup copies of critical magnetic media to an off-site storage location. We evaluated physical security and environmental protection controls over backup media stored on-site. In addition, our scope included a review of the Transportation Division's control practices regarding the issuance of annual school bus driver certificates and identification decals to intrastate and interstate commercial carriers. For selected periods during the 2003 and 2004 fiscal years, we reviewed the reliability of data recorded in the applications reviewed, compliance with statutory authority and Commonwealth regulations, and the accuracy and completeness of revenue received for the school bus driver certificates and identification decals.

Audit Objectives

Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that IT resources would be safeguarded, properly accounted for, and available

when required. We sought to determine whether appropriate security controls were in place and in effect to provide reasonable assurance that only authorized parties could access IT-related resources and that system information was sufficiently protected against unauthorized disclosure, change, or deletion. In addition, we determined whether adequate controls had been implemented to provide reasonable assurance that only authorized users were granted access to the network and the office business applications residing on the microcomputer workstations. We sought to determine whether adequate control procedures were in place over the network configuration to prevent and detect unauthorized access to automated systems. In addition, we sought to determine whether DTE was aware of ITD's "Enterprise Information Security Policy," as of November 2001 and had complied with its provisions. We sought to determine whether adequate physical security and environmental protection controls were in place and in effect to restrict access to IT resources to only authorized users in order to prevent unauthorized use, damage, or loss of these resources.

We sought to determine whether adequate business continuity planning had been performed and whether plans were in place to restore mission-critical and essential business operations in a timely manner should the automated system be unavailable for an extended period. Further, we determined whether adequate control procedures were in place regarding on-site and off-site storage of backup copies of magnetic media. Another objective was to review and evaluate control practices regarding the accounting for IT-related resources, including computer equipment and software.

We sought to determine whether all requirements regarding the completion of applications and the submission of supporting documents were performed prior to the issuance of school bus driver certificates and identification decals to interstate and intrastate motor vehicle carriers; the application process was in compliance with statutory authority and Commonwealth regulations; and whether revenue received for the period under review was correct, properly accounted for in Department records, and deposited in the bank in a timely manner.

Audit Methodology

To determine our audit scope and objectives, we initially obtained an understanding of DTE's mission and business objectives. Through pre-audit interviews with the managers and staff and reviews of the website and selected documents, such as the "Transitional Briefing to Governor Romney, December 2002," business operations and statutory authority, we gained an understanding of the primary business functions supported by the automated systems. We documented the

significant functions and activities supported by the automated systems and reviewed automated functions related to operations designated as mission-critical or essential. Further, we gained an understanding of the significant manual components of selected business functions performed by the DTE's eleven divisions.

As part of our audit work, we reviewed and evaluated the organization and management of IT operations at the administrative office. In that regard, we reviewed relevant policies and procedures, reporting lines, and job descriptions. In conjunction with our audit, we determined whether written, authorized, and approved policies and procedures for control areas under review had been implemented. We determined whether the policies and procedures provided management and users sufficient standards and guidelines to describe, review, and comply with statutes, regulations, generally accepted control objectives for IT operations and security, and policy directives, such as ITD's "Enterprise Information Security Policy," as of November 2001.

We interviewed DTE management to discuss internal controls regarding physical security and environmental protection over and within the administrative office and data center housing the automated systems and the on-site storage area. We inspected the administrative office, including the data center, reviewed relevant documents, such as the internal control plan, and performed selected preliminary audit tests. In conjunction with our review of internal controls, we performed an assessment of risks and threats to selected components of the IT environment.

To determine whether physical access over IT-related resources, including computer equipment, was restricted to only authorized users and that the IT resources were adequately safeguarded from loss, theft or damage, we performed audit tests at the administrative office. We reviewed physical security and environmental protection over IT-related equipment through inspection and interviews with DTE management and staff. To determine whether adequate controls were in effect to prevent and detect unauthorized access to the offices housing automated systems, we inspected physical access controls, such as locked entrance and exit doors, the presence of a security officer at the entrance to the building housing DTE offices, a receptionist at the entrance point to the administrative office, and whether visitors were required to sign in/out. We reviewed access control procedures, such as the list of staff authorized to access the administrative office and data center, and control practices regarding the management of card-key access to the building housing DTE business offices, data center and other restricted areas within the office. As an additional test

of physical security, we compared the list of employees with active access privileges to the business offices and data center to the current personnel roster as of September 2003.

To determine whether adequate environmental protection controls were in place to properly safeguard automated systems from loss or damage, we checked for the presence of smoke and fire detectors, fire alarms, fire suppression systems (e.g., sprinklers and inert-gas fire suppression systems), an uninterruptible power supply (UPS), surge protectors for automated systems, and emergency power generators and lighting. We reviewed general housekeeping procedures to determine whether only appropriate office supplies and equipment were placed in the data center or in the vicinity of computer-related equipment. To evaluate temperature and humidity controls, we determined whether appropriate dedicated air conditioning units were present in the data center. Further, we reviewed control procedures to prevent water damage to automated systems, official records, and on-site storage for backup copies of magnetic media.

With respect to system access security, our audit included a review of access privileges of those employees authorized to access the network and associated microcomputer workstations. To determine whether DTE's control practices regarding system access security adequately prevented unauthorized access to automated systems, we initially sought to obtain policies and procedures regarding system access and data security. We reviewed security practices with the MIS Director and evaluated selected access controls to the network and applications residing on the network and microcomputer workstations. Further, we reviewed DTE's control procedures regarding remote access privileges to the network. In addition, through interviews with the Deputy Director, Executive Director, and the MIS Director, physical observations, reviews of documentation, and selected audit tests, we determined whether DTE was aware of ITD's "Enterprise Information Security Policy," and whether stated control practices were in place and in compliance with the policy. We determined whether DTE's internal control documentation included control practices, such as a risk assessment, an acceptable use policy for IT resources, and security awareness training required by ITD's "Enterprise Information Security Policy."

To determine whether the administration of logon ID and passwords was being properly carried out, we reviewed and evaluated control practices regarding system access security. We reviewed the security procedures with the MIS Director responsible for access to the automated systems on which the Department's business-related applications operate. In addition, we reviewed control practices used to assign DTE staff access to the application programs and data files. To determine

whether adequate controls were in place to ensure that access privileges to the automated systems were granted only to authorized users, we reviewed and evaluated procedures for authorizing, activating, and deactivating access to application software and related data files. Because DTE did not maintain documentation authorizing users to be granted access to automated systems until December 2003, we reviewed a sample of these documents provided to us by DTE management for employees hired after December 2003. To determine whether 172 (100%) users with active privileges were current employees or outsourced staff, we obtained the list of individuals granted access privileges to the network and business-related applications and compared all users with active access privileges, as of September 2003, to DTE's personnel roster of current employees. We determined whether all employees authorized to access the automated systems were required to change their passwords periodically and, if so required, we reviewed the frequency of the changes.

Regarding inventory control over IT-related resources, we first reviewed formal policies and procedures promulgated by the Massachusetts Office of the State Comptroller (OSC) regarding inventory control. To determine whether IT-related resources were being properly safeguarded and accounted for, we reviewed the roles of the MIS Director and Computer Operations Supervisor regarding the accounting for computer equipment and software, reviewed the inventory control procedures for IT resources, and performed selected tests. We determined whether DTE was complying with Operational Services Division (OSD) regulations for the disposition of surplus property.

During our audit period, we obtained the hardware inventory record with a listed value of $223,245 as of December 10, 2003. To determine whether the IT-related inventory record was current, accurate, and complete, we initially chose a statistical sample of 102 (25.6%) of 397 pieces of computer equipment, including 194 monitors and 203 central processing units listed on the record for review. We then attempted to confirm the selected pieces of equipment recorded on the inventory list to the actual computer equipment installed at the Department. We determined whether computer equipment installed at the administrative office was tagged with state identification numbers and whether the tag numbers were accurately listed on the inventory record. Further, we confirmed nine file servers with a listed value of approximately $102,000 to the equipment installed in the data center. In addition, we confirmed a judgmental sample of 34 pieces of equipment located at the Department to the hardware inventory record. We compared the tag numbers attached to the computer equipment to the corresponding numbers listed on the record and determined whether serial numbers were accurately recorded on the record. We reviewed the

inventory record to determine whether appropriate "data fields," such as state identification number, manufacturer's model number, serial number, location, and cost were included in the record. In addition, we determined whether adequate controls were in place to properly account for 46 laptop computers.

To determine whether equipment purchased during the 2002 and 2003 fiscal years were listed on the inventory record and located at DTE offices, we confirmed 45 pieces of equipment with a listed value of $20,642 to the inventory record and to the actual equipment on hand. Further, we reviewed software inventory control practices, including the current software inventory record with a listed value of $44,537.

To assess disaster recovery and business continuity planning, we reviewed the adequacy of formal business continuity plans to resume mission-critical and essential operations in a timely manner should the file servers and the microcomputer workstations be unavailable for an extended period. We reviewed and evaluated the authorized and approved business continuity plan as of February 20, 2004. We interviewed the MIS Director and selected business managers to determine whether the criticality of application systems had been assessed, whether risks and exposures to computer operations had been evaluated, and whether a written business continuity plan was in place. In addition, we interviewed the Transportation Division's Director and Assistant Director and the directors of the Rates and Revenue Requirements Division and the Natural Gas Division to determine the impact on program operations should the automated systems be unavailable for an extended period.

To determine whether controls were adequate to ensure that data files and software for business applications would be available should the automated systems be rendered inoperable, we interviewed the MIS Director responsible for generating backup copies of magnetic media. Further, we reviewed the adequacy of provisions for on-site and off-site storage of backup copies of mission-critical and essential magnetic media at the administrative office. We reviewed procedures for transferring to and retrieving backup media from the off-site storage location. We did not visit the off-site storage location. We did not review ITD's backup procedures for transactions processed through the Massachusetts Management Accounting and Reporting System (MMARS) and the Human Resources Compensation Management System (HR/CMS).

Regarding selected business functions performed by the DTE's Transportation Division, we gained and recorded an understanding of the control practices for the granting of annual school bus driver

certificates and the issuance of identification decals to interstate and intrastate commercial carriers under the aegis of the Single State Registration Program. We reviewed the adequacy of physical security controls regarding the applications, associated documentation, and checks received for the certificates and decals issued. In conjunction with our review, we interviewed the MIS Director and the Transportation Division's Director and Assistant Director. To determine whether all requirements were met prior to the issuance of school bus driver certificates, we selected a judgmental sample of 183 applications received during March and June of the 2003 fiscal year and August and September of the 2004 fiscal year for review. Further, we chose a judgmental sample of 103 applications for identification decals for the months of January, May, and June of the 2003 fiscal year and November of the 2004 fiscal year. During the 2004 fiscal year, DTE processed approximately 5,455 school bus applications and 4,578 identification decals for common carriers. We then reviewed the applications to determine whether all required fields, such as fee amount, applicant's signature, appropriate driver's license, successful completion of road tests for new drivers, and vehicle insurance were completed. We also reviewed the files for the presence of required documentation, such as the medical report and the Registry of Motor Vehicle's "Commercial Driver's License Score Sheet." We confirmed whether DTE had performed a Criminal Offender Record Information (CORI) review required for all school bus driver certificates and had documented the CORI check in the application. We reviewed the date stamp recorded on the application. To determine whether appropriate controls were in place to ensure that revenue received for the bus driver certificates and identification decals was correct, properly accounted for in Department records, and deposited in the bank, we examined the processing of three consecutive days of receipts obtained by DTE during February 2004.

Our audit was conducted in accordance with Generally Accepted Government Auditing Standards (GAGAS) of the United States and generally accepted computer industry control practices and auditing standards.

AUDIT CONCLUSION

Based on our audit at the Department of Telecommunications and Energy (DTE), we found that adequate physical security and environmental protection controls were in place and in effect to provide reasonable assurance that automated systems were properly safeguarded and protected from damage or loss. Our audit indicated that although important control practices were in place and in effect to provide reasonable assurance that IT-related resources were properly accounted for in DTE records, certain controls needed to be strengthened. With respect to system access security, we determined that adequate controls were in place and in effect to provide reasonable assurance that only authorized users could access IT-related resources and that system information was sufficiently protected against unauthorized disclosure, change, or deletion.

Regarding availability of systems, our audit disclosed that adequate control practices were in place to provide reasonable assurance that normal business operations could be resumed for DTE in a timely manner should the file servers or the microcomputer workstations be unavailable for an extended period. Further, we determined that control practices regarding on-site and off-site storage of backup copies of magnetic media for administrative and programmatic activities processed at DTE were adequate.

Our audit disclosed that control practices regarding the approval and issuance of annual school bus driver certificates and identification decals to intrastate and interstate commercial carriers by the DTE's Transportation Division were appropriate and complied with statutory authority and Commonwealth regulations, that all applications were properly completed and supporting documentation was provided, and that revenue received for the time period examined was correct, documented in Department records, and deposited in a timely manner.

Our review of internal controls indicated that management was aware of the need for internal controls, had a defined organizational structure for the Department, an established chain of command, clearly delineated reporting responsibilities, and documented job descriptions for the MIS Director and information technology staff. Our audit revealed that DTE's internal control plan included certain control procedures regarding the designation of the Executive Director as the internal control officer, selected physical security procedures regarding DTE's administrative office, and descriptions of financial management systems. DTE should further develop its policies and procedures regarding environmental protection, management and control over IT resources, and system access security. Further, appropriate officials should sign the current version of the plan and

the effective date of implementation should be indicated on the plan. In addition, our audit indicated that DTE was aware of and in compliance with certain control practices documented in the Executive Office for Administration and Finance's Information Technology Division's "Enterprise Information Security Policy," such as an IT-related risk assessment, acceptable use of IT resources, and business continuity planning (See Summary of Internal Control Practices, Appendix B, page 19.)

Our audit revealed that appropriate physical security controls had been implemented over and within the building housing the DTE administrative office. Responsibility for physical security had been assigned to the Executive Director and the Deputy Director. Further, the controls included security officers stationed at the main entrance to the building and foot patrols inside and outside the building 24/7. All visitors were required to show identification to the security guard. Further, temporary passes were processed though an automated system and issued to the visitors prior to admittance to DTE offices and visitors were escorted within the business offices. With respect to the DTE administrative office, we determined that the primary entrance/exit to the office was staffed for entrance to the administrative office, and that employees were required to use card-keys to access all business offices at all times and to the building after normal business hours. According to DTE management, two additional points of entry to business offices were limited to certain Department officials, managers, and staff; the entrances were monitored by a security officers; and staff were required to use card-keys or key pads for access. Adequate control practices were in place regarding the activation and deactivation of card-keys. We found that all staff granted physical access to both the business offices and data center were listed on the DTE's official roster of current employees.

Our audit disclosed that the file server room was located in a non-public area that could not be accessed from outside the building, the door to the room was locked at all times, and access to the room was restricted to IT staff employed by DTE. With respect to confidential client information in hardcopy form, we determined that sufficient controls were in place to protect records from unauthorized access. To improve physical security controls, we recommend that DTE management consider the installation of security cameras within DTE business offices.

We found that adequate environmental protection, such as smoke detectors and alarms, sprinkler systems, and an emergency power supply were in place in the building housing DTE's administrative office to help prevent damage to, or loss of, IT resources. We confirmed that a vendor had tested

the fire alarms on a regular basis and fire drills were conducted periodically. Our audit indicated that the data center was neat and clean, general housekeeping procedures were adequate, and temperature and humidity levels within the room were appropriate. There was a dedicated air-conditioning unit installed in the room. We found that an uninterruptible power supply (UPS) device was in place to permit a controlled shutdown and to prevent a sudden loss of data. Hand-held extinguishers were located within the data center. Evacuation and emergency procedures were documented by building management and available in the administrative office. To strengthen environmental controls, we recommend that DTE periodically review policies and procedures, modify documentation when appropriate, and include the policies and procedures in the Department's internal control plan.

Our audit disclosed that DTE had developed appropriate procedures regarding authorization and recording of access privileges to automated systems and activation of logon IDs and passwords. We found that informal procedures were in place to deactivate access privileges for users no longer authorized or needing access to the automated systems. These procedures had not been documented. Because DTE did not maintain documentation authorizing users to be granted access privileges to automated systems until December 2003, we were unable to determine whether all users had been properly authorized. DTE provided selected documents authorizing access privileges for users hired after that date. Users were assigned access levels by appropriate supervisors based upon pre-determined "roles" of the staff. Further, all users were required to sign a formal statement acknowledging the confidentiality of their passwords and commitment to protect the password from unauthorized use and/or disclosure. Audit tests of access security that compared 172 (100%) DTE users to the Department's personnel roster of current employees, as of September 2003, indicated that these users were current employees or outsourced staff. DTE should ensure that for all system users that the authorization to use IT system has been authorized.

With respect to logon ID and password administration, we determined that to access automated systems, users were required to enter a logon ID and password and that passwords were required to be changed periodically. Adequate documentation was in place regarding password formation and use, including minimum length of passwords and schedules for password changes. We found that DTE had implemented appropriate controls regarding remote access to network resources by the staff. To improve controls over system access security, we recommend that DTE document control practices regarding authorization to access automated systems, activation of logon IDs and

passwords, and deactivation/deletion of access privileges. These policies and procedures should be included in the DTE's internal control plan.

Our audit revealed that, at the close of our audit, adequate control practices and procedures were in place to provide reasonable assurance that IT-related resources were properly accounted for in Department records. We determined that DTE had complied with important control practices required by the Internal Control Act, Chapter 647 of the Acts of 1989, and associated requirements regarding fixed-asset management promulgated by the Office of the State Comptroller, as of the 2003 fiscal year. On our recommendation, DTE tagged computer equipment with state identification numbers and provided us with a hardware inventory record that included appropriate fields, such as state identification number, serial number, location, and cost. Our audit tests indicated that, with few exceptions, computer equipment was properly tagged with state identification numbers and that, except for laptop computers, the inventory record with a listed value of $223,245, as of December 10, 2003 was current, accurate, and complete. When notified of errors, DTE took corrective action to affix tags to equipment and update the inventory record. Additionally, we found that a separate inventory record was maintained for 46 laptop computers. The record included appropriate fields, such as state identification number, serial number, location, and date of purchase. Further, the record contained important information regarding the current status of the laptops, including the number of computers distributed to staff, used on site, placed in storage, or designated as surplus. We determined that DTE was aware of Operational Services Division requirements regarding surplus property and was collaborating with the Division to dispose of certain property. In addition, software licenses for the business-related applications were appropriately on file at the administrative office.

To strengthen inventory control over IT-related resources, we recommend that DTE maintain a perpetual inventory record. Purchases of equipment should be entered into the inventory record within seven days of acquisition as required by the Office of the State Comptroller and surplus equipment be removed from the inventory record and recorded on a surplus inventory in a timely manner when the asset is no longer in service, but is still in the custody of the agency. In addition, physical inventory and reconciliation should be conducted at least annually, as required by the OSC. Further, cost figures for laptop computers should be included in the inventory record. DTE should document policies and procedures regarding management and control over IT resources and include the documentation in the internal control plan.

Our audit disclosed that DTE had developed a business continuity plan as of February 2004 that outlined a strategy for maintaining system availability in the event of a major disaster or disruption of IT operations. The plan included important control practices, such as a criticality assessment, a list of IT-related resources, and a description of telephone and voice mail review and evaluation of risks to systems, projects, and vendors, and recovery strategies to address potential disruptions. Further, the plan included classification of types of delays or disruptions for each division and procedures to help staff resume normal business operations. Potential alternate processing sites had been designated and recovery of network services had been tested. We acknowledge that DTE had ready access to on-site and off-site backup tapes and had appropriate procedures in place to perform its normal business functions manually or with limited IT resources. To improve controls, we recommend that testing of systems and recovery strategies be updated in the plan and that DTE maintain a current contact list of staff and telephone numbers in the event of an emergency.

Our audit indicated that adequate control procedures were in place regarding on-site and off-site backup of magnetic media. We determined that DTE had implemented procedures and schedules for generating backup copies of magnetic media, and had documented procedures for maintaining descriptions of data files and software that were backed up. Documentation was in place indicating which backup tapes were stored off-site and logs were maintained demonstrating the authorized schedule for the transport and return of backup copies. We also found that physical security and environmental protection over the on-site storage location was adequate. We did not visit the storage facility housing off-site backup copies of magnetic media.

We determined that adequate control practices were in place to provide reasonable assurance that all requirements for the granting of school bus driver certificates and identification decals for intrastate and interstate commercial carriers were performed prior to the issuance of the certificates and decals. Our audit revealed that all fields in the application forms were properly completed, appropriate documentation was submitted, and the fees for the certificates were correct. In addition, we found that, for the time period examined, all revenue received was correct, properly accounted for in Department records, and deposited in the bank in a timely manner. To strengthen controls, we recommend that DTE management implement a separate review of checks prior to processing by accounting staff.

Auditee's Response:

> *We are pleased with your findings that our internal control systems for IT resources are appropriate and welcome your suggestions for improvement. Specifically, we will download the Comptroller's advisory on inventory control and model our procedures accordingly.*

Auditor's Reply:

We agree with DTE management's decision to comply with Office of the State Comptroller's requirements regarding IT-related fixed-asset management and control and will address our recommendations. We will review inventory control over IT resources at our next audit. In addition, we reiterate that DTE should review its internal control documentation and strengthen policies and procedures regarding environmental protection, inventory control over IT resources, and system access security.

Name of Division	Description of Business Functions	Revenue Source(s)	Amount of Revenue
Telecommunications Division	Supports the Commission regarding regulation of $3 billion telecommunication industry in the Commonwealth and ensures that telecom companies provide most reliable telecom resources at lowest cost by reviewing new registrations from companies providing telecom services; reviewing individual tariff filings for new services or to change rates, terms, conditions of existing services; monitoring quality of service for incumbent local exchange carrier (Verizon), analyzing major federal regulatory decisions; and enforcing Department regulations and policies	N/A	N/A
Energy Facilities Siting Board	Independent nine-member review board ensures reliable energy supply for the Commonwealth with minimum impact on environment at lowest cost. Licenses construction of major infrastructure, such as power plants, electric transmission lines, natural gas pipelines, and storage facilities.	Utility siting fees	$0
Natural Gas Division	Supports Commission in regulation of Commonwealth's 10 investor-owned natural gas companies (aka local distribution companies or "LDCs") serving approximately 1.4 million customers with operating revenues of $1.7 billion..	N/A	N/A
Electric Power Division	Subsequent to passage of Electric Industry Restructuring Act in 1997, Division ensures that Commonwealth electric companies provide reliable distribution and customer service at lowest cost and retail competitive suppliers provide generation service consistent with Department regulations and Restructuring Act.	N/A	N/A

Name of Division	Description of Business Functions	Revenue Source(s)	Amount of Revenue
Cable Television Division	Oversees 10 cable television operators serving 1.9 million cable subscribers in 309 of Commonwealth's 351 cities and towns. Retains ultimate authority in licensing issues.	CTV franchise fees	$1,561,864
Rates and Revenue Requirements Division	Provides technical expertise for DTE to determine appropriate rates and charges for 7 investor-owned electric companies, 9 gas companies, and 25 water companies in Commonwealth. Assists Legal Division in developing evidentiary record in legal proceedings regarding rates or finances of public natural gas, electric or water companies.	N/A	N/A
Consumer Division	Responsible for enforcing and monitoring compliance with Mass laws and DTE regulations protecting consumers of gas, electricity, telecom, water, and cable services. Over 1,000 companies are monitored (largest number is telecom companies). Responds to approximately 85,000 telephone inquiries and investigates approximately 12, 000 complaints annually.	N/A	N/A
Pipeline Engineering and Safety Division	Responsible for technical and safety oversight of 10 natural gas companies and 4 municipal companies. As certified agent of US Department of Transportation enforces federal regulations pertaining to natural gas distribution pipelines and gas safety regulations. Enforces "dig safe" law, inspects and tests gas meters for accuracy and safety.	Meter inspections Fines and Penalties, Dig Safe	$869,260 $146,390

Name of Division	Description of Business Functions	Revenue Source(s)	Amount of Revenue
Transportation Division	Provides regulatory oversight over motor vehicle and railroad common carriers; regulates 2,500 intrastate and 1,500 interstate carriers, such as residential movers, hazardous waste haulers, and tow companies authorized to conduct business in Commonwealth. Regulates Commonwealth's regional transportation authorities and MBTA bus, trolley car, and subway system. Regulates over 300 bus companies providing route, charter, and sightseeing services. Decisions affect commuters, consumers and public safety. Issues permits for motor, bus, and school bus driver certificates	SSRS, document copies, bus driver exams, bus inspections, motor stock acquisitions, fees: cab cards, certification, permits, and applications, truck decals/RMV, towers reports, tariff filings, bus permits, bus driver licenses, stamps	$2, 574, 307
Executive Division	Provides administrative support to the Department for procurement, financial management, management information systems, public relations, human resources, payroll, and budget preparation; Liaison to OCABR and EOAF's Fiscal Affairs Division and Human Resources Division.	Document filings, late fees, sale of forms, miscellaneous income	$213,058
Legal Division	Provides legal support to all Department divisions; Attorneys preside over adjudicatory proceedings and conduct rulemakings; Division provide primary liaison with the Legislature, specifically Committees on Government Regulation and Energy	N/A	N/A
		Total Revenue:	$5,364,879

Pg.ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	**Adequacy of Documentation**
11	Physical Security	Provide reasonable assurance that only authorized staff can access business offices, file server room, microcomputer workstations, and client records in hardcopy form to prevent unauthorized use, loss or damage	Control over access to offices, computer rooms, file servers, and microcomputer workstations; designated facilities manager; intrusion detection devices; locked doors, foot patrols	In Effect	Yes	Adequate
11	Environmental Protection	Provide reasonable assurance that IT-related resources operate in an appropriate environment and are adequately protected from loss or damage	Proper ventilation, temperature control, fire alarms, fire suppression mechanisms, water sprinklers, posted emergency procedures	In Effect	Yes	Adequate

Status of Control-Key:

In Effect = Control in place sufficient to meet control objective.

None = No internal control in place.
Insufficient = Partial control in place but inadequate to meet control objective.

Adequacy of Documentation-Key:
Adequate = Standard or guideline sufficient to describe, review, and follow significant controls.
Inadequate = Standard or guideline insufficient to describe, review, and follow significant controls.
N /A = Not Applicable

Pg. ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation.
12	System Access Security	Provide reasonable assurance that only authorized users are granted access to the automated systems	Passwords required to access automated systems, changes of passwords required at least every 60 days; formal rules for password formation and use; formal procedures for deactivation of logon IDs and passwords	In Effect	Yes	Adequate, except for procedures to authorize, activate, and deactivate access to automated systems
13	Inventory Control over IT-related Resources	Provide reasonable assurance that IT-related resources are properly safeguarded, accounted for in the inventory record.	Maintenance of an up-to-date inventory record; hardware tagged with state ID tags; annual physical inventory and reconciliation performed; sign-out/in log for laptop computers	In Effect	No	Inadequate
14	Business Continuity Planning	Provide reasonable assurance that DTE can restore mission-critical and essential functions in a timely manner should file servers and microcomputer workstations be rendered inoperable or be inaccessible.	Current, formal, tested business continuity plan; alternate processing site; periodic review and modification of plan; plan implemented and distributed; and staff trained in its use	In Effect	Yes	Adequate

Pg.ref	Control Area	Control Objective	Control Activities	Status of Control	Documented Controls	Adequacy of Documentation
14	On-site storage	Provide reasonable assurance that backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Magnetic media backed up nightly; appropriate records maintained of backup; physical access security and environmental protection of storage are adequate; storage area is a separate on-site location	In Effect	Yes	Adequate
14	Off-site storage	Provide reasonable assurance that critical and important backup copies of magnetic media are available should computer systems be rendered inoperable or inaccessible	Same as above. Storage area in a separate off-premises location	In Effect	Yes	Not reviewed
14	Issuance of school bus driver certificates and identification decals; Receipt of revenue for certificates and decals	Provide reasonable assurance that all requirements regarding completion of applications and submission of supporting documentation prior to issuance of certificate or decal; Revenue received was correct, properly accounted for in Department records, and deposited in bank in timely manner.	Adequate security over applications and documents; all required fields in applications completed and appropriate documentation submitted; applicant signature on application; fees correct for certificate or decal issued; correct amount entered into records and deposited on time	In Effect	No	No