Commonwealth of Massachusetts
Office of the State Auditor
Suzanne M. Bump
Making government work better

Official Audit Report – Issued July 20, 2011

The Department of Transportation's Office of Information Technology's Activities Relating to the Registry of Motor Vehicles

For the period July 1, 2009 through October 31, 2010

TABLE OF CONTENTS/EXECUTIVE SUMMARY

The Massachusetts Department of Transportation (MassDOT) was established in June 2009 by Chapter 25 of the Acts of 2009, An Act Modernizing the Transportation Systems of the Commonwealth of Massachusetts, which required the Commonwealth to integrate transportation agencies and authorities into a new, streamlined MassDOT to be established by November 1, 2009. A five-member Board of Directors appointed by the Governor with expertise in transportation, finance, and engineering was established to oversee the new organization and serve as the governing body of both MassDOT and the Massachusetts Bay Transportation Authority (MBTA), which is part of MassDOT but retains a separate legal existence. MassDOT's Office of Information Technology (OIT) currently maintains, supports, and operates all network and telecommunications infrastructure and is responsible for application design and development as well as application maintenance and support for all MassDOT information technology (IT) operations, including the RMV's application systems.

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an evaluation of MassDOT's OIT's general controls over information technology. The audit, which covered the period July 1, 2009 through October 31, 2010, included an examination of OIT's general controls pertaining to program change controls for Registry of Motor Vehicles (RMV) application systems and logical access security controls in place to protect the integrity and confidentiality of data within the Automated Licensing and Registration System. Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that OIT controls over program changes to the RMV's application systems were in place and in effect to process all requests (including maintenance and patches) for changes to application systems in a standardized and controlled manner.

Based on our review we have concluded that during the period July 1, 2009 through October 31, 2010, MassDOT's OIT maintained adequate internal controls regarding program changes to the RMV's application systems and processed changes to application systems in a standardized and controlled manner. However, as addressed in the Audit Results section of this report, we found that OIT's controls over logical access security needed to be enhanced to provide reasonable assurance that only authorized users would have access to MassDOT/RMV applications.

Our audit disclosed that although certain logical access security controls were in place, other control practices needed to be enhanced to provide reasonable assurance that only authorized users have access to MassDOT network resources, certain information technology application systems, and data files. Although OIT had adequate password administration controls and security procedures in place and in effect to authorize and activate user privileges for access to MassDOT's and RMV's network resources, we found controls needed to be enhanced regarding the timely deactivation or deletion of network

user accounts for staff and contractors who are no longer employed by MassDOT/RMV. We also found that OIT did not have procedures in place to ensure that generic accounts that are not assigned to individual users are periodically reviewed for current activity and that their use is linked to authorized users. In addition, we determined that OIT did not have formal enterprise-wide logical access policies and procedures governing user access to network resources and the RMV's mission-critical Automated Licensing and Registration System. The absence of adequate controls over logical access security may place critical and personally identifiable information at risk by allowing unauthorized users to modify, delete, or disclose sensitive information.

INTRODUCTION

Background

The Massachusetts Department of Transportation (MassDOT) was established by Chapter 25 of the Acts of 2009, An Act Modernizing the Transportation Systems of the Commonwealth of Massachusetts, which required the Commonwealth to integrate transportation agencies and authorities into a new, streamlined MassDOT to be established by November 1, 2009. A five-member Board of Directors appointed by the Governor with expertise in transportation, finance, and engineering was established to oversee the new organization and serve as the governing body of both MassDOT and the Massachusetts Bay Transportation Authority (MBTA), which is part of MassDOT but retains a separate legal existence.

MassDOT is administered by a Secretary of Transportation appointed by the Governor to serve as Chief Executive Officer. The organization oversees four divisions: Highway, Mass Transit, Aeronautics, and the Registry of Motor Vehicles (RMV), in addition to an Office of Planning and Programming. MassDOT's mission is to deliver customer service to people who travel in the Commonwealth and to provide safe and reliable transportation systems in a way that strengthens our economy and quality of life.

MassDOT's Office of Information Technology (OIT) currently maintains, supports, and operates all network and telecommunications infrastructure, including business applications, networks, servers, architecture, telephones, mobile devices, desktop computers, and Internet services. OIT is also responsible for application design and development as well as application maintenance and support for all MassDOT divisions' information technology (IT) operations, including the RMV's application systems.

The RMV's mission is to provide customer service in issuing driver's licenses, vehicle registrations, and titles while also protecting public safety through its development of vehicle and traffic safety programs. The agency conducts outreach and education on vehicle and traffic safety through its partnerships with cities, towns, other agencies, and professional associations. To achieve this goal, the RMV issues and maintains records related to motor vehicle registrations and operator's licenses; enforces motor vehicle laws to promote highway safety by ensuring that every driver meets minimum competency standards, and revokes driving privileges from violators of motor vehicle laws who are deemed to be an immediate threat to other drivers. The RMV is also responsible for

collecting fees for registrations, titles, driver's licenses, special plates, inspection stickers, and other miscellaneous fees, and remitting them to the Office of the State Treasurer.

The RMV's mission-critical application, which is called the Automated Licensing and Registration System (ALARS), was developed in mid-1980 as the RMV's mainframe and database for all registry transactions. ALARS is used to maintain all records for Massachusetts-licensed drivers, including licenses, registrations, criminal and civil citations, inspection stickers, and various miscellaneous fees. The RMV's offices are able to access ALARS data files and software directly through the wide area network (WAN) connected to the Executive Office for Administration and Finance's Information Technology Division (ITD) mainframe containing the ALARS database. Through the WAN, the workstations also provide access to the state's Human Resources/Compensation Management System (HR/CMS) and the Massachusetts Management Accounting and Reporting System (MMARS).

Audit Scope, Objectives, and Methodology

In accordance with Chapter 11, Section 12, of the Massachusetts General Laws, we performed an evaluation of MassDOT's OIT's general information technology controls at RMV. The audit, which covered the period July 1, 2009 through October 31, 2010, included an examination of OIT's general controls pertaining to program change controls to RMV application systems and logical access security controls[1] in place to protect the integrity and confidentiality of data within ALARS.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Our audit was also conducted in accordance with generally accepted industry practices. Audit criteria used in the audit included management policies and procedures and control guidelines outlined in Control Objectives for Information and Related Technology (CobiT version 4.1) issued by the Information Systems Audit and Control Association, July 2007.

[1] Logical access controls are controls designed to protect computer resources from unauthorized modification, loss, or disclosure, specifically those controls that prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically. U.S. Government Accountability Office Testimony: Information Security Weaknesses Place Commerce Data and Operations at Serious Risk, August 3, 2001. GAO-01-1004T.

Our primary audit objective was to determine whether adequate controls were in place to provide reasonable assurance that OIT controls over program changes to the RMV's application systems were in place and in effect to process all requests (including maintenance and patches) for changes to application systems in a standardized and controlled manner. In this regard, we sought to determine whether the IT-related internal control environment, including policies, procedures, practices, and organizational structure, provided reasonable assurance that application program changes to the RMV's business systems were authorized and documented, and that changes were developed, tested, and implemented in a secure environment. We also sought to determine whether OIT-related roles and responsibilities for program modification and maintenance were clearly defined, points of accountability were established, and appropriate change control and logical access policies and procedures were in place. We assessed the adequacy of controls in place to protect the integrity and confidentiality of data within ALARS. We also determined whether only justified and approved changes are made; only authorized individuals have access to application program codes and related data files; test and production environments are adequately segregated; all program changes are adequately documented; and considerations for data and system integrity, security, and availability are made during the change control process.

To determine our audit scope and objectives, we initially reviewed the RMV's internal controls to obtain an understanding of the RMV's mission and business objectives. Through pre-audit interviews with OIT managers and staff and a review of documentation such as descriptions of IT organization and operations, we gained and documented an understanding of the primary business functions supported by IT systems. To assess the adequacy of the planning, design, development, and testing of program changes to application systems, we requested and obtained a listing of program change control projects completed during the period July 2009 through August 2010. To select a project, we reviewed the project request, date, and number of budgeted hours. In addition, we reviewed 60 closed change management projects for the period July 2009 through August 2010 that required approximately 200 to 17,000 work hours to complete. Based on our review, we judgmentally selected for testing an RMV project that would enable an automobile owner to return license plates at a stand-alone kiosk.

To determine whether requests for system changes were implemented in a structured manner, we evaluated our sample project to ensure compliance with OIT's policies governing the change application software used by OIT to define, document, prioritize, and report progress throughout the change management control process. We found that the OIT developer may use one or a

combination of three third-party project management tools during the development phase to organize, manage, and protect software codes. The project management tool ultimately used to code the change is determined by whether the request is associated with a licensing-, web-, or mainframe-based application.

To evaluate whether appropriate controls were in place to ensure that emergency changes are justified and approved, documented, developed, tested, and moved to production in a timely manner, we reviewed documentation and assessed OIT's change application software. To assess the adequacy of the planning, design, development, and testing of program changes to application systems, we compared the Information System Audit and Control Association's generally accepted standards for change management controls to our sample project, including system change requests, project evaluations, risk assessments, program change approvals, resource allocations, testing processes, and program quality assurance.

With respect to logical access security, our audit included an examination of privileges of those programmers and developers authorized to access the network and associated IT systems. To evaluate whether only authorized user access could be gained to the MassDOT/RMV network and systems, we reviewed the access security policies and procedures with OIT's Business Application Director. To determine whether logical access security controls were in place and in effect, we reviewed and evaluated the administration of logon IDs and passwords and selected control practices regarding logical access to network resources. Our audit included an evaluation of password configuration and whether all persons authorized to access computing systems were required to change their passwords periodically and, if so, the frequency of the changes. To assess whether all users with active privileges were current employees, we obtained a list of programmers, developers, and individuals granted access to project management applications and other business-related applications, such as ALARS, and compared a list of all users with active access privileges composed of 2,380 user IDs as of October 8, 2010 to MassDOT's list of then-current employees and outsourced staff. To determine whether access privileges that were no longer required or authorized were disabled in a timely manner, we also compared the active network user listing to MassDOT's listing of terminated employees and their respective termination dates.

Based on our review we have concluded that, during the period July 1, 2009 through October 31, 2010, OIT maintained adequate internal controls regarding program changes to the RMV's application systems and processed changes to application systems in a standardized and controlled

manner. However, as addressed in the Audit Results section of this report, we found that OIT's controls over logical access security needed to be enhanced to provide reasonable assurance that only authorized users would have access to MassDOT/RMV applications.

AUDIT RESULTS

IMPROVEMENTS NEEDED IN LOGICAL ACCESS SECURITY CONTROLS

Our audit disclosed that although certain logical access security controls were in place, other control practices needed to be enhanced to provide reasonable assurance that only authorized users have access to the Massachusetts Department of Transportation's (MassDOT) network resources, certain information technology (IT) application systems, and data files. MassDOT's Office of Information Technology (OIT) had adequate password administration controls and security procedures in place and in effect to authorize and activate user privileges for access to MassDOT and Registry of Motor Vehicles (RMV) network resources. However, we found that controls needed to be enhanced regarding the timely deactivation or deletion of network user accounts for staff and contractors who are no longer employed by MassDOT/RMV. We also found that OIT did not have procedures in place to ensure that generic accounts that are not assigned to individual users are periodically reviewed for current activity and that their use is linked to authorized users. In addition, we determined that OIT did not have formal enterprise-wide logical access policies and procedures governing user access to network resources and the RMV's mission-critical Automated Licensing and Registration System (ALARS).

Our audit revealed that OIT had controls in place that provide for password creation, expiration, logon, and password configuration requirements and that procedures were in place that require new hires and contractors to receive a Criminal Offender Record Information check and sign the appropriate user acceptance and security agreements. However, we found that OIT did not have controls in place to disable or deactivate MassDOT/RMV employee access privileges for users who terminate employment or transfer to other agencies. Our audit included an evaluation of 2,380 active user accounts consisting of 1,409 accounts associated with employees and 971 generic user accounts. Our audit tests revealed that of the 1,409 active user accounts, 365 (26%) were no longer associated with MassDOT/RMV. OIT subsequently reviewed our findings and found that of the 365 user IDs not associated with MassDOT's list of current employees, 118 were valid user IDs applicable to external agencies requiring access to the ALARS or user IDs associated with employees who may have had a recent name change. OIT also identified 95 user IDs designated as needing to be deleted and 152 that required further investigation.

Our review of the 971 generic accounts not linked to identified users found nine valid accounts associated with OIT and six that were disabled. However, our analysis of the remaining 956 generic accounts found that there were 840 non-OIT active accounts, 111 non-OIT "test" accounts, and

five pseudonyms not associated with an identifiable person. OIT subsequently identified the status and owners of 908 generic accounts as valid and determined that 36 of the 908 needed to be disabled and that 12 required further investigation.

The failure to deactivate user accounts in a timely manner places MassDOT/RMV at risk of unauthorized use of established privileges, such as using another individual's user account having higher access privileges, or to unauthorized access. For example, areas of significant impact would include the handling of ALARS transactions that involve the exchange of cash and the suspension/revocation of licenses.

Our audit also disclosed that OIT did not have formal enterprise-wide logical access security policies and procedures to enable management to guide operations in a consistent manner and allow employees to understand their roles and responsibilities within predefined limits. We noted that on November 1, 2009 OIT assumed operational control at the secretariat level for MassDOT's subsidiary agencies, including the RMV, and that OIT is now in the process of formalizing enterprise-wide policies and procedures for all IT-related functions.

Recommendation

We recommend that OIT strengthen its access security controls to ensure that access privileges for unauthorized users are deactivated or modified when a change in the employee's status results in the user no longer requiring access to IT resources, or when a change in an employee's position or responsibilities requires a change in access privileges. To ensure that user levels of authorization and access privileges are properly maintained, we recommend that MassDOT/RMV implement formal notification procedures requiring that electronic notification or a standard form be used by human resources or department management to notify OIT personnel of changes in employee status, such as terminations, extended leaves of absence, or employee transfers. OIT should also implement controls to periodically review generic user accounts to ensure these accounts are only used by authorized employees and, when appropriate, are deactivated. In addition, we recommend that OIT expedite its review of the 152 user and 12 generic accounts that require further investigation. This will help to ensure that sufficient security controls are in place to protect the confidentiality and integrity of important and sensitive data and to limit access to data and system functions to authorized parties, only. We also recommend that OIT aggressively pursue completion of its enterprise-wide policies and procedures for all IT security initiatives. Formally documented policies and procedures will enable IT management to ensure compliance with existing rules and regulations and help to mitigate risks associated with the unauthorized use of user accounts.

Auditee's Response

MassDOT's Information Technology department is dedicated to providing secure and effective services to the MassDOT Divisions as well as the citizens of the Commonwealth. This audit has uncovered a few areas where we can improve our security and it is our goal to meet the recommendations outlined by the State Auditor's team in this report. Our review of the outstanding 152 user and 12 generic accounts will be completed by April 15, 2011. Following this review, all subsequent account deactivations will be completed by April 29, 2011; this will address both user and generic accounts. To ensure that access privileges are properly secured, we have put a three-fold process into place:

1. ***Immediate Employee Separation Response:*** *Upon notification from Human Resources that an employee is no longer working for MassDOT, an email is sent to representatives of IT and the RMV, alerting all necessary parties that user accounts and access privileges must be disabled. The following areas are covered in this response:*
    a. *User Accounts*
    b. *VPN Accounts*
    c. *ALARS Accounts*
    d. *Email Accounts*
    e. *Application Access not governed by Windows Authentication*

This is documented in Standard Operating Procedure IT-NET-001-006 IT Procedures – Actions Upon Employee Separation.

2. ***Monthly Review of Separated Employees:*** *Human Resources will provide a list of all employee separations, year-to-date, to IT. This list will be reviewed to ensure that all account deactivations have been completed. Some employee separations come with requests to keep accounts active for a period of time to facilitate knowledge transfer or accommodate professional needs, and this monthly review will ensure that these accounts are closed out. This is documented in Standard Operating Procedure – DRAFT – User Account Review Protocols.*

3. ***Quarterly Review of Generic User Accounts:*** *IT will conduct reviews of all generic user accounts every 90 days to determine if they are still in active use. This will ensure that generic user accounts that are created for testing efforts or projects are still necessary. IT will also require a deactivation date for all future generic user accounts. This is documented in Standard Operating Procedure – DRAFT – User Account Review Protocols.*

These procedures are industry best practices and have been followed in the past within our organization, but have never been formally documented. We have taken this audit as an opportunity to codify our processes and will continue to make necessary adjustments as they arise.