Fairfax County Internal Audit Office

Department of Vehicle Services and
Department of Purchasing and Supply Management
Fleet Management and Maintenance Services Audit
Final Report

August 2015

"promoting efficient & effective local government"

Introduction

The Fairfax County Department of Vehicle Services (DVS) provides fleet management and maintenance services to the County and the Fairfax County Public School (FCPS) vehicle fleets. DVS employees work at the Government Center and at four maintenance facilities located at Alban, Jermantown, Newington and West Ox. The four maintenance facilities service and maintain approximately 6,437 vehicles, including 1,540 school buses. The DVS administrative office, motor pool vehicles and some County agency vehicles are located at the Government Center.

DVS provides additional services including: maintaining the County's fuel program, and 53 fuel sites; road side emergency repair services; vehicle replacement (reserve fund); the County motor pool consisting of 41 vehicles; as well as technical support and review for all County vehicle purchases. The Department of Purchasing and Supply Management (DPSM) supports DVS by providing inventory report reconciliations, inventory spot checks and oversight of County vehicle inventory management, including vehicle auction sales. There were approximately 3,600 County vehicles, with an approximate book value of $268.5 million at the end of fiscal year 2014. DVS manages vehicle maintenance, repair and inventory information on the M5 Fleet Management System (M5), a web-based application system.

Executive Summary

Our audit was to determine the adequacy of controls over the purchase, internal billing, repairs, maintenance, inventory management and recording of vehicles managed by DVS and DPSM. We found that internal billings were performed timely and in accordance with the established rates and proper segregation of duties was in place. Vehicle purchases were properly monitored and controlled. Sufficient documentation was kept on file to support repairs and maintenance expenses; data input into M5 appeared to be complete and accurate; and an adequate disaster recovery plan was implemented and tested.

However, we noted the following control weaknesses related to vehicle inventory management and M5 system controls:

- County agencies were not performing periodic physical verifications of vehicle inventories. As a compensating control, DPSM employed an alternative verification method by performing reconciliations of FOCUS and M5 inventory reports, which provided some oversight over vehicle inventories. DPSM has updated the County policy to strengthen vehicle inventory controls, and the required periodic review changed from three years to every two years.

- Source code of M5 system software was not held in an escrow to safeguard against failure by the vendor to properly maintain or update the software.

- The M5 system did not produce a complete audit trail for system users, which is needed to effectively track and detect security violations, performance problems and flaws in the application.

- The M5 system did not have adequate password controls, which allowed system administrators to view all user passwords.

- There was no formal process to grant and document M5 system users' access, increasing the risk of unauthorized access.

Scope and Objectives

This audit was performed as part of our fiscal year 2014 Annual Audit Plan and was conducted 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. The audit covered the period of January 1, 2013, through December 31, 2013 and our audit objectives were to determine that:

- Department billings for work completed was accurate.
- Adequate supporting documentation was maintained for vehicle repairs and services.
- Adequate separation of duties exists over vehicle repairs, maintenance and services.
- Vehicle inventories were properly accounted for.
- M5 system access controls were adequate.
- M5 system had proper password controls.
- M5 system contained adequate audit log data.
- Adequate data backup and restore procedures existed for the M5 system.
- Revenue collected from auction sales was accounted for properly.

Methodology

Our audit approach included interviewing management and staff of areas responsible for billing, recording and collection of revenue; vehicle inventory oversight; vehicle services; and M5 system maintenance and access controls. We conducted walk-throughs of business processes and M5 system operations and controls; performed various reconciliations; and performed testwork on a sample of internal billings, vehicle services and related accounting system reports. Also, we obtained and reviewed sample documentation of M5 system screen prints, reports, and a copy of the M5 user guide to obtain an understanding of the business processes and controls in place.

The Fairfax County Internal Audit Office (IAO) is free from organizational impairments to independence in our reporting as defined by Government Auditing Standards. We report directly and are accountable to the County Executive. Organizationally, we are outside the staff or line management function of the units that we audit. We report the results of our audits to the County Executive and the Board of Supervisors, and IAO reports are available to the public.

Findings, Recommendations, and Management Response

1. Verification of Vehicle Inventory

County agencies were not performing periodic physical verifications of their vehicle inventories. As a compensating control, DPSM employed an alternative verification method by performing yearly reconciliations of vehicles recorded in the M5 system, FOCUS vehicle inventory reports and M5 vehicle service reports, which provided some oversight over vehicle inventories. However, vehicles not serviced in the past 12 months were not accounted for and physically verified by County agencies to ensure existence.

DPSM's *Accountability of Fairfax County's Accountable Equipment (PM12-03)* requires County agencies conduct regular physical inventory verifications. Physical counts and verifications of vehicle inventories reduce the risks of unauthorized use and theft of vehicles as well as erroneous vehicle accounting records.

Recommendation: We recommend the County agencies with vehicles not verified by DPSM's alternative validation process perform physical verification of all vehicles not serviced in the prior 12 months and reconcile them to FOCUS in compliance with *PM 12-03.* DPSM should provide oversight for the physical verification of vehicles not processed through this alternative verification method. During our audit, DPSM updated the policy to include the alternative verification method and changed the required review period from three to every two years.

Management Response: This finding is based on FY2014 procedures. In FY2015, DPSM required and oversaw departments' physical verification of vehicles not reconciled through the alternative validation method described above. This requirement was formalized in the recent revision to PM12-03. This item was implemented in July 2015.

2. M5 Application System Source Code

The M5 application system source code was not deposited in an escrow account to protect the County in the event the vendor goes out of business, files for bankruptcy or fails to maintain and update the software. The source code controls the processing of data and the functionality of the software and is essential for any ongoing development or proper maintenance of the software application. A copy of the up-to-date source code must be in escrow to ensure the continued operation and maintenance of the software if the licensor becomes unable to do so. Lack of a software escrow agreement could result in interruption of the operation, maintenance of the software and disruption of critical operations.

Recommendation: We recommend DVS consult with DPSM and consider entering into a source code escrow agreement with the vendor. The source code escrow agreement should include but not be limited to the subject and scope of the escrow, licensor's obligation to put updated versions of the software in escrow in specific intervals, the conditions that must be met for the agent to release the source code to the licensee, etc. Upon entering into the agreement, we recommend DVS periodically monitor the information being stored with the escrow company to ensure it is up to date.

Management Response: Prior to the next contract expiration of December 31, 2017, DVS will work with DPSM to negotiate a source code escrow agreement. AssetWorks recently provided DVS with a quote of $1,000 per year to have a third party hold the source code. The price would be higher for Fairfax County to hold the code. Management anticipates completing this item by October 31, 2017.

3. Audit Trails for System Users

The M5 system did not produce a thorough audit trail of changes by system administrator roles or other system users. The audit trail is the evidence that demonstrates how a specific action was initiated, processed, and summarized. It should enable management to determine who performed the action, what the action accomplished, and when the action was taken.

The audit trail report generated by the application contained the date, time, user ID and record content, but did not provide the nature of the change. There was no before and after image of the record contents in the audit trail information. There were five users with system administrator roles.
These roles had the capability to delete database and audit trail records, and create accounts, user roles and reports.

The Fairfax County *Information Technology Security Policy (PM 70-05.01)* mandates the use of audit log trails for all confidential and sensitive data. These audit logs should include records of all modifications to the databases, granting or removing user access and creating accounts and reports. The presence of a thorough audit trail can assist management in detecting violations, reconstructing events, and resolving application processing problems.

Recommendation: We recommend M5 be configured to produce reports of all user activities occurring on production databases and the overall system. Also, management should review audit trail reports periodically (at least monthly).

Management Response: According to AssetWorks, there are no specific audit trial reports in the system. However, DVS can look at individual tables in the database to see who made changes, updates and deletions, and will do so monthly. Security in the system is based on roles, and each role has access to only the minimum necessary functionality. Management anticipates completing this item by July 31, 2015.

4. M5 Application Password

Our review of M5's password capabilities for compliance with Fairfax County *Information Technology Security Policy* (*PM* 70-*05.01*) identified several weaknesses. The application did not enforce the use of strong passwords that include special characters or case sensitive with a minimum of 6 characters. Password changes were not required by a new user the first time an account was established. Passwords were not encrypted and were not required to be changed at a specific time frame (60 days or 90 days). As a compensating control, a user can only access the M5 system through the County network, which has strong password controls. However, the M5 system and data is still at risk for unauthorized access by users after they gain access to the County network.

The County's IT Security Policy requires the following for strong passwords:

- All initial passwords should be changed,
- Passwords shall be routinely changed (at a minimum, not longer than every 90 days),
- Passwords should adhere to a minimum length of six characters,
- Passwords should adhere to a specific case sensitive format of uppercase letters, lowercase letters, numbers and special characters,
- Passwords should not be anything that can be easily tied back to the account owner: user name, SSN, nickname, relative's names, birth date, etc.,
- Passwords shall not be dictionary words or acronyms, and
- Password history shall be retained to prevent the reuse of a password.

Failure to encrypt passwords and not enforcing password changes the first time an account is established, allows the system administrator(s) to view the users' passwords. In addition, by not enforcing strong passwords, both the system and the data are more vulnerable to unauthorized access through password cracking.

Recommendation: We recommend DVS request the vendor upgrade security in the application to support strong password requirements during next upgrade or update of the M5 system. In accordance with IT Security policy #70-05.01, this requirement in the policy should be adhered to in all newly created systems and system development. This should be documented in the M5 procedures and implemented at training sessions.

Management Response: As discussed with Internal Audit at the exit meeting, DVS will require users with a system administrator role in M5 to comply with the IT Security policy regarding strong password requirements. Management anticipates completing this item by July 31, 2015.

5. User Access Authorization Documentation

DVS did not have a formalized process to grant and document user access. DVS IT support manager received the request for adding or changing user access rights to the M5 application through e-mail; however, DVS did not keep e-mail communications for these requests. A review of M5 users showed a former County employee still had access to the system.

Fairfax County Information Technology Security Policy 70-05.01 states that, all accounts created shall have an associated request and approval that is appropriate for the Fairfax County system or service. System administrators or other designated staff:

- Are responsible for removing the accounts of individuals who change roles within Fairfax County or are separated from their relationship with Fairfax County.
- Shall have a documented process to modify a user account to accommodate situations such as name changes, accounting changes, and permission changes.

The lack of a standardized access request form creates risks of granting users excessive access rights, adding new users, or changing users' access rights without a manager's approval, and keeping transferred or terminated users active in the system.

Recommendation: We recommend DVS use a standard access request electronic form or email to document authorization and modification of access privileges approved by an authorized manager, and maintain the completed forms or emails on file. Additionally, formal written procedures should be developed and communicated to employees. Finally, the County employee with inappropriate access should be removed.

Management Response: As discussed at the exit meeting, DVS will formalize a procedure where the system administrator is notified by DVS HR when an employee is hired, transferred or terminated. Role change or new user requests will be sent to the system administrator by email and a copy sent to the DVS assistant director for administration. The system administrator will confirm approval of the role change or new user request with the employee's supervisor and maintain all emails on file. Management anticipates completing this item by August 31, 2015.