



# Fairfax County Internal Audit Office

**Department of Tax Administration  
Revenue Collection Process Audit  
Final Report**

**May 2005**

*"promoting efficient & effective local government"*

# Executive Summary

We found the overall controls for collecting, depositing, and posting personal property revenue were sufficient and operating effectively. Our review of the transaction process and documentation for personal property revenue collections concluded that personal property revenue collections were deposited in a timely manner and accurately posted to customer accounts and the accounting records for the period reviewed. DTA maintained a current list of authorized users with appropriate system profiles to match their job responsibilities. Software changes were also authorized, documented, and maintained accordingly. However, specific areas where internal controls can be strengthened include the adjustment documentation process and the physical control and accountability over cash. In addition, we identified system access weaknesses that can be improved to protect application data. General controls improvement is needed in system maintenance, and documentation over the revenue collection systems.

The primary issues noted were:

- Documentation supporting adjustments to personal property revenue collection did not provide a complete audit trail.
- Accountability over cash collected by express tellers during SMILES was not in place in some cases.
- There was excessive access to system production records which could allow unauthorized or inaccurate modification of database records, tables, queries, and reports.
- Due to the use of proprietary software, password management and access controls were not in line with County Information Technology Security Policy.
- System administration duties were not adequately documented.
- There was a need for a coordinated system development consolidation effort.

Certain security related and revenue collection information has been omitted from general disclosure. This information would, if disclosed, subject the County to potential system vulnerabilities and operational disruptions.

## Scope and Objectives

This audit was scheduled as part of our Fiscal Year 2004 Annual Audit Plan and was conducted in accordance with Generally Accepted Government Auditing Standards. The audit covered the period from January 2003 through June 2003 and the period during the SMILES program. Our objectives were to determine that:

### **DTA Revenue Collections**

- Personal property revenue collections were deposited in a timely manner.
- Collections were accurately posted to customer accounts and accounting records.
- Adjustments to collections were accurate.
- Controls were in place to prevent loss or theft of payments.
- Collections through the SMILES Program were adequately safeguarded

## **DTA System Controls**

- A current list of authorized users was available and up-to-date and system profiles matched job responsibilities.
- Physical and logical access controls were in place to prevent or detect unauthorized access to DTA's (Revenue Collection Division) mainframe and client/server application systems.
- Access to computer systems was monitored, security violations were investigated, and appropriate remedial actions were taken.
- Authorizations for software modifications were documented, maintained, and properly authorized.
- Adequate documentation had been developed to cover system administration functional duties and system development coordination.

## **Methodology**

Our audit approach included interviewing appropriate employees, observing employee work functions, conducting detailed testing of the Revenue Collection Division's transactions on a sample basis, and performing a review of the general system controls over financial information produced. We evaluated the processes for compliance with Accounting Technical Bulletins and the United States Government Accountability Office's Federal Information System Controls Audit Manual.

We did not examine system controls for all of the applications used in the DTA revenue collection process. We concentrated our system examination on the most significant applications, Cashier for Windows (CFW) and Revenue Collector (RC) systems. This scope limitation does not alter our conclusion about the revenue collection process. The Fairfax County Internal Audit Office is free from organizational impairments to independence in our reporting as defined by the generally accepted 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 we audit. We report the results of our audits to the County Executive and the Board of Supervisors, and reports are available to the public.

## **Findings, Recommendations, and Management Response**

### **1. Adjustments to Personal Property Revenue Collection Report Documentation**

Transaction reports reviewed from January through June 2003 revealed daily written adjustment notations to individual cashier collection totals by revenue type. These also included amounts reported for deposit as recorded on the Daily Report of Tax Collections. The adjustments did not identify the individual making the corrections, the date the correction was made, or any evidence of approval of the amended amounts. Daily adjustments to transaction reports for amounts collected from taxpayers and revenues for deposit should identify the person making the adjustment, the date, and the reason for the adjustment. In addition,

approval of the adjustment should be documented. These records serve as a control reference for postings to the ALIS and FAMIS systems and support amounts credited on the bank statements. The causes necessitating these corrections are: pre-paid taxes; seriously delinquent taxes; reclassification of personal property taxes and decal fees; collections from some organizations not established on the ALIS system, missing account or property numbers in the ALIS system rejecting acceptance of the transactions; and necessary adjustment notations to the Daily Report of Tax Collections due to late submissions of Cashiers work to the deposit room for verification.

**Recommendation:** Management should require that all written adjustment notations be documented to reflect the initiator, approval and the date performed. This should include adjustments made to the Cashier Export Download Report, Daily Report of Tax Collections, Personal Property Distribution Reports pertaining to amounts to be deposited, classification of revenues collected, and individual taxpayer collections. Adjusted transactions or totals should also indicate a brief reason as to why the adjustment was necessary. This is of particular importance for those adjustments that are material in nature.

**Management Response:** The audit was conducted during the implementation of the Real Estate Tax module. DTA was still formulating business practices at that time. Since the Internal Audit study personal property and decals have been split into two distinct payment types. Payment posting is a batch process using files from Revenue Collector, the program that accumulates all CFW workstations. Payment posting is not driven by the Daily Tax Reconciliation Report (DTCR) or the deposit. If a property number should be incorrect there is no impact to or from the DTTCR. The entry to post that particular payment properly is fully documented in the personal property system's audit trail. A cashier can no longer submit a "late" balance sheet. If a cashier cannot balance within the scheduled time a supervisor must be notified. The implementation has resulted in automation that eliminates the need for the manual tracking described in the audit findings. DTA recommends that this item be categorized as complete.

## 2. **Production Access by DIT Programmers**

DIT programmers had access to production records for the Cashier for Windows (CFW) and Revenue Collector (RC) systems. They had access to both the production (s572kgc11) and development (s572kgc12) servers. The DIT programmers:

- a. Provided support to the DTA Technical Section to maintain and coordinate change control issues with the vendor as necessary.
- b. Used the date activated maintenance feature in CFW to change system profiles at the request of DTA through a change management request.
- c. Used the date activated maintenance feature to change screen settings and configurations.

Programmers should not have access to production data when they are also

responsible for modifying, testing, and distributing program changes. Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed and that improper program changes could be implemented without the knowledge of the user department. The division of duties between DTA and DIT was established during CFW and RC implementation. A programmer acting independently could inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies.

**Recommendation:** We recommend DTA work with DIT Server Support Branch staff to restrict DIT programmers to the development (s572kgc12) server only, similar to the access arrangement that exists with the vendor. DTA's change requests should be programmed and tested by the DIT programmers in the development region as they are currently done and moved over to production after DTA's approval in a controlled manner. DIT programmers should never have continuous access to the production (s572kgc11) server for data and programs.

**Management Response:** DIT Programmers provide troubleshooting support to the users/cashier supervisors when real-time problems occur. DIT access to production is required to troubleshoot problems in real time and to expediently adjust payment postings. Application changes are implemented in the development region and tested by DTA prior to migration to the production environment. Changes are moved to production only after DTA approval. Change management procedures (CSCRs) have been instituted to track the migration process.

DTA appreciates the risk(s) associated with granting production access to DIT. DTA will revisit this issue in March 2006 once the product integration with IAS and full functionality has been implemented. During the period (3/05 – 3/06) DTA will keep a record of issues requiring immediate turnaround. The number of documented incidents will be the basis for continuing/discontinuing DIT's access to production. If product stability is achieved during this evaluation period DIT access to production will be revoked. In the interim DIT restrictions to production access will be explored with DIT's server branch.

### 3. Excessive Permission Rights

DTA and DIT users had excessive permission rights from their desktop computers to access the Cashier for Windows and Revenue Collector systems on the network. The CFW and RC systems were installed on the same network drive where the application data, programs, and system files reside. The CFW and RC users and the DIT support staff had full access (read, write, and execute) to change or delete files that may cause irreversible damage and denial of service to these client/server based application systems. If the data is found to be corrupt, system availability may be delayed until DIT completes the restore process, and there would be no assurance for the reconstructed data.

CFW and RC users were set up on the same network drive and the logical folder (SIIHome) to a production server designated as 's572kgc11' in DTA. Not all CFW users had authorized access to the RC system and the reverse is true as well.

However, they all had logical network access to the production server where the CFW and the RC systems were installed.

Appropriate logical access controls should help protect against unauthorized modification or manipulation of:

- Operating systems (executable files) and data (database files)
- Integrity and availability of information (by restricting the number of users and processes with access)
- Confidential information from being disclosed to unauthorized individuals

Access should be granted to system users based on the least privilege principle as prescribed in the County's Information Technology Security Policy. The current Windows 2000 Server Active Directory setup provides users with unrestricted permission rights to the network drive and the logical folder that allow them to access the application files even though they may not be authorized CFW and RC users.

**Recommendation:** We recommend DTA continue to work actively with the vendor and the DIT Server Support Branch division to restrict users from having logical network access to the files and folders that contain the CFW and RC data, programs, and system files unrelated to their job duties. The users should not be set up in the same home directory and/or to all the home directory folders unless they are authorized to use both systems. In addition, users should not have full control access to use CFW and RC where they could potentially delete critical files. Changes to the full control access should be evaluated in a testing environment with a copy of CFW and RC to ensure that users continue to have the same capability as before.

**Management Response:** This recommendation can only be implemented with the assistance of the COTS vendor. DTA has explored this finding with the vendor, however implementation would necessitate major architectural changes to the COTS product. The vendor has not committed to making the required application modifications since this does not appear to be a security concern with most clients. DIT implemented user restrictions to files and folders containing RC and CFW data, however, user access to the application failed once these restrictions were in place. User profile group authorities are presently used to control application permissions.

#### 4. Password Management

The Cashier for Windows and Revenue Collector systems did not require minimum password length. An individual could establish a single character alpha or numeric password. There was no lockout restriction; therefore, users could type in password guesses multiple times until they discovered the correct password. In addition, the CFW system allowed users to reuse their existing passwords each time that the password was changed, while the RC system had no requirement at all to change passwords.

Password administration for CFW and RC systems differed; however, they both

required initial setup and/or reset capability by a DTA system administrator, DIT programmer, or a Cashier's supervisor depending on the system. Passwords were initially defaulted to the word "password." Upon initial sign-on, the user was automatically prompted to change the password. CFW prompted users to change passwords at a defined interval of time. At the end of this period, the users could elect to retain or change their passwords. There was no history of saved passwords tracked to preclude users from reusing their passwords until a certain number of different passwords were used. On the other hand, RC passwords had to be setup and reestablished by the DTA system administrator only. The users were not able to change their passwords, and they were not prompted to do so. Passwords could be reset by either the DTA system administrator or the DIT system administrator only.

Password identification and authentication is critical to every computer system. Minimum password length and routine changes are required by the County's Information Technology Security Policy. This policy was adopted in 2003 subsequent to the DTA implementation of these application systems. In addition, password guessing should be limited to no more than three attempts, to minimize unauthorized users. CFW and RC are both computer off-the-shelf (COTS) packages developed by the same vendor who designed the password administration capability as it exists today. Unauthorized users may be able to access the CFW and the RC systems with relative ease, undermining data and program integrity, confidentiality, and availability in both systems. There is a potential for authorized users to disguise themselves as someone else by guessing the passwords, undermining the available audit trail.

**Recommendation:** We recommend DTA coordinate with the vendor to design password features in CFW and RC that require a minimum of at least six alpha/numeric characters, disallow the use of the five previous passwords, and establish a maximum of three lockout attempts to preclude unauthorized users from accessing these systems. In the meantime, DTA should require CFW users to establish and change their passwords to no less than six alpha/numeric characters in compliance with the strong password requirements based on the County's Information Technology Security Policy (PM 70.05 and 70-05.01). CFW users should also be required to change their passwords at least every 90 days to different passwords.

DTA should not allow DIT programmers to reset passwords for the RC system since they are also users of this system. Furthermore, the RC system should require all users to change their assigned passwords. Password administration responsibilities should remain with the DTA's system administrators so that they may stay informed of the need for user security awareness training, monitor unacceptable practices and overall security concerns, and report exceptions to management as appropriate.

**Management Response:** Version 3.0 of Revenue Collector permits users to

change their own passwords. DTA system administrators retain sole responsibility for assisting users with password issues.

The vendor has agreed to incorporate “strong” password standards in accordance with DIT PM 70.05 and to implement “lock-out” procedures. These standards were not required when the contract was awarded. DTA is funding password enhancements which are planned to be programmed beginning April 2005, i.e., outside of the scheduled version release schedule. This recommendation is scheduled to be completed by June 30, 2005.

## 5. System Administration Documentation

There was no documentation to describe the duties, functions, and responsibilities of the DTA systems administrator regarding the Cashier for Windows and Revenue Collector systems. There was no document that described how the DTA systems administrator should maintain, configure, and setup new users.

Documentation is a necessary part of an application system that supports the overall control environment by ensuring appropriate safeguard of DTA data and security access to system files. Documentation is needed to outline the functional tasks performed by the systems administrator and the backup administrator. This documentation should reflect the systems administration duties for the security and maintenance of the systems managed. DTA relied on the in-house expertise and knowledge of their system administrator to maintain systems with assistance from DIT programmers and the vendor as necessary.

In the absence of sufficient documentation, the knowledge of functional requirements for a systems administrator rests with the existing staff. In the absence of the primary or backup systems administrator, there was no guideline to describe their responsibilities and how they were to be administered effectively. Extra steps may become necessary to determine how a particular system function works.

**Recommendation:** We recommend DTA develop documentation to describe the system administrator duties and maintenance of their COTS systems (CFW and RC). The documentation should include the current process for working with the DIT programmers, DIT Server Support Branch staff, and the vendor. Lastly, this documentation should be updated to reflect changes to CFW and RC resulting from DIT or vendor support and any future enhancements.

**Management Response:** Documentation preparation is in progress. Samples have been provided to Internal Audit. This recommendation is expected to be complete by April 30, 2005.

## 6. System Development Coordination

There were other sub-systems such as the spreadsheet applications used by the Revenue Collection Division staff, in addition to the CFW and RC systems, with insufficient security controls. Systems developed without the knowledge and consultation with the IT staff makes management of these systems difficult such that adequate security controls may not be considered. In-house expertise in the DTA Revenue Collection Division made it possible for the Cashier's staff to automate generating the tax bills at the counter. The accounts receivable staff can generate the same tax bills if they were misplaced in transit from the counter to the back office. It's particularly helpful for the first five days in January of each year when the ALIS mainframe system is temporarily down for the annual rollover maintenance and personal property tax information is not available.

All application software systems require appropriate physical and logical access controls to preclude unauthorized access and modification to the data and programs. There were no automated systems available to assist the Revenue Collection Division staff in conducting their business in an efficient manner. Therefore, these systems were built to address efficient processing, but they did not include adequate controls. The absence of appropriate logical control undermines data integrity and reliability of the software application system.

**Recommendation:** We recommend DTA adopt the practice of involving the DTA Technical Division staff in all future system development requests. DTA should inventory and evaluate all of the ancillary application systems used by the staff in the DTA Revenue Collection Division. These include the applications developed in the Microsoft Office Suite such as the MS-Access database and the Excel spreadsheet developed by in-house staff.

**Management Response:** Development of ancillary systems by Revenue Collection staff using MS Access and Excel will be suspended. DTA Technical Staff will inventory cashiering ancillary systems. MS Access databases and Excel spreadsheets will be reprogrammed as appropriate using tools such as SAS to provide better physical access controls. This recommendation is expected to be complete by April 30, 2005.