



Fairfax County Internal Audit Office

Department of Housing and Community Development
YARDI Application Audit
Final Report

June 2011

"promoting efficient & effective local government"

Executive Summary

The Department of Housing and Community Development (DHCD) uses the comprehensive housing management software package from YARDI Systems, Inc. called YARDI Voyager to provide integrated, comprehensive management and accounting systems for housing programs. It ensures DHCD's compliance with HUD's reporting requirements and incorporates all partnership program financial information on one platform.

Our audit found that the application system controls were adequate and information was entered into the YARDI system accurately and completely. Based on our testwork, we determined that calculations of rent subsidies and payments performed by the application were accurate and all transactions were verified and approved before being sent to FAMIS for payment. Reconciliation was performed to ensure payments processed by the FAMIS application were recorded correctly in the YARDI application. Data and system files were backed up on a daily basis and DHCD maintained a backup site at the South County building. Separation of duties among staff of DHCD was adequate and physical safeguards were in place. However, we noted areas where internal controls could be strengthened in regard to the physical security of the servers, application access security, and contract completeness. We found that:

- DHCD did not have established procedures to periodically review the user access and determine whether it remained appropriate. Two errors were found in the user list for the YARDI application.
- There was no record being kept of persons entering the two locked rooms containing the primary and backup servers. Facilities Management Department (FMD) staff and YARDI system administrators had access to both server rooms.
- The contract with YARDI Systems, Inc. did not allow for the county to own the source code nor was the vendor required to maintain a copy of the source code in escrow with a third party for county access if necessary.

Scope and Objectives

This audit was performed as part of our fiscal year 2011 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. This audit covered the period of November 1, 2009, through October 31, 2010, and our audit objectives were to determine that:

- System controls for the application were adequate and in place.
- Data maintained in the database was accurate and up-to-date.
- Calculations performed by the application were correct.
- The application was in compliance with the county's IT Security Policy.
- Backup and recovery was tested and documented.

Methodology

Our audit approach included a review and analysis of internal controls over the YARDI application data input and processing. We interviewed appropriate employees to understand the application process, observed employees' work functions; determined if controls were in place to prevent data from unauthorized modification; and tested rent subsidy and low-income housing application transactions on a sample basis.

Our audit did not examine the YARDI interfaces with other systems. These interfaces were covered by the external audit conducted by Clifton Gunderson, LLC in September 2010.

Findings, Recommendations, and Management Response

1. User Access Maintenance

The user list for the YARDI application contained errors in access permissions for some DHCD staff. One employee changed job assignments within DHCD but was still in the old access group in YARDI. Also, one access group had the capability to override payment standards for individual accounts but did not appear to need it based on their job duties. The system administrator could change the access for user groups and move users to and from groups without appropriate oversight.

Fairfax County Information Technology Security Policy 70-05.01 states that 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.
- Shall have a documented process for periodically reviewing existing accounts for validity.

It also states that the concept of least privilege, i.e., providing only those privileges necessary to perform one's job function, will be used to insure the security of networks, computer systems, and county data.

It is essential to notify the system administrator immediately when an employee is terminated, changes job roles, or for other reasons is no longer authorized to access certain high-risk transactions in the YARDI application. DHCD did not establish procedures to periodically review the user list and determine whether it remained appropriate.

Recommendation: It is recommended that all user groups be reviewed on a regular basis to determine if access exists that is not necessary to perform the duties

of the job and to verify that all users within each group are appropriate. Changes to user group access should be approved by the user's supervisor and a record of approval should be maintained. Controls should be in place to ensure the YARDI system administrator is notified when an employee changes roles within the organization. Additionally, the system administrator should not be allowed to change users' access without approval from the user's manager.

Management Response: DHCD is establishing a new system to monitor access to YARDI. The first step is to modify the agency's IT Systems Access form and to require that any request for changes, deletions or additions to YARDI system access would trigger the need to submit the revised form. The use of the form will be incorporated into DHCD's human resources process so that any personnel changes will trigger assessment/reassessment of access.

A new lead person (not the YARDI systems administrator) is being identified to replace the recently retired employee who had responsibility to monitor employee access to YARDI and maintain records of approvals. Quarterly quality control reviews will be incorporated as a job duty in the position description.

A new inter-divisional team is also being formed to better coordinate access issues, ensuring that employees are given appropriate access to YARDI to do their jobs and are assigned to proper user groups. The access team will spread control and allow for a more thorough review and discussion of each access assignment.

The anticipated completion date is July 2011

2. Physical Security of Hardware

There were control weaknesses over the level of physical security of the primary and backup servers used by the YARDI application. The servers were maintained in locked rooms in the Pender Drive and South County buildings, respectively. However, the rooms also contained telephone equipment and storage which required FMD and information technology staff to enter without accountability.

Access to servers should be limited to necessary staff and monitored to track the actual access. Fairfax County Information Technology Security Policy 70-05.01, 2.12 Physical Access states that, "a system of monitoring and auditing physical access to all information systems restricted facilities shall be implemented (e.g., badges, cameras, access logs)."

Recommendation: The use of access cards to register who entered the rooms and when, should be implemented. If such a control cannot be implemented, a list should be made of all staff including FMD staff that has access to the two server rooms. If any is deemed unnecessary or inappropriate, the locks should be changed and keys redistributed to those who should have access. This could be used as a compensating control.

Management Response: DHCD is in the process of upgrading the door to its server room at Pender Drive and installing a cypher lock, rather than current master

key system. The combination to the cypher lock will be shared with a very limited number of employees who “need to know.” A clip board has also been placed in the room and all persons entering the room must sign in.

HCD staff will work with FMD and building security staff at South County Center to address the security issues related to the server room there. A clipboard with sign-in sheet will be placed in the server room; however, HCD does not have authority to make any physical changes to the door or locking system at that building – at this time.

The anticipated completion date is August 2011.

3. Software Ownership and Access

The source code for the YARDI application is owned by YARDI Systems, Inc. The county did not have a copy nor was one kept in escrow by a third party. Without access to a copy of the code, should this company no longer be in business or be unable to support the county, DHCD would not be able to fix and/or change the application to meet its needs if the situation arose.

Recommendation: We recommend the DHCD contract with YARDI Systems, Inc. be amended to include the requirement that a copy of the source code be maintained by a third party, to be accessible by the county in the event of the company becoming unable to do business with the county within its contract period.

Management Response: The new YARDI contract will address this issue with contract wording as follows :

Source Code License – Upon the occurrence of the release conditions set forth in the Software Escrow Agreement, YARDI grants to client a non-exclusive, non-transferable, limited, perpetual license to use and modify the Code to support Client’s Use of the Licensed Programs.

Maintenance of Escrow Agreement - During the term of this Agreement, YARDI agrees to maintain the Software Escrow Agreement or an escrow agreement materially similar to the Software Escrow Agreement.

The proposed contract with Department of Purchasing and Supply Management is under review.