



Fairfax County Internal Audit Office

Department of Finance
Department of Purchasing and Supply Management
Fixed Assets System Audit
Final Report

November 2006

"promoting efficient & effective local government"

Executive Summary

The Department of Finance (DOF) and the Department of Purchasing and Supply Management (DPSM) use the Fixed Asset System for Government (FASGOV) to process county fixed assets data. The FASGOV system, a commercial-off-the-shelf application, has two modules and they are the Asset Accounting Module and the Asset Inventory Module. DOF primarily uses the Asset Accounting Module to process fixed assets accounting data, and DPSM uses the Asset Inventory Module to process fixed assets inventory data. Each module has its own system administrator.

We found that policies and procedures for the proper recording and financial reporting of fixed assets were in place, and county fixed assets data were entered into the FASGOV system accurately and completely. However, internal controls related to segregation of duties controls between end-user and system administrator, and application security controls using FASGOV were not adequate. We noted that compliance with the county's Information Technology Security Policy 70-05.01 related to account management, passwords and segregation of duties, needs to be strengthened.

The primary issues noted were:

- There was no formal request form to document the changes of user's access rights.
- Users were not required to set up strong passwords.
- The system administrator had the privilege to view user's passwords.
- The Asset Accounting Module user list was not current. During the audit, the system administrator removed three users upon notification by Internal Audit.
- For the FASGOV Asset Inventory Module, segregation of duties control was weakened by the system administrator also serving as an end-user. During the audit, DPSM addressed this issue.

Weak passwords cannot adequately protect fixed assets data from unauthorized modification, and inadequately segregated duties increase the risk that fraudulent transactions could be processed in the FASGOV system.

Scope and Objectives

This audit was performed as part of our fiscal year 2005 Annual Audit Plan and was conducted in accordance with generally accepted government auditing standards. The audit covered the period of January 2005 through June 2005, and our audit objectives were:

- Determine whether fixed assets data are authorized and entered into the FASGOV system in an accurate, complete, and timely manner.
- Determine whether the fixed assets data are properly processed by the FASGOV system.
- Determine whether all fixed assets transfers and dispositions are appropriately tracked and recorded in the FASGOV system.
- Determine whether the FASGOV system has controls to help prevent unauthorized modification.

Our audit did not include a review of the general controls environment, including the security and controls over the SQL Server database in which the FASGOV application data is stored. The effect of this scope limitation is that if weaknesses exist in the general controls environment, this could have a negative impact on the integrity of the application data.

Methodology

Our audit methodology included a review and analysis of policies and procedures for proper recording of fixed assets, and system controls for the FASGOV application. Our audit approach included interviewing appropriate employees to understand DOF and DPSM responsibilities in the fixed assets process, performing a walkthrough to understand the fixed assets process using the FASGOV system, observing employees' work functions, determining if controls were in place to prevent fixed assets data from unauthorized modification, and testing of fixed assets transactions on a sample basis.

The Fairfax County Internal Audit Office 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 reports are available to the public.

Findings, Recommendations, and Management Response

Department of Finance & Department of Purchasing and Supply Management

1. Access Request Documentation

All requests for adding, changing and removing FASGOV system users were made through e-mails or phone conversations. There was no formal access request form. In addition, the system administrators did not keep all the email communications for the requests of authorizing access to the FASGOV system.

Fairfax County Information Technology Security Policy 70-05.01 states: "All accounts created must have an associated request and approval that is appropriate for the Fairfax County system or service. A record of authorization for system access should be maintained."

There were less than fifteen users from DOF, DPSM and the Department of Housing and Community Development (HCD) using the FASGOV. DOF and DPSM had not established formal access request procedures. All requests for authorizing or changing user access rights in the systems were made through phone and e-mail. The lack of a standardized access request process creates risks of mishandlings, alterations, and misunderstandings.

Recommendation: We recommend that DOF and DPSM establish a standard access request form to document authorization and modification of access privileges approved by an authorized manager and maintain the completed forms on file. Changes to user's access rights should be authorized and documented.

Management Response: DPSM and DOF will work together to develop an appropriate standard access request form. A system administrator's log will also be developed to document changes to the FASGov system. The anticipated completion date is November 30, 2006.

Department of Finance

2. FASGOV System Passwords

The FASGOV system did not require users to set up strong passwords. It accepted a password with only one character during a test. In addition, the passwords did not have expiration dates.

Fairfax County Information Technology Security Policy 70-05.01 states that all passwords, including initial passwords, must be constructed and implemented according to the following Fairfax County Information Resource rules. Passwords must:

- Be routinely changed
- Adhere to a minimum length
- Be a combination of alpha and numeric characters
- Not be anything that can be easily tied back to the account owner such as: user name, social security number, nickname, relative's names, birth date, etc.
- Not be dictionary words or acronyms and password history must be kept to prevent the reuse of a password

The FASGOV system resides on the county network. Users are required to log-on to the county network in order to access the system. The FASGOV system is a commercial-off-the-shelf product developed by Best Software, Inc. This application does not have the built-in functions to enforce strong passwords and periodic password changes. Password identification and authentication is critical to every computer system. Weak passwords cannot adequately protect fixed assets data from unauthorized modification, disclosure, loss, or impairment.

Recommendation: We recommend that DOF coordinate with the vendor to develop password features in the FASGOV system that require a minimum of at least six alpha/numeric characters, enforce password change at least every 90 days, disallow the use of the five previous passwords, and establish a lockout mechanism after three consecutive logon failures to preclude unauthorized access to the system.

In the meantime, DOF should require the FASGOV system users to 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 70-05.01.

Management Response: FASGov was implemented in June 2003 to meet new

financial reporting requirements as promulgated by the Governmental Accounting Standards Board that could not be satisfied by the previous system called FAACS. FAACS was a mainframe system which contained outdated functionalities. FASGov has given DOF the flexibility to manage data as well as the capability to calculate depreciation and capture infrastructure in a more efficient manner. In addition, the old FAACS required five positions plus a consultant to manage the accounting of the assets while FASGov is currently supported by two positions. The total number of system users is less than fifteen, consisting of staff within DOF, DPSM, and the Department of Housing and Community Development.

Two of the four DOF audit findings are due to FASGov limitations. DOF will immediately contact the vendor, Best Software Inc., and recommend that a “strong” password capability be developed and included in their next upgrade. In the meantime, DOF will require users to use “strong” passwords.

3. FASGOV Administrator Privileges

The FASGOV system provided the system administrators the privilege to view each of the user’s passwords in the user profiles list.

Fairfax County Information Technology Security Policy 70-05.01 states: “An unencrypted password must not be written or stored in a location (physical or logical) in which any person other than the password owner has access.” The FASGOV system is a commercial-off-the-shelf product developed by Best Software, Inc. This application has the built-in function to allow the system administrator to view users’ passwords.

The user ID and password are used to identify and authenticate the user. Password identification and authentication is critical to every computer system. Passwords used to authenticate identity should be known only by the individual user.

Recommendation: We recommend that DOF coordinate with the vendor to take away system administrators’ privileges of viewing user passwords in the FASGOV system.

Management Response: DOF will immediately contact the vendor, Best Software Inc., and will request that the capability of system administrators to view user’s passwords be revoked. In addition, DOF will recommend that an option that allows the system administrator to view users’ passwords be excluded in their next upgrade.

4. System User List

The user list for the Asset Accounting Module was not current at the time of the audit. During the audit, the system administrator removed three users. Fairfax County Information Technology Security Policy 70-05.01 states:

System Administrators or other designated staff:

- Are responsible for removing the accounts of individuals that change roles within Fairfax County or are separated from their relationship with Fairfax County
- Must have a documented process for periodically reviewing existing accounts for validity

DOF has not established procedures to periodically review the user list and determine whether it remains appropriate. It is very important to notify the system administrator immediately when an employee is terminated or, for some other reason, is no longer authorized access to the FASGOV system. Terminated employees who continue to have access to critical or sensitive resources pose a threat, especially those individuals who may have left under acrimonious circumstances.

Recommendation: We recommend that DOF establish procedures to periodically review the FASGOV system user list and assign responsibility for notifying the system administrator when an employee is terminated or, for some other reason, is no longer authorized access to the FASGOV system.

Management Response: DOF will develop procedures to periodically review the FASGov system user list and notification of non-active users. The anticipated completion date is November 30, 2006.

Department of Purchasing and Supply Management

5. Segregation of Duties

DPSM was using the FASGOV System Asset Inventory Module to process county fixed assets inventory data and assigned its own system administrator. During the audit, we noted the following issues:

- The FASGOV System Manager Group is a user security profile which provides system administrator level capabilities. These capabilities allow a user to carry out transactions to manage security for users including creating new users, deleting users, granting user access rights. There were three users in the System Manager Group; one of them was the DOF accountant who worked for the DOF Fixed Assets team and used the FASGOV System Asset Accounting Module to process fixed assets accounting data. The DOF accountant should only have the access needed to perform his duties. The likelihood of fraud and errors are increased when an individual is given access rights beyond his job function. For example, a system administrator could have the ability to create a user, perform transactions, and then delete the user record.
- The DPSM system administrator was also an end-user of the FASGOV system. Assigning these two incompatible duties to a single person increased the risk that errors or fraud could occur and not be detected in a timely manner.
- The DOF Fixed Assets team staff had access to the FASGOV Asset Inventory Module and they were assigned to the System Data Entry Group. Users in this group had “edit” access to most files, including the records that belong to DPSM

and not to DOF. Therefore, the potential risk of inappropriately updating the fixed assets inventory data by the DOF staff was increased.

Industry best practices recommend that work responsibilities should be segregated so that one individual does not control all critical stages of a process. DPSM has not identified incompatible duties and assigned these duties to different individuals. Inadequately segregated duties increase the risk that erroneous or fraudulent transactions could be processed in the FASGOV system.

Recommendation: We recommend that DPSM remove the DOF accountant from the System Manager Group of the Asset Inventory Module, create a new group that only has read access for DOF staff, and assign a new system administrator who is not an end-user of the FASGOV system.

DPSM has addressed these issues during the course of this audit. No further action is needed.