REPORT NO. 2010-188
APRIL 2010

DEPARTMENT OF MANAGEMENT SERVICES

MYFLORIDAMARKETPLACE (MFMP)

Information Technology Operational Audit

For the Period
August 2009 Through January 2010
and Selected Actions from January 1, 2009

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF MANAGEMENT SERVICES

Pursuant to Section 20.22(1), Florida Statutes, the Secretary of the Department of Management Services is appointed by the Governor, subject to confirmation by the Senate. Linda H. South served as Secretary during the audit period.

The audit team leader was Cathy Jones, CISA, and the audit was supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF MANAGEMENT SERVICES

MyFloridaMarketPlace (MFMP)

SUMMARY

MyFloridaMarketPlace (MFMP) is a Web-based electronic procurement system for State agencies. Maintained and operated by Accenture, LLP, (Accenture) under contract with the Department of Management Services (Department), MFMP is designed to enable State agencies to procure commodities and contractual services online and electronically communicate information on purchasing activities to the State's accounting system, the Florida Accounting Information Resource Subsystem (FLAIR).

Our audit of MFMP focused on evaluating selected information technology (IT) controls relevant to the Buyer and Vendor Modules during the period August 2009 through January 2010, and selected actions from January 1, 2009. We also determined the status of corrective actions regarding selected prior audit findings disclosed in our report No. 2007-076.

The results of our audit are summarized below:

Finding No. 1: As similarly noted in prior audit reports, most recently our report No. 2007-076, the Department had no documentation to demonstrate that background checks were performed for Accenture employees working on MFMP.

Finding No. 2: As similarly noted in our report No. 2007-076, some Accenture employees working on MFMP had excessive access privileges in MFMP.

Finding No. 3: Access privileges for one reassigned Accenture employee had not been fully inactivated in a timely manner. A similar finding was noted in our report No. 2007-076.

Finding No. 4: Contrary to the requirements of the Department of State General Records Schedule for retention of network access control records, the Department's practice was to physically delete network access accounts within 30 to 60 days after the accounts were disabled.

Finding No. 5: As similarly noted in our report No. 2007-076, some data integrity issues regarding vendor information and purchase order dates existed within MFMP.

Finding No. 6: Certain Department security and application controls in the areas of safeguarding social security numbers, authenticating system users, and logging system activity needed improvement. Our prior audit reports on MFMP have included some of the same issues.

BACKGROUND

As authorized by Section 287.057(23)(a), Florida Statutes, the Department, on October 9, 2002, contracted with Accenture, LLP (Accenture), for the development and operation of MFMP. Accenture serves as the application service provider for MFMP. A contract modification, effective July 12, 2007, transferred MFMP's hosting environment from the service provider's facility to the Shared Resource Center (now the Southwood Shared Resource Center) in Tallahassee.

Accenture developed MFMP by customizing the Ariba, Inc. (Ariba) commercial off-the-shelf procurement solution. The Ariba procurement solution is a standardized software product that is upgraded and supported by Ariba. However, portions of MFMP are not part of the Ariba product and were customized, developed, and integrated with the Ariba software by Accenture.

Pursuant to Section 215.94(4), Florida Statutes, the Department is the functional owner of MFMP. As of the end of our audit period, MFMP was being used by 32 State agencies.

MFMP automates the State's order, approval, invoicing, and payment approval process for State purchasing activities; serves as a tool to collect data from those purchasing activities; and communicates applicable data to the State's accounting system, FLAIR. MFMP was not designed as an accounting system and does not perform accounting functions such as the recording, classifying, summarizing, and reporting of financial information. MFMP can optionally initiate an encumbrance in FLAIR for MFMP-approved requisitions. Additionally, once goods are received and the process for payment is completed in MFMP, the transaction is sent to FLAIR for payment. Payment information is then sent back from FLAIR and posted in MFMP.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Background Checks

Department of Management Services Rule 60DD-2.001(2)(a)(80), Florida Administrative Code, defines "special trust or position of trust" as a position in which an individual can view or alter confidential information or is depended upon for the continuity of information resources imperative to the operations of the agency and its mission. Department of Management Services Rule 60DD-2.008(2)(c), Florida Administrative Code, additionally requires that agencies shall conduct background investigations for personnel in positions of special trust. The contract between the Department and Accenture provides that Accenture shall perform reasonable security and background searches on all its employees and subcontractors' employees performing work on MFMP.

As similarly noted in prior audit reports, most recently our report No. 2007-076, the Department had no documentation to demonstrate that background checks were performed for Accenture employees working on MFMP. On a quarterly basis, Accenture provided the MFMP Operations Manager an MFMP access list for Department and Accenture employees. We were informed that, during the joint Department and Accenture review of access privileges for appropriateness, Accenture verbally confirmed the completion of a background check for any new Accenture employee identified on the access list. However, no documentation of the review was maintained by the Department. Additionally, we noted that the list used in the above-described review of access privileges was an MFMP system user access list. Accenture technical employees (i.e., system administrators) who did not have system access privileges established through a defined user access group did not appear on the access list. As a result, Accenture technical employees working on MFMP may be omitted during the verbal background check confirmation process. Under these conditions, the risk was increased that an employee with an inappropriate background could be placed into a position of special trust.

In response to audit inquiry, Department management stated that, beginning in January 2010, the confirmation of background checks for new Accenture employees would be documented using a standard memorandum from Accenture to the Department providing the names of the new Accenture employees and MFMP project start dates. The memorandum would provide documentation and certification from Accenture that background checks were completed on the new Accenture employees and would be signed by both Accenture and the Department and maintained by the MFMP Operations Manager (or designee).

Recommendation: The Department should ensure that background checks are performed for all Accenture employees working on MFMP. Additionally, the Department should obtain and review documentation of the performance and results of the background checks.

Finding No. 2: Management of Access Privileges – Superuser Account

An important aspect of IT security management is the establishment of system access privileges that restrict users to only those system functions necessary to perform their assigned duties. Properly configured access privileges help enforce an appropriate separation of incompatible duties and minimize the risk of unauthorized system actions. Additionally, effective IT access controls include a process for the unique identification and authentication of system users. The unique authentication of system users allows management to affix responsibility for system activity to an individual user.

The Ariba System superuser account was needed by specific Accenture employees who worked on MFMP to perform their assigned job duties. Eleven Accenture employees shared the superuser account and password. Additionally, the superuser account granted the employees excessive access to the MFMP Buyer Module. In response to audit inquiry, Department management stated that, because of Ariba software restrictions, the superuser account could not be duplicated and specific functions needed by Accenture employees assigned to MFMP to perform their job duties could only be performed by the superuser account. However, not all functions held by the superuser account were needed by each employee.

Inappropriate or unnecessary access privileges increase the risk of unauthorized disclosure, modification, or destruction of data and IT resources. Additionally, the sharing of user IDs and passwords may limit the Department's ability to assign responsibility for system activities.

Recommendation: The Department should remove all unnecessary functions from the superuser account and analyze the need of the Accenture employees who have access privileges to the account. Where possible, employees should be assigned a unique user ID. Additionally, the Department should request an enhancement to the Ariba software to provide the ability to appropriately configure access privileges. The Department should also monitor the use of the superuser account.

Finding No. 3: Management of Access Privileges – Timely Removal of Access Privileges

Effective management of system access privileges includes provisions to timely remove or adjust employee or contractor access privileges when job reassignments occur. Prompt action is necessary to ensure that a reassigned employee or contractor's access privileges are not misused by the reassigned employee, contractor, or others.

We reviewed MFMP application access privileges of all 21 Department and Accenture employees who terminated employment or were reassigned from MFMP during the period January 1, 2009, through October 30, 2009. Our review disclosed that the application access privileges of one reassigned Accenture employee were shown on an Accenture-provided access privileges report as remaining active for 84 days after her reassignment. A similar finding was noted in our report No. 2007-076. In response to audit inquiry, Accenture management stated that, because of a processing error, the account was not fully inactivated, causing the reassigned Accenture employee to be included on the access privileges report. However, neither the Department nor Accenture could provide documentation of the inactivation of the access privileges. In response to audit inquiry, the access privileges of the reassigned Accenture employee were fully inactivated by Accenture on November 23, 2009. The access privileges of the reassigned

Accenture employee had not been used subsequent to her reassignment. Without timely deletion of the access privileges of Accenture employees who are reassigned from MFMP, the risk is increased that access privileges could be misused by the reassigned Accenture employees or others.

Recommendation: The Department should ensure that MFMP application access privileges of reassigned Accenture employees are removed in a timely manner.

Finding No. 4: Access Records Retention

State of Florida, General Records Schedule GS1-SL for State and Local Government Agencies, revised by the Department of State effective September 2007, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment.

Upon notification of a terminated employee, Department policy was to immediately disable the employee's network account. However, within 30 to 60 days, the disabled network account was physically deleted from the system, contrary to the Department of State's General Records Schedule. Without adequate retention of access control records, the risk increases that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur, and would not be in compliance with the State's record retention requirements. In response to audit inquiry, Department management revised the policy as of December 10, 2009, to disable but not delete the network accounts in order to retain the records pursuant to the Department of State's General Records Schedule.

Recommendation: The Department should monitor its compliance with the Department of State's General Records Schedule with regard to the retention of access control records.

Finding No. 5: MFMP Data Integrity

Data integrity relates to the accuracy and completeness of information as well as its validity in accordance with business values and expectations. Our audit disclosed some issues with data integrity in MFMP. Specifically:

- As similarly noted in prior audit reports, most recently our report No. 2007-076, when a transaction was recorded in MFMP, the system recorded only the vendor number associated with that transaction. MFMP maintained additional vendor data, such as name and address for each vendor; however, MFMP did not maintain historical values for the additional vendor data. The vendor data present at the time of the transaction was not preserved or displayed in the system if the data had been changed subsequent to the entry of the transaction. In such circumstances, when displaying transactions, MFMP provided only the current vendor information rather than the historical vendor information that was valid when the transaction was processed. Under these conditions, the risk was increased that management decision making could be hindered by inaccurate or misleading vendor information in MFMP.
- As similarly noted in our report No. 2007-076, the purchase order start date and end date fields on the MFMP requisition form were used to provide the vendor with the terms of the contract. The system allowed a purchase order start date to be entered as a date after the purchase order end date, increasing the risk that an erroneous purchase order start date could be entered into the system without timely detection.

Recommendation: The Department should take action regarding the issues described above to enhance the integrity of MFMP data.

Finding No. 6: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security and application controls related to MFMP that needed improvement in the areas of safeguarding social security numbers, authenticating system users, and logging system activity. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department staff of the specific issues. Some of the issues were also included in our prior reports on MFMP, most recently our report No. 2007-076. Without adequate security and application controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should implement the appropriate security and application controls in the areas of safeguarding social security numbers, authenticating system users, and logging system activity to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

PRIOR AUDIT FINDINGS

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2007-076 that were applicable to the scope of this audit.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit in accordance with applicable 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 objectives of this IT operational audit were to determine the effectiveness of IT controls relevant to the MFMP Buyer and Vendor Modules in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations; and to determine whether the Department had corrected, or was in the process of correcting, selected deficiencies disclosed in our report No. 2007-076.

The scope of our audit focused on evaluating selected IT controls relevant to the MFMP Buyer and Vendor Modules during the period August 2009 through January 2010 and selected actions from January 1, 2009, including selected general IT controls over systems development and modification, systems software and database, logical access to programs and data, and physical and environmental safeguards. The audit also included selected application IT controls and selected user controls.

In conducting our audit, we:

- Interviewed Department and Accenture personnel.
- Evaluated the Department's placement of the IT and security management functions within the overall organizational structure.
- Obtained an understanding of the Department's efforts to communicate and work with State agencies to increase agency utilization of MFMP functions and to monitor MFMP transaction fees and exemptions.
- Observed and tested selected controls surrounding the maintenance and protection of data within MFMP.
- Observed and tested selected controls for the MFMP Statistical Sampling function.
- Observed and tested the effectiveness of selected input, processing, and output controls for the MFMP Buyer Module.
- Obtained an understanding of the transaction flow within the application, interfaces with internal and external systems, and external reconciliation processes.
- Observed and tested the effectiveness of selected input, processing, and output controls for the MFMP Vendor Module.
- Obtained an understanding of the MFMP Vendor Module transaction flow and interface between MFMP and FLAIR.
- Observed and tested the effectiveness of selected controls over the design, testing, approval, and implementation of application program modifications.
- Observed and tested the effectiveness of the procedures that provide for management and implementation of systems software patches.
- Observed and tested the adequacy of the Department's risk assessment, backup, and recovery procedures.
- Obtained an understanding of logical access paths to MFMP and tested whether logical access controls ensured that the application, software, and data access privileges of Department and Accenture employees assigned to MFMP were appropriately restricted.
- Evaluated the adequacy of the Department's security administration policies and procedures and guidance provided by the Department to State agencies for the implementation and management of MFMP user access privileges.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated April 12, 2010, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

Department of Management Services

Office of the Secretary
4050 Esplanade Way
Tallahassee, Florida 32399-0950
Tel: 850.488.2786
Fax: 850.922.6149
www.dms.MyFlorida.com

Governor Charlie Crist

Secretary Linda H. South

April 12, 2010

Mr. David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our response to your report, *Department of Management Services, Information Technology Operational Audit of MyFloridaMarketPlace.* Our response corresponds with the order of your tentative and preliminary findings and recommendations contained in the draft report.

The Department has made continuing efforts to improve controls and system enhancements of the MyFloridaMarketPlace electronic procurement system. The Department appreciates the Auditor General's efforts to evaluate this system and to make recommendations for further improvement.

We appreciate the professionalism displayed by your audit staff. If further information is needed concerning our response, please contact Steve Rumph, Inspector General, at 488-5285.

Sincerely,

Linda H. South
Secretary

Attachment

cc: Charles Covington, Director of State Purchasing
Walt Bikowitz, Chief of State Purchasing Operations

We serve those who serve Florida.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Mr. David W. Martin, CPA
April 12, 2010
Page 1

Department of Management Services' Response
To the Auditor Generals' Information Technology Operational Audit of the
Department of Management Services MyFloridaMarketPlace
Division of State Purchasing

Finding No. 1: Background Checks

As similarly noted in prior audit reports, most recently our report No. 2007- 076, the Department had no documentation to demonstrate that background checks were performed for Accenture employees working on MyFloridaMarketPlace (MFMP).

Recommendation:

The Department should ensure that background checks are performed for all Accenture employees working on MFMP. Additionally, the Department should obtain and review documentation of the performance and results of the background checks.

Response:

The Department concurs with the recommendation. On January 21, 2010 the Department made modifications to its Quarterly Access Review process to address the recommendation. The process includes recording in a memo, which is signed by the MFMP Operations Manager and the Accenture Project Director a formal certification that background screening checks have been completed for all Accenture employees who are working on MFMP during that quarter.

The Department has also succeeded in obtaining and reviewing Level 2 Background Security checks for Accenture employees that require access to the Southwood Shared Resource Center (SSRC).

The Department intends to provide for Level 2 Background Security Checks for all Service Provider employees in the new Invitation to Negotiate (ITN) that is anticipated to be issued in September 2010.

Finding No. 2: Management of Access Privileges – Superuser account

As similarly noted in our report No. 2007-076, some Accenture employees working on MFMP had excessive access privileges in MFMP.

Recommendation:

The Department should remove all unnecessary functions from the superuser account and analyze the need of the Accenture employees who have access privileges to the account. Where possible, employees should be assigned a unique user ID. Additionally, the Department should request an enhancement to the Ariba software to provide the ability to appropriately

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Mr. David W. Martin, CPA
April 12, 2010
Page 2

configure access privileges. The Department should also monitor the use of the superuser account.

Response:

The Department concurs with the recommendation. On September 17, 2009 the Department reviewed the need of the Accenture employees having access privileges. Accenture employees still have access to the superuser account; however, several controls have been put in place to mitigate the risk associated with this account:

- Mandatory password changes for all Accenture staff were implemented;
- Security Awareness training was communicated to Accenture staff on the importance of password complexity and protection;
- On October 31, 2009 a software code change was implemented that prevents employees from installing a password that matches the user name;
- Monitoring of the superuser account has been included as part of the Quarterly Access Review process effective January 21, 2010.

Unique user IDs could not be created for each employee, however each Accenture staff member selected a unique password for access to the superuser account. On March 30, 2010 a formal Change Request (CR) was filed by Accenture with Ariba to request an enhancement to the Ariba software to provide the ability to appropriately configure access privileges.

Finding No. 3: Management of Access Privileges – Timely Removal of Access Privileges

Access privileges for one reassigned Accenture employee had not been fully inactivated in a timely manner. A similar finding was noted in our report No. 2007-076.

Recommendation:

The Department should ensure that MFMP application access privileges of reassigned Accenture employees are removed in a timely manner.

Response:

The Department concurs with the recommendation. On January 21, 2010, the Department made modifications to its Quarterly Access Review process when an employee has departed or been reassigned. The application access privileges are reviewed for all reassigned or departed employees within the quarter under review.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Mr. David W. Martin, CPA
April 12, 2010
Page 3

Finding No. 4: Access Records Retention

Contrary to the requirements of the Department of State General Records Schedule for retention of network access control records, the Department's practice was to physically delete network access accounts within 30 to 60 days after the accounts were disabled.

Recommendation:

The Department should monitor its compliance with the Department of State's General Records Schedule with regard to the retention of access control records.

Response:

The Department concurs with the recommendation. DMS instructed Departmental IT to keep Local Area Network domain accounts for one year after the separation of an employee or contractor. This was implemented March 1, 2010. DMS will continue to monitor compliance with the Department of State's General Records Schedule with regard to the retention of access control records.

Finding No. 5: MFMP Data Integrity

As similarly noted in our report No. 2007-076, some data integrity issues regarding vendor information and purchase order dates existed within MFMP.

Recommendation:

The Department should take action regarding the issues described above to enhance the integrity of MFMP data.

Response:

The Department concurs with the recommendation. The Department has taken the following corrective action to enhance the integrity of the MFMP data:

- Log and implement a CR to retain historical vendor information;
- Implement a CR to include appropriate edits on start and end dates on the PO.

The Department advised its MFMP Change Review Board (CRB) of its intent to correct audit findings as enterprise CRs at its March 25, 2010 CRB meeting. The Department is proceeding to develop cost estimates to implement CRs required to correct audit findings and should have a cost estimate no later than July 1, 2010. Once a cost estimate is available the Department will determine whether to implement the CR in the near future or during the upcoming Ariba upgrade. The MFMP Ariba Buyer Upgrade is scheduled to be implemented no later than September 2011.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Mr. David W. Martin, CPA
April 12, 2010
Page 4

Finding No. 6: Other Security Controls

Certain Department security and application controls in the areas of safeguarding social security numbers, authenticating system users, and logging system activity needed improvement. Our prior audit reports on MFMP have included some of the same issues.

Recommendation:

The Department should implement the appropriate security and application controls in the areas of safeguarding social security numbers, authenticating system users, and logging system activity to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Response:

The Department concurs with this recommendation. The Department advised its MFMP CRB members of its intent to correct audit findings as enterprise CRs at its March 25, 2010 CRB meeting. The Department is proceeding to develop cost estimates to implement CRs required to correct audit findings and should have a cost estimate no later than July 1, 2010. Once a cost estimate is available the Department will determine whether to implement the CR in the near future or during the upcoming Ariba upgrade. The MFMP Ariba Buyer Upgrade is scheduled to be implemented no later than September 2011.