DEPARTMENT OF MANAGEMENT Services

Office of Inspector General
Department of Management Services
4040 Esplanade Way, Suite 135
Tallahassee, Florida 32399-0001
Tel: 850.488.5285
Fax: 850.921.3066
www.dms.MyFlorida.com

Governor Charlie Crist

Secretary Linda H. South

MEMORANDUM

RECEIVED
OCT 18 2010
BY:

DATE: October 15, 2010

TO: Linda South, DMS, Secretary

FROM: Steve Rumph, Inspector General

SUBJECT: **Six-Month Follow-Up to Auditor General Report No. 2010-188**

Pursuant to Section 20.055(5)(g), Florida Statutes, the following is our explanation of the six-month status of findings and recommendations included in the Auditor General's Report No. 2010-188, ***Department of Management Services – MyFloridaMarketPlace (MFMP), Information Technology Operational Audit.*** Our response addresses the findings and recommendations in the same order as they appear in the report.

Six-Month Status Report

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.

Current Status of 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 and includes a formal certification that background screening checks have been completed for all Accenture employees who are working on MFMP during that quarter. This process has been followed for the three quarters (January 2010, April 2010, and August 2010) since the finding was identified.

The Department included Level 2 Background Security Checks requirements for all Service Provider employees in the draft Invitation to Negotiate (ITN) for the new eProcurement contract.

The ITN was scheduled to launch in September 2010; however it has been delayed pending the approval of the MFMP Business Case by the Florida Legislature.

OIG Position

We agree with the actions taken by the Department and recommend this finding be closed.

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 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 protection;
- On October 31, 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. However, 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.

Current Status of Recommendation

An enhancement request was filed with Ariba (ER# 1-AYDISD) and Ariba has included this enhancement in the 9r1 service pack 9. The Department is proceeding with the Upgrade to the Ariba 9r1 platform. When the upgrade launches in September 2011, this item will be resolved.

OIG Position

We agree with the actions taken by the Department; however, until the upgrade has been completed the finding will remain open.

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.

Current Status of 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 and includes a formal certification that access privileges have been reviewed for reassigned or departed employees. This process has been followed for the three quarters (January 2010, April 2010, and August 2010) since the finding was identified.

OIG Position

We agree with the actions taken by the Department and recommend this finding be closed.

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 on 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.

Current Status of Recommendation

The recommendation was completed on March 1, 2010.

OIG Position

We agree with the actions taken by the Department and recommend this finding be closed.

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.

Current Status of Recommendation

The Department is proceeding with the MFMP Buyer Upgrade, which will launch in September 2011; the upgrade will address a number of these recommendations. The enhancement bandwidth for the MFMP Buyer upgrade is 750 hours. It is estimated that the effort to enhance MFMP Buyer to include appropriate edits on start and end dates of the PO is approximately 40 hours. This will be included in the MFMP Buyer Upgrade. It is estimated that the effort to enhance Buyer to retain historical vendor information would take approximately 750 hours ($168,000). This enhancement will not be included in the MFMP Buyer upgrade as the current project schedule allotment of upgrade hours will not support this modification.

OIG Position

We agree with the actions taken by the Department; however, until the MFMP Buyer Upgrade has been completed the finding will remain open.

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.

Current Status of Recommendation

The Department is proceeding with the MFMP Buyer Upgrade, which will launch in September 2011; the upgrade will address a number of these recommendations.

OIG Position

We agree with the actions taken by the Department; however, until the MFMP Buyer Upgrade has been completed the finding will remain open.

JSR/gz

cc: Kathy Dubose, Staff Director
Joint Legislative Auditing Committee

David W. Martin, Auditor General

Rachael Lieblick, Chief of Purchasing Operations, DMS