



AUDITOR GENERAL
WILLIAM O. MONROE, CPA



**DEPARTMENT OF MANAGEMENT SERVICES
AND OTHER SELECTED STATE AGENCIES**

MYFLORIDAMARKETPLACE SYSTEM

Information Technology Audit

July 1, 2005, Through June 30, 2006,
And Selected Actions Through September 14, 2006

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives and scope of this audit were:

- To determine the effectiveness of selected general and application controls related to the MyFloridaMarketPlace Buyer Component and to determine whether the Department of Management Services (DMS) had corrected, or was in the process of correcting, all deficiencies disclosed in audit report No. 2006-015. For this objective, our audit scope focused on evaluating selected information technology (IT) controls applicable to MyFloridaMarketPlace during the period July 1, 2005, through June 30, 2006, including selected actions through August 31, 2006.
- Concurrently, we conducted audit field work at the 14 agencies, including DMS, listed below to evaluate the effectiveness of MyFloridaMarketPlace processes and related internal controls as implemented by each agency. For this objective, our audit focused on the period July 1, 2005, through January 31, 2006, and selected actions through September 14, 2006.

Agency Name	As Used In Report
Department of Children and Family Services	DCFS
Department of Corrections	DOC
Department of Education	DOE
Department of Financial Services	DFS
Department of Health	DOH
Department of Highway Safety and Motor Vehicles	DHSMV
Department of Law Enforcement	DLE
Department of Management Services	DMS
Department of Revenue	DOR
Department of State	DOS
Department of Transportation	DOT
Department of Veterans' Affairs	DVA
Executive Office of the Governor	EOG
Fish and Wildlife Conservation Commission	FWCC

In conducting this audit, we interviewed appropriate agency and contractor personnel, observed processes and procedures, reviewed documentation, tested transactions, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls and evaluate the effectiveness of MyFloridaMarketPlace processes.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. This audit was conducted by Chris Gohlke, CPA, * and Clint Boutwell, CPA,* and supervised by Shelly Posey, CISA, and Nancy Tucker, CPA.* Please address inquiries regarding this report to Jon Ingram, CPA,* CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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

*Regulated by State of Florida.

DEPARTMENT OF MANAGEMENT SERVICES
AND OTHER SELECTED STATE AGENCIES

MYFLORIDAMARKETPLACE SYSTEM

TABLE OF CONTENTS

	PAGE NO.
SUMMARY OF FINDINGS	1
System Performance	1
Agency Utilization of MFMP Functions	1
Monitoring of Transaction Fees and Exemptions	1
Risk Assessments.....	1
Security of Data and IT Resources	2
Application Systems Change Management.....	2
Data Management	2
Agency Procedural Deficiencies	2
Statistical Sampling of Payments for Preauditing	2
Continuity of Service.....	2
 BACKGROUND.....	 3
 FINDINGS AND RECOMMENDATIONS.....	 4
Finding No. 1: System Performance.....	4
Finding No. 2: Agency Utilization of MFMP Functions.....	5
Finding No. 3: Monitoring of Transaction Fees and Exemptions.....	7
Finding No. 4: Risk Assessments	8
Finding No. 5: Background Checks	9
Finding No. 6: MFMP Logical Access Controls	9
Finding No. 7: Management of Project Staff Access Privileges	10
Finding No. 8: Management of User Access Privileges	11
Finding No. 9: MFMP Security Administration Policies and Procedures	12
Finding No. 10: Security Controls	13
Finding No. 11: Systems Modification Controls	13
Finding No. 12: Systems Documentation	13
Finding No. 13: Management of Attachments	14
Finding No. 14: Retention of Data	16
Finding No. 15: Agency Procedural Deficiencies	16
Finding No. 16: Duplicate Payments - Agency Issues.....	17
Finding No. 17: Duplicate Payments - MFMP Issues	18
Finding No. 18: Other Data Integrity Issues.....	18
Finding No. 19: MFMP and FLAIR Reconciliation	19
Finding No. 20: Statistical Sampling.....	20
Finding No. 21: Disaster Recovery Risk Assessments.....	21
Finding No. 22: MFMP Back-up	21
Finding No. 23: Environmental Controls	22
 OTHER MATTERS.....	 23
Functional Acceptance	23
Project Staffing.....	23
 PRIOR AUDIT FINDINGS	 24
 AUTHORITY.....	 25

DEPARTMENT OF MANAGEMENT SERVICES
AND OTHER SELECTED STATE AGENCIES

MYFLORIDAMARKETPLACE SYSTEM

TABLE OF CONTENTS – (CONTINUED)

	PAGE NO.
MANAGEMENT RESPONSES	26
APPENDIX LIST	27
Appendix A: MFMP Utilization Survey Summary	28
Appendix B: MFMP Agency Liaison Survey Results	29
Appendix C: Management Responses.....	43
Department of Management Services.....	43
Department of Children and Family Services	60
Department of Corrections	62
Department of Education	65
Department of Financial Services	67
Department of Health.....	69
Department of Highway Safety and Motor Vehicles	73
Department of Law Enforcement	75
Department of Revenue	77
Department of State	80
Department of Transportation	82
Department of Veterans’ Affairs	85
Executive Office of the Governor.....	86
Fish and Wildlife Conservation Commission	87

SUMMARY OF FINDINGS

MyFloridaMarketPlace (MFMP) is a Web-based electronic procurement system for State agencies. Maintained and operated by Accenture, LLP, (Accenture) under contract with DMS, MFMP is designed to enable State agencies to procure commodities and contractual services on-line 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 selected general and application information technology (IT) controls related to the MFMP Buyer Component during the period July 1, 2005, through June 30, 2006, and selected DMS actions through August 31, 2006. We also evaluated DMS's progress in addressing MFMP control deficiencies noted in audit report No. 2006-015. In addition, we conducted audit field work at 14 State agencies, including DMS, for the period July 1, 2005, through January 31, 2006, and selected actions through September 14, 2006, that focused on evaluating agency MFMP processes and related internal controls.

As a part of this audit, we conducted two surveys of State agencies regarding their use of, and satisfaction with, MFMP. The results of these surveys are disclosed in Appendices A and B, respectively.

Our audit of MFMP disclosed that DMS is making progress in addressing the issues noted in the prior audit report No. 2006-015 and initiated actions to address certain issues raised in our current audit. However, numerous MFMP IT controls and State agency user controls still need improvement. These matters are summarized below:

System Performance

Proper management of system performance is an important aspect of IT service delivery. We observed, and MFMP users reported, instances of MFMP system performance problems throughout the audit period. DMS had taken steps to address system performance, but we continued to note aspects of DMS's management of system performance that needed improvement. **(Finding No. 1)**

Agency Utilization of MFMP Functions

Our audit field work at the 14 State agencies disclosed that few agencies were fully utilizing all the functional capabilities available in MFMP. Agencies gave various reasons for not using certain MFMP functions and some agencies relied on workarounds or alternate systems in lieu of MFMP functionality. **(Finding No. 2)**

Monitoring of Transaction Fees and Exemptions

Florida law and administrative rules provide that DMS may collect fees from vendors for the use of MFMP. While transactions may be exempt for a number of reasons, agency transactions involving commodities and contractual services are generally assessed a one-percent transaction fee, which the vendor shall pay to the State. We noted that improvements were needed in DMS's review and follow-up process for the appropriateness of the application of transaction fees and exemptions. **(Finding No. 3)**

Risk Assessments

IT risk assessment is a process of identifying and evaluating information risks that are relevant to the achievement of entity business objectives. The MFMP project team had not been tracking project risks as described in the approved Risk Management Process for MFMP. **(Finding No. 4)**

Security of Data and IT Resources

IT security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that the management of MFMP security continued to need improvement in the areas of conducting background checks of Accenture personnel; controlling access at the application system, operating system, and database levels; ensuring the appropriateness of project staff and user access privileges; providing comprehensive security policies and procedures; and other specific areas not disclosed in detail in this report to avoid jeopardizing MFMP security. **(Finding Nos. 5 through 10)**

Application Systems Change Management

Effective management of application system changes helps ensure that the ongoing integrity of a system is preserved over time as the system is changed. Our audit disclosed instances where neither DMS nor end-user approval of system changes and operational data updates (data changes made by Accenture on behalf of users) had been obtained prior to the changes becoming operational. We also noted instances where the MFMP design specifications had not been updated to reflect system changes or contained inaccuracies. **(Finding Nos. 11 and 12)**

Data Management

Effective data management controls help ensure the integrity of information stored within a system. We continued to note deficiencies in the management of electronic documents within MFMP that serve as attachments to procurement records. Additionally, DMS had not established maintenance procedures to ensure the ongoing retention and usability of electronic records pursuant to Department of State Rules. We also noted instances of duplicate payments initiated from MFMP and processed by FLAIR for payment. We noted other data integrity issues within MFMP and we continued to find data inconsistencies between MFMP and FLAIR. Further, DMS had not established a mechanism for reconciling MFMP and FLAIR transaction data. **(Finding Nos. 13, 14, 16, 17, 18, and 19)**

Agency Procedural Deficiencies

Effective procedures and guidelines are necessary to promote end-users' complete understanding and proper use of MFMP. Our audit field work at the 14 State agencies disclosed instances where written procedures or guidelines for key MFMP processes were lacking and where procedural deficiencies existed regarding the issuance of direct orders (purchase orders), invoice reconciliations (the process whereby invoices are compared to direct orders), and processing of payments. **(Finding No. 15)**

Statistical Sampling of Payments for Preauditing

MFMP's Statistical Sampling Module was used by DFS to perform a preaudit of payments. Improvements were needed in the operation of the sampling process to provide increased assurance of its validity. **(Finding No. 20)**

Continuity of Service

IT service continuity is protected through such measures as disaster recovery planning and appropriate provisions for making and safeguarding copies of software and data. Risk assessment elements within the MFMP disaster recovery plan needed enhancement. Additionally, improvements were needed in MFMP program and data back-up provisions and in environmental controls at the Tallahassee facility that housed the MFMP development environment and served as a back-up site to the primary hosting facility. **(Finding Nos. 21 through 23)**

BACKGROUND

As authorized by Section 287.057(23)(a), Florida Statutes, DMS, 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. In addition, portions of the contract, such as the hosting facility where the MFMP hardware is housed, have been subcontracted by Accenture.

Accenture developed MFMP by heavily customizing Ariba's commercial off-the-shelf procurement solution. The Ariba procurement solution is a standardized software product that is upgraded and supported by Ariba, and it contains a significant amount of proprietary code and related documentation to which neither Accenture nor DMS have full access.

Pursuant to Section 215.94(4), Florida Statutes, DMS is the functional owner of MFMP. As a result, DMS staff are responsible for the final decisions regarding features and implementation of MFMP. DMS maintains that MFMP is a tool for the agencies to use and, as such, allowed the system to be customized to a certain extent for each individual agency's needs. DMS characterized the level of customizations of the Ariba software for the State of Florida as being major.

MFMP interfaces with the State's accounting system, FLAIR, and an interface with the State's replacement accounting system (Aspire) was under development as of the completion of our audit. MFMP was designed and serves as a tool to collect data from State purchasing activities and to communicate applicable data to FLAIR. MFMP is also able to store necessary supporting documents as attachments to transactions. As such, it 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 could optionally initiate an encumbrance in FLAIR for MFMP approved requisitions. Additionally, once goods were received and the process for payment was completed in MFMP, the transaction was to be sent to FLAIR for payment. Payment information was then to be sent back from FLAIR and posted in MFMP.

DFS performs a preaudit of invoices on a sampling basis before they are paid in FLAIR. For MFMP-initiated transactions, the DFS sampling and preaudit takes place in MFMP.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: System Performance

An important aspect of IT service delivery is the management of system performance. Effective performance management includes the following:

- Monitoring and assessment of system performance on an ongoing basis, taking into consideration forecasts of future system workload, to address capacity and efficiency issues before system performance becomes significantly degraded.
- A sound plan for archiving data, consistent with legal and business requirements, to provide efficiencies in data storage.

Our review of Help Desk calls, MFMP status reports, Third-Party Monitor Interim Project Progress Reports, and other internal DMS communications, as well as our observations of MFMP performance as a part of various audit procedures, disclosed that system performance problems occurred throughout the audit period. In addition, responses to our survey of agency liaisons (Appendix B) included numerous comments regarding poor system performance and indicated that this issue was impacting the ability of the agencies to use the system.

We noted the following issues related to system performance and DMS's management thereof:

- DMS had not performed a load or stress test of the system since July 15, 2003, despite additions to hardware capacity. Load testing refers to the process of modeling the expected usage of a software program by simulating multiple users accessing the program's services concurrently. When the load placed on the system is raised beyond normal usage patterns in order to test the system's performance at unusually high or peak loads, it is known as stress testing. In the Third-Party Monitor (North Highland) Interim Project Progress Report submitted to DMS on October 19, 2005, North Highland also noted the lack of load testing. In response to our audit inquiries, DMS staff stated on June 22, 2006, that Accenture had purchased Mercury LoadRunner, a load testing software product, and was in the process of developing a load testing strategy.
- On October 18, 2005, DMS and Accenture executed Modification 4 to the MFMP contract. Attachment A, Section 3.0 of this modification prescribed specific performance criteria for the operation of MFMP, specifically, software application average response time. This was the primary metric for measuring system performance. Our evaluation of this metric concluded that it was not adequate to report on the true state of system performance because it relied on averaging all measurements from the month, thereby smoothing any peaks in the measurements. In response to our audit inquiries, DMS staff acknowledged that the metrics were not a complete indication of system performance.
- The data that drives the reporting on average response time was provided by Accenture, but DMS was unable to independently verify the accuracy of this data in its entirety. In response to our audit inquiries, DMS recognized the need to be able to independently verify this data. DMS staff further indicated that they and North Highland were working with Accenture to develop a process to independently verify the metrics, but that the process was extremely resource intensive and required skill sets that DMS was actively trying to acquire.

DMS's efforts to improve system performance included installing additional central processing units in March and May of 2005. In May 2006, DMS also installed a new application server to improve MFMP system response time. However, issues were encountered impacting system stability and performance, resulting in DMS reverting back to the former server. DMS also made adjustments to the application, issued guidance, and provided training to users, to assist in improving the performance of MFMP.

DMS also noted that attachment size, search parameters, the number of concurrent users, agency workflow configurations, and application memory management all have potentially contributed to system performance issues. DMS staff indicated that they were tracking each of these issues and discussing them at the MFMP project weekly meetings. However, without periodic load and stress testing and comprehensive, verifiable performance metrics, DMS lacks a baseline to determine the effectiveness of its efforts to improve performance.

DMS was running version 7.1a of the Ariba Buyer application. Ariba will cease providing technical support and fixes for version 7.1a on March 31, 2007. On August 22, 2006, DMS staff indicated that Accenture was in the process of making arrangements for support of version 7.1a past March 31, 2007.

The latest version of Ariba Buyer is 8.2 and Ariba plans to release version 9 in Winter 2006. Version 8.2 provides improved memory management and more effective load balancing to more evenly spread the transaction workload. In addition, a new feature in version 8.2 is the ability to archive data, which would free up space in the database. DMS staff stated that these capabilities would be of great benefit in helping to resolve ongoing system performance issues. DMS staff stated that they would be implementing the Ariba upgrade to version 8.2 and that they were working to establish an implementation date.

Recommendation: DMS should continue with efforts to resolve system performance issues. DMS should also ensure that periodic load and stress testing is performed and that verifiable performance metrics are maintained.

Finding No. 2: Agency Utilization of MFMP Functions

Agencies are required by Section 287.057(23)(a), Florida Statutes, to participate in the online procurement system and by DMS Rule 60A-1.030(2), Florida Administrative Code, to procure commodities and contractual services from MFMP-registered vendors unless granted a specific exemption. In order to gain an understanding of the degree to which agencies were utilizing MFMP, we conducted a survey of the 14 State agencies regarding the functionalities used as of April 30, 2006. Our analysis of the survey responses, as shown by Appendix A, disclosed that few agencies were fully utilizing all the functional capabilities available in MFMP. We found that several agencies were using MFMP to create and approve requisitions; initiate encumbrances; authorize payments for direct (purchase) orders; search for and select vendors; and store procurement support documents. However, few agencies were using MFMP to encumber or make payments on master agreements (contracts); process purchasing card transactions; assist with year-end reporting; report to oversight entities; or report spend (expenditures initiated through MFMP) for budget requests. As described in the paragraphs below, agencies cited functional limitations, system performance, and workflow inefficiencies as reasons for not using all MFMP functions:

- Users have the option of encumbering funds in MFMP when initiating a procurement. When a requisition is encumbered, MFMP utilizes a FLAIR interface, whereby a request is automatically sent to FLAIR to verify availability of funds, allowing for a budget check prior to creation of a direct order. As described below, our review disclosed that some agencies were not utilizing MFMP for either encumbrance or receiving functions.
 - DOE staff did not process encumbrances in MFMP, stating that encumbrances initiated in MFMP could not be modified manually, impeding control of encumbrances for planning and budgeting purposes.
 - DOR staff stated that as of July 1, 2006, they had ceased processing encumbrances in MFMP, because they had experienced the following system errors: purchase requests had been double encumbered, accounting information had been improperly split during the Invoice Reconciliation

process, and MFMP transactions failed to encumber in FLAIR. DOR staff further indicated that the MFMP assignment of different numbers to procurement documents for a single transaction hindered research. Finally, DOR staff stated that they stopped using the receiving function in MFMP in January 2006 due to confusion that the process caused with end-users.

- DOT staff ceased using MFMP for processing encumbrances on March 15, 2004, utilizing an in-house information system, as described below.
- Some agencies had only recently begun processing payments in MFMP on a limited basis, while other agencies had discontinued processing payments in MFMP. Users have the option to bypass MFMP and process payments for goods and services directly in FLAIR. However, by doing so, users may also bypass some of the system control features, such as edit checks against processing invoices for payment multiple times. (Refer to Finding No. 16.) In response to our audit inquiries, agencies provided a variety of explanations for choosing to process payments directly in FLAIR rather than MFMP, as described below:
 - DCFS staff indicated that initial testing of system performance, workload considerations, and workforce reductions persuaded staff that prompt payment compliance goals would not be met if payments were processed through MFMP. Thus, DCFS did not begin to utilize the MFMP payment process until November 2005, and then only for two district offices. Some additional districts began utilizing the process in January 2006.
 - As of September 2005, DOR discontinued processing payments through MFMP and attaching documents (for example, invoices) except those initiated via an invoice eform (electronic invoice) from a vendor stating “Due to the volume of errors encountered, the inflexibility of MFMP in correcting payment-related issues, and the apparent inability to modify the system to correct the problems, we were unable to find a practical and efficient way to utilize MFMP to process FLAIR payments.”
 - In January 2006, DOT Central Office discontinued paying for all purchases through MFMP, suggesting that MFMP system performance issues jeopardized meeting the 20-day invoice filing requirements mandated by Section 215.422, Florida Statutes. To enhance workload efficiencies, DOT discontinued processing payments for services requiring master agreements in MFMP in February 2006.
 - In May 2006, DOH and DLE discontinued utilizing the MFMP payment process, both citing numerous problems encountered with paying invoices in MFMP, as well as problems with invoice attachments containing confidential information.

Our review also disclosed that some agencies were utilizing alternative systems in place of certain functionalities available in MFMP, as described below:

- DOT staff utilized an in-house information system to manage encumbrances indicating that they encountered numerous difficulties in trying to process encumbrances in MFMP and that MFMP’s encumbrance function did not facilitate compliance with the statutory requirements of Section 339.135(2)(a), Florida Statutes.
- DCFS and DOC utilized an in-house system for initiating and approving purchase requisitions. After approval and budget check, the information was entered into MFMP.
- Except for three field offices, DLE staff used e-mail for initiating and assigning purchase requisitions to Purchasing staff. Alternatively, requesters completed a hardcopy requisition form and submitted the form to the Purchasing staff for approval and entry of the information into MFMP.

It appears from responses to our surveys (Appendices A and B) that State agency utilization of MFMP is declining for a variety of reasons. In response to our audit inquiries regarding agency utilization of MFMP functions, DMS staff stated that they had initiated measures to address various problems utilizing the functional capabilities available within MFMP. These measures included maintaining an MFMP Help Desk, providing

system training, facilitating multi-agency focus groups, and providing monthly on-line system updates. Also, DMS had recently revamped the MFMP training environment and added a Process Improvement Team consisting of expert end-users from various agencies. Notwithstanding these efforts of DMS, our audit showed that rather than embracing the functionality of MFMP, some agency users have found it necessary to rely upon workarounds and alternate systems. Should DMS's efforts fail and the inconsistent use of MFMP functionality continue, it is not clear that MFMP will be able to operate efficiently and effectively as an agency-level procurement system or as a subsystem of the Florida Financial Management Information System, pursuant to Section 215.93, Florida Statutes.

Recommendation: In addition to resolving the performance problems, as discussed in Finding No. 1, DMS should continue to communicate and work with State agencies to increase user awareness and expertise regarding MFMP functionality. We also recommend that State agencies reconsider their utilization of MFMP functionality and the necessity of maintaining alternative systems.

Furthermore, DMS should conduct a complete survey of all State agencies, subject to the Florida Financial Management Information System Act (Sections 215.90 through 215.96, Florida Statutes), to identify the MFMP functionality used by each and, for the functions not employed, explanations as to why MFMP is not being used. This information should be provided to the Financial Management Information Board for its use in ensuring that the Florida Financial Management Information System operates efficiently as an integrated financial management information system and provides accurate and complete financial information necessary to the effective operation of State government.

Finding No. 3: Monitoring of Transaction Fees and Exemptions

Section 287.057(23)(c), Florida Statutes, provides that DMS may collect fees for the use of the on-line procurement system. The fees may be imposed on an individual transaction basis or as a fixed percentage of the cost savings generated. At a minimum, the fees must be set in an amount sufficient to cover the projected costs of such services, including administrative and project service costs in accordance with the policies of DMS.

DMS Rule 60A-1.031, Florida Administrative Code, further provides that unless the transaction is exempt from the fee, all agency transactions involving commodities and contractual services shall be assessed a transaction fee of one percent, which the vendor shall pay to the State. Transactions can be exempt depending upon the type of vendor, the type of product or service, and the program for which the purchase is made. For example, transactions relating to government and non-profit vendors are exempt from the fee. The MFMP operations plan indicated that it is the responsibility of DMS to review exempted transactions for compliance with the above rule.

In audit report No. 2006-015, we noted that DMS staff were reviewing exempted transactions, but that there were aspects of the review process that needed improvement. Our current audit disclosed the following:

- Pursuant to Section 20.055(5)(g), Florida Statutes, the DMS Inspector General provided, on April 4, 2006, a report to the Secretary on the status of corrective actions taken regarding the findings in audit report No. 2006-015. The status report stated that the DMS MFMP team continued to review the three exemption code categories that encompassed 98 percent of the exemption volume. Our audit noted that DMS had not performed a transaction fee exemption verification since September 2005, which was for the month of August 2005. In response to our audit inquiries, DMS staff stated that they performed an internal review of the monthly MFMP Fee Exemption Analysis report prepared by Accenture; however, they took no formal actions as a result of the review. DMS staff also stated that they expected to resume monitoring exemptions on September 1, 2006.

- The Transaction Fee Exemption Verification Process diagram was not up-to-date and there were no associated written desk procedures for the process. In response to our audit inquiries, the Transaction Fee Exemption Verification Process diagram was updated on May 11, 2006.
- Section 570.07(41), Florida Statutes, provides that the Department of Agriculture and Consumer Services has been exempted from using MFMP and allowed to continue with its use of its own on-line system. However, vendors utilizing such system shall be pre-qualified as meeting mandatory requirements and qualifications and shall remit fees pursuant to Section 287.057(23)(c), Florida Statutes. DMS did not have a mechanism in place to monitor Department of Agriculture and Consumer Services transactions for payment of the one-percent transaction fee.
- DMS instituted a Vendor Registration Verification Process to evaluate vendors suspected of incorrectly registering as government or non-profit organizations when they should have registered as corporations that would be subject to the transaction fee. On December 16, 2005, DMS sent a mass e-mail to 2,946 vendors of which 2,242 were successfully transmitted and 704 failed transmission. The e-mail requested the vendors to update their business designation in MFMP and stated that if they did not, their business designation would be updated to corporation status in January 2006. The e-mail further stated that if the vendor did not respond by January 6, 2006, it would be assumed that the vendor approved the update. Despite the January 6, 2006 deadline, this update process was not completed until April 27, 2006, at which time 2,192 vendors had their designations changed. In response to our audit inquiries, DMS staff indicated that they were following-up on the 704 failed e-mails and anticipated completing this process in August 2006. DMS staff also indicated that they had no plans to attempt to recoup the unassessed fees. We requested, but as of August 25, 2006, DMS had not yet quantified, the resulting dollar amount of unassessed fees.

Absent sufficient monitoring of vendor application of the transaction fee, the risk is increased that exemptions not properly applied according to Florida law and rules will not be detected by DMS.

Recommendation: DMS should enhance its monitoring of exemptions to the one-percent transaction fee to include a thorough and documented review of exemptions to provide further assurance that exemptions are appropriately applied and fees appropriately assessed for past and future transactions. DMS should also determine whether other findings in this report, for example Finding Nos. 2, 15, 16, 17, and 19, have any potential impact on the one-percent transaction fee.

Finding No. 4: Risk Assessments

IT risk management practices include the establishment of a systematic risk assessment framework through which an assessment is performed on a regular basis of the relevant information risks to the achievement of business objectives. The risk assessment forms the basis for determining how the risks should be managed at an acceptable level.

Deliverable 14 of the contract between DMS and Accenture, a Risk Management Process, was approved by DMS on July 7, 2003, and defined a process to predict, capture, monitor, avoid, manage, and resolve risks that may adversely affect the MFMP project. We determined that the MFMP project team had not been tracking project risks as described in the Risk Management Process. Additionally, in the Third-Party Monitor Interim Project Progress Report submitted to DMS on October 19, 2005, North Highland reported that the Risk Management Process was not being followed and indicated that no risks had been noted since February 2005.

DMS staff stated that, between September 2005 and May 2006, they requested Accenture to provide a risk assessment on several occasions. In response to our audit inquiries, DMS staff stated that they received a draft risk assessment from Accenture in May 2006. DMS staff additionally stated that, on June 7, 2006, a MFMP management meeting was conducted to review the assessment and a continuing risk review process was being

implemented. The lack of a comprehensive risk management process increases the risk that management will not plan for, and attempt to mitigate, all relevant risks to the MFMP project.

Recommendation: Consistent with the approved Risk Management Process, DMS should ensure that risks relevant to the successful operation of MFMP, and the business objectives dependent thereon, are regularly identified and assessed. DMS should use the risk assessment information to identify cost-effective risk reduction solutions, and monitor and report on the progress of risk reduction actions.

Finding No. 5: Background Checks

State Technology Office (STO) Rule 60DD-2.001(2)(a)(80), Florida Administrative Code, defines “position of special 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. STO Rule 60DD-2.008(2)(c), Florida Administrative Code, additionally requires that agencies shall conduct background investigations for personnel in positions of special trust. DMS’s internal administrative policy incorporates these rules and provides that they are applicable to contractor employees in positions of special trust. The contract between DMS and Accenture provides that Accenture shall perform reasonable security and background searches on all its employees and subcontractors’ employees performing work on MFMP.

DMS had no documentation to demonstrate that background checks were performed for Accenture staff working on the MFMP project. DMS staff stated that they had inquired as to Accenture’s performance of background checks for staff working on the project, as well as for new staff added to the project. Absent DMS review of documented background checks, the risk is increased that a person with an inappropriate background could be placed in a position of special trust.

Recommendation: DMS should obtain and review documentation of the performance and results of all background checks performed for contractor employees.

Finding No. 6: MFMP Logical Access Controls

Logical access controls are intended to restrict electronic, as opposed to physical, access to computer software and data files. STO Rule 60DD-2.002(1)(b), Florida Administrative Code, provides that access to data files shall be limited to those individuals authorized. STO Rules 60DD-2.004(1)(a) and 60DD-2.004(2)(a), Florida Administrative Code, respectively, provide that unique identifiers and personal passwords will be used to authenticate users. Strong password controls include provisions requiring an initial password change on first use, limits on the number of invalid log-on attempts, and prohibition on the reuse of recent generations of passwords.

Our review of logical access controls at the application, operating system, and database levels disclosed the following deficiencies:

- End-users were not automatically required by the system to change their application access account password upon the first log-on to the system. On May 25, 2006, DMS implemented a system modification requiring users to change their account password at initial sign-on.
- Individuals with access accounts used by Accenture system and database administrators to remotely connect to off-site MFMP equipment were not automatically required by the system to change their account password upon the first log-on to the system. In response to our audit inquiries, DMS staff indicated that Accenture had a manual process in place where the new account holder was requested to change his or her password in the presence of a security administrator immediately after the account was

created. However, if not enforced by the system, this control may be insufficient to assure that the password is changed on the user's first log-on.

Weak MFMP logical access controls increase the risk of unauthorized use of MFMP.

Recommendation: DMS should strengthen MFMP logical access controls to reduce the risk of compromise to MFMP information.

Finding No. 7: Management of Project Staff Access Privileges

Proper access controls limit system access privileges to only what is needed to perform assigned duties and restrict individuals from performing incompatible functions. Such controls include taking immediate action to remove access privileges for terminated or reassigned employees and contractor staff. Management's oversight of the use of access privileges is facilitated by assigning a unique system identifier (user ID) to all users for their sole use, thereby allowing all system activities to be traced to the responsible individual.

Our audit of MFMP access controls disclosed instances of excessive or inappropriate project staff access privileges and other deficiencies, as described below:

- Six DMS MFMP project staff had application update access greater than what was needed for their job functions. Between May 16, 2006, and May 26, 2006, subsequent to our audit inquiries, the excessive access was removed for all six individuals.
- Four Accenture MFMP project staff had application update access greater than what was needed for their job functions. Subsequent to our audit inquiries, the excessive access was removed on June 26, 2006.
- The application access privileges of two Accenture employees no longer assigned to the MFMP project were not removed in a timely manner. For these two employees, access was removed 23 and 25 days after leaving the project. For an additional two employees no longer assigned to the MFMP project, Accenture was unable to document exactly when access was removed, but was able to demonstrate that access had been removed by April 18, 2006. As a result, for these two employees, we were unable to determine if the access was removed in a timely manner. However, we determined that none of the four accounts were used after the date the respective Accenture staff member left the MFMP project.
- For 16 Accenture staff no longer on the MFMP project, Accenture had not documented when their network access was removed. Therefore, we were unable to determine if access was removed in a timely manner. Additionally, Accenture could not determine whether the accounts had been used after termination; however, it was able to demonstrate that all access was removed as of May 19, 2006.
- For one database access account, an Accenture staff member had various update capabilities that were not necessary for the staff member's job function. Subsequent to our audit inquiries, the account was deactivated on June 7, 2006.
- A database ID created to facilitate a security scan was not deleted upon the December 14, 2005, completion of the scan. Subsequent to our audit inquiries, the account was deleted on June 1, 2006, 169 days after it was no longer needed.
- Database administrators did not have unique user IDs for accessing the database and shared the same account to perform their database administrative functions. Therefore, activities performed in the system by these individuals could not be traced to the responsible person.
- Perforce is a software configuration management system designed to manage and control revisions to source program code. Two Accenture MFMP systems administrators had Perforce access to perform code migrations. This access was incompatible with their systems administrator functions.
- Accenture was contracted by another state for a separate project. Accenture used the same Perforce environment to manage both projects. As a result, 11 Perforce accounts belonging to the other state's

Accenture project employees inappropriately had access to Florida's MFMP source code. With this access, Accenture's staff had the ability to view and change Florida's source code. However, in response to our audit inquiries, DMS staff stated that Accenture's change control process would have prevented these changes from being migrated to the production environment. DMS staff also stated that Accenture was unable to determine if any of the other state's project staff had used this ability to access Florida's source code. Subsequent to our audit inquiries, five of the accounts were deleted as of June 9, 2006, after Accenture determined that these accounts were assigned to staff that were no longer on the other state's project. We noted one additional account that was inappropriately shared between the two projects. In a response dated June 27, 2006, DMS staff indicated that Accenture was in the process of researching ways to segregate the two projects' resources managed through Perforce.

- One Perforce account was assigned to an employee who terminated on October 31, 2003. We determined that the account was last used on June 1, 2006. DMS staff indicated that this account was being used as an Accenture administrative account by other Accenture staff, but acknowledged that there was no justification for its use. Subsequent to our audit inquiries, Accenture deleted this account on June 8, 2006, or 951 days after the user left the project.
- We identified one additional Perforce user account that DMS staff indicated Accenture agreed was unnecessary. Subsequent to our audit inquiries, the account was removed on June 9, 2006.

Without proper segregation of duties and controls over access privileges, individuals may possess more access rights than are necessary to perform their job functions. Excessive access to the system could enable an individual to commit malicious or harmful actions. Sharing of access accounts limits the ability to trace system activities to the responsible individual.

Recommendation: DMS should periodically analyze the functions of MFMP project staff to ensure that access privileges are appropriate and commensurate with individuals' job duties. In addition, DMS should ensure that MFMP access for terminated, transferred, or reassigned Accenture personnel is removed in a timely manner. Additionally, database administrators should immediately cease the sharing of user IDs and each designated individual should be assigned a unique user ID with a corresponding password.

Finding No. 8: Management of User Access Privileges

As similarly discussed in Finding No. 7, access privileges must be appropriately managed for end-users of an application system to ensure that users can only perform those system functions needed for their job duties, to enforce a proper segregation of duties, and to enable management to monitor employees' system activity.

In MFMP, users are designated certain roles authorized by management, based upon the agency's workflow and other access needs. Within roles, management grants users permissions to perform various functions. Roles and permissions comprise the user's profile and, when used appropriately, provide an effective means of internal control over Web-based procurement.

Our audit field work disclosed the following end-user access control deficiencies in MFMP:

- At DFS, we noted that an unusually large number of expenditure transactions (30 of 40 tested) were requisitioned under the same user ID. In response to our audit inquiries, DFS staff informed us that the user ID was shared by two employees. At DLE, purchasing staff used a common password to accommodate workload sharing. The sharing of a user ID or password limits the ability to assign responsibility for a transaction to an individual employee, thereby overriding a basic control of any IT system.
- At DMS and FWCC, staff did not routinely review the weekly Buyer Adoption Report (a listing of current users and their respective roles and permissions) during the audit period. Without routinely

reviewing the report, agencies may be unaware of user accounts that are no longer appropriate and that should be inactivated. For example, at DMS, the Buyer Adoption Report contained outdated, conflicting, and erroneous role assignments:

- Two “temporary” accounts with the role of System Administrator and an unlimited dollar approval threshold were included in the DMS Buyer Adoption Report. In response to our audit inquiries, DMS staff stated that they were unaware of who had access to these temporary accounts or the purpose for their continuance.
- Contrary to the instructions provided by MFMP Buyer Training, one employee had the conflicting roles of “FLAIR Access Controller” and “Invoice Manager.” These roles should be segregated to ensure that encumbrances are properly validated. DMS staff stated that this employee had performed system testing during the implementation phase of MFMP and had apparently retained the related roles and permissions after being transferred from the MFMP project team.
- One employee, other than the designated System Administrator and back-up and the two temporary accounts mentioned above, had the role of System Administrator erroneously included in his MFMP user profile.

The above-listed deficiencies increase the risk that inappropriate transactions could be processed without timely detection and assets could be misappropriated.

Recommendation: Agencies should periodically analyze the functions of their employees to ensure that MFMP user access privileges are appropriate and commensurate with users’ job duties. Additionally, agencies should immediately cease the sharing of user IDs or passwords and assign each designated system user a unique user ID with a corresponding password. Further, agencies should regularly review the weekly Buyer Adoption Report and immediately remove any user accounts deemed no longer appropriate.

Finding No. 9: MFMP Security Administration Policies and Procedures

STO Rule 60DD-2.001(3), Florida Administrative Code, provides that each agency shall develop, implement, and maintain an information resource security program that produces, among other things, documented and distributed security policies. This rule also provides that the responsibilities and roles of information security managers and data security administrators must be clearly defined.

We noted deficiencies in MFMP security administration policies and procedures. Specifically:

- As also noted in audit report No. 2006-015, DMS had not developed policies that defined the responsibilities of security administration for DMS. Such policies should include responsibilities for overseeing agencies’ administration of agency-level security and Accenture’s administration of system security. Additionally, DMS had not developed policies and procedures to periodically monitor Accenture staff access to MFMP. Subsequent to our audit inquiries, DMS established, by June 23, 2006, written procedures for these responsibilities.
- DMS had not developed procedures to guide the agencies in administering application access, including guidance in the appropriate segregation of duties when delegating user authority and in revoking or adjusting access privileges as a result of the termination, transfer, and reassignment of system users. In response to our audit inquiries, DMS staff stated that they developed guidance for terminations, transfers, and reassignments on March 1, 2006, and for segregation of duties on June 20, 2006. Additionally, in July and August 2006, DMS held training sessions with agency system administrators to review MFMP security policies.

The lack of these procedures may have contributed to the deficiencies disclosed in Finding Nos. 7 and 8, regarding MFMP project staff and State agencies’ access. Without effective written policies to govern the security

administration functions of MFMP, the risk is increased that nonstandard or inconsistently applied operating and control activities could compromise the system's integrity. In the absence of defined security administration responsibilities, including appropriate checks and balances from DMS, the risk is increased that Accenture will not appropriately administer its staff's access to MFMP.

Recommendation: DMS should ensure that its newly implemented security administration policies and procedures are followed. Additionally, in future system development projects of this nature, DMS should establish relevant policies and procedures more timely upon system implementation.

Finding No. 10: Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of data and IT resources. During our audit, we identified deficiencies in certain aspects of DMS's IT security controls in addition to the matters noted in Finding Nos. 5, 6, 7, 8, and 9. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising DMS's IT security controls. However, the appropriate DMS personnel have been notified of the deficiencies.

Recommendation: DMS should improve the deficient security control features and enhance the safeguarding of DMS IT resources.

Finding No. 11: Systems Modification Controls

Effective system modification controls include procedures for a documented evaluation and acceptance of information system modifications by both user and IT management. During both the system modification and operational data update processes, neither DMS nor the end-user officially approved changes subsequent to development and prior to Accenture migrating the changes into production. We examined 30 system modifications and 20 operational data updates and found no evidence of DMS or end-user approval for any of the items tested.

For system modifications, DMS staff stated that Accenture prepared a list of program modifications for DMS management's review prior to migration into production. If there was no explicit objection from DMS, approval of the changes was implied. In response to our audit inquiries, DMS staff indicated that, beginning in July 2006, they anticipated implementing an official sign-off release document. DMS staff also stated that end-user involvement was optional at DMS's discretion for system modifications. DMS staff acknowledged that documentation of approvals and end-user involvement were areas for improvement.

Lack of management and user approvals increase the risk that either unauthorized or unintended changes could be migrated into the production environment.

Recommendation: DMS should ensure that the program change process incorporates adequate user involvement and written approval for all system enhancements and changes.

Finding No. 12: Systems Documentation

A proper implementation of system changes includes updates to the applicable system and user documentation and procedures. Our review of MFMP design specifications noted the following instances in which the design specifications were not updated to reflect system changes or to correct inaccuracies in the documents:

- Design ID: FLDD002 – Business Rules, did not document the existence of exemptions for certain agencies for interagency approval for certain commodities (information technology, insurance, and fleet).
- Design ID: FLDD072 - Authentication, contained contradictions with regard to the specifications for password length and composition requirements.
- We tested 20 systems development changes that involved code changes and would, therefore, require updates to systems design specifications. We noted that the systems design specifications were not updated for any of the 20 changes.

In response to our audit inquiries regarding the above items, DMS staff stated that the original design specifications were not updated because these were contractual deliverables representing a point in time and that subsequent changes to system functionality were captured via separate design documents. Our review of the separate design documents noted that they were not comprehensive and were specific only to the change being made. DMS staff also stated that they were in the process of creating crosswalks to tie these changes to the related overall design documents. We reviewed an example of a crosswalk and determined that it was a complex, inefficient process for determining the current state of the system. Additionally, this mechanism would only cover changes to documentation due to system changes and, as a result, there was no mechanism for making changes to systems documentation to correct errors or contradictions in the design specifications.

Without continuous updates to systems documentation, the risk is increased that documentation will become obsolete and unusable for the purpose of understanding and documenting the system. This, in turn, increases the risk that future changes may adversely affect the system by conflicting with previous, undocumented or poorly documented changes.

Recommendation: In addition to maintaining a historical copy of the original design documents, DMS should maintain updated versions of the documents to serve as documentation of the current state of the system.

Finding No. 13: Management of Attachments

MFMP has the ability to store documents electronically as attachments to procurement records, and these documents may at times contain information deemed nonpublic pursuant to various provisions of State and Federal laws. State and Federal laws limiting the disclosure of certain information include, for example:

- Section 119.071(5)(a)3., Florida Statutes, provides that all social security numbers held by agencies are confidential and exempt from public disclosure.
- Section 119.071(4)(d)1., Florida Statutes, provides additional exemptions for personal information relating to law enforcement officers.
- Section 985.31(4)(k), Florida Statutes, provides that selected juvenile medical records are confidential.
- Title II of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) sets a national standard to protect the privacy of an individual's health care information in any format (including oral, physical, and electronic media) and ensures the security of an individual's health care information that is maintained or transmitted electronically when created, used, and disposed.

Sections 215.93(5) and 215.94(4), Florida Statutes, provide that DMS, as functional owner of MFMP, is legally responsible for the security and integrity of all data records existing within or transferred from its information subsystems. Furthermore, Section 119.07(2)(b), Florida Statutes, provides that the custodian of public records shall provide safeguards to protect the contents of public records from unauthorized remote electronic access or

alteration and to prevent the disclosure or modification of those portions of public records which are exempt or confidential.

In audit report No. 2006-015, we noted that there was not a mechanism in MFMP to purge attachments from the system. On November 29, 2005, DMS implemented an attachment removal request process to allow the agencies to request a purge of attachments containing confidential information.

As also noted in audit report No. 2006-015, deficiencies existed with regard to the storage of confidential information as attachments in MFMP. Additionally, certain documents were illegible, incomplete, not relevant to the transaction to which they were attached, or unable to be viewed due to the improper naming of the file extension. We reviewed these items again and noted that, at the time of our audit testing, none had been corrected. In response to our audit inquiries, DMS staff indicated that a mass purge of attachments was subsequently completed on May 15, 2006, for all invoices and invoice reconciliations with a status of paid as of April 21, 2006. As a result of this mass purge, the noted attachments were removed from the system.

Our audit tests of additional attachments disclosed 3 attachments that were not in a usable format and 33 attachments that contained confidential information. We notified DMS as well as the agencies from which the transactions containing the attachments originated. In response to our audit inquiries, DMS staff stated that as a result of the mass purge of attachments previously discussed, all of these attachments, except one, were subsequently removed from the system. The remaining attachment was removed on May 25, 2006.

During our audit field work at the 14 State agencies, including DMS, we inquired whether each agency had developed policies and procedures that addressed preventing the introduction of confidential information into MFMP, monitoring documents stored as attachments into MFMP for confidential information, and redacting any confidential information so discovered. While some agencies described measures taken to address confidential information, none of the agencies provided written policies and procedures that specifically addressed confidential information issues within MFMP.

In audit report No. 2006-015, we noted that while DMS had released guidelines to the agencies for handling the above issues, DMS staff also indicated that they believed DMS did not have the authority to require agencies to follow these guidelines. Subsequent to our current year audit inquiries, DMS developed Rule 60A-1.033, Florida Administrative Code, incorporating the above-mentioned guidelines. The draft rule was advertised in the Florida Administrative Weekly on June 2, 2006, and a public hearing was held on June 23, 2006. Additionally, DMS staff indicated that on July 27, 2006, they implemented a system change that would require users to check a box indicating that they were not attaching any confidential information prior to being allowed to attach a document. In further response to our audit inquiries, DMS staff stated that they planned to implement an audit process to monitor and control inappropriate data.

Although access to MFMP was limited to authorized State users, without effective procedures to limit the inclusion of confidential data within MFMP, the risk is increased of the information being disclosed to unauthorized parties. Furthermore, without a mechanism to correct identified errors, the reliability and usability of the data is diminished.

Recommendation: DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to assure that the rule is being followed. Also, DMS should ensure that all confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Finding No. 14: Retention of Data

Department of State Rule 1B-26.003, Florida Administrative Code, governs electronic recordkeeping and provides that for storing record (master) copies of electronic public records through their life cycle, agencies shall select appropriate media and systems which permit easy and accurate retrieval in a timely fashion and allow for the records to be retained in a usable format until their authorized disposition and, when appropriate, meet the requirements necessary for transfer to the Florida State Archives. In addition, the rule provides that agencies should establish procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of the electronic records throughout their authorized life cycle.

As also noted in audit report No. 2006-015, DMS did not have procedures to perform maintenance to ensure the retention and usability of the electronic records throughout their authorized life cycle. On August 29, 2006, in response to our audit inquiries, DMS staff indicated that certain aspects of their design, processes, and procedures conformed to the code and that further analysis would be required to determine if it was fully compliant with the State rule. Without a mechanism to perform regular maintenance, the reliability and usability of the data may be diminished.

Recommendation: DMS should implement procedures to ensure compliance with Department of State Rule 1B-26.003, Florida Administrative Code.

Finding No. 15: Agency Procedural Deficiencies

State agencies are required by Section 287.057(23)(a), Florida Statutes, to participate in the on-line procurement program (MFMP) developed by DMS. MFMP provides Web-based tools to replicate the functions of a typical paper-based purchasing system. In order to use MFMP effectively, State agencies require well-trained staff with a complete understanding of MFMP, agency procurement procedures, and available system support resources.

In our audit field work of the 14 State agencies, we noted that some agencies had not established written procedures or guidelines for key MFMP processes utilized, as well as procedural deficiencies regarding the issuance of direct orders (purchase orders), invoice reconciliations (the process whereby invoices are compared to direct orders), and timely processing of payments. Specifically:

- At DOH, DMS, and DOS, we noted that written procedures or guidelines for key MFMP processes had not been developed. Without written procedures providing guidance on processes utilized such as establishing encumbrances, invoice reconciliations, and payment processing, agencies are at risk that transactions will be processed in a manner inconsistent with management's intent, and sound internal controls.
- Direct orders record management's authorization to acquire goods and services and provide a basis for controlling budgeted appropriations. Our review disclosed that for 54 direct orders tested at DMS, 8 totaling \$26,894 were for services and in some cases were dated subsequent to the beginning of the service period and, in other cases, after receipt of the services.
- DMS procedures did not always ensure that payment of MFMP transactions directly in FLAIR were processed properly. Of 40 invoices tested, we noted 2 that were processed directly in FLAIR but MFMP was not updated for the FLAIR payment data.

Recommendation: To ensure that transactions are consistently and properly reviewed and processed, State agencies should establish written procedures and guidelines for key MFMP processes utilized. These written procedures should specifically:

- Require that approved direct orders are obtained prior to the receipt of any goods or services.
 - Enhance procedures to ensure that MFMP is appropriately updated for invoices paid directly in FLAIR.
-
-

Finding No. 16: Duplicate Payments - Agency Issues

User controls help ensure the integrity of the results of system processing. Our review of selected transactions at 14 State agencies disclosed that the capability to process the payment of a MFMP transaction through either MFMP or directly in FLAIR (see further discussion in Finding No. 19) introduced the risk that an invoice may be paid twice without detection. When making a payment directly in FLAIR, agencies have been instructed to 1) complete and submit an Invoice eForm, 2) check the “Payment completed in FLAIR” box, and 3) complete and submit a Payment Update eForm. According to MFMP, performing these steps updates the payment information in MFMP and assists in keeping FLAIR and MFMP synchronized. When agency personnel complete and submit an Invoice eForm in MFMP, an edit check designed to prevent payment on the same invoice twice is initiated. MFMP performs this edit check a second time, along with verifying encumbrance availability, during the invoice reconciliation process in MFMP. These edit checks are an effective enhancement to DFS preaudit of agency vouchers, but only by following the process outlined above can agencies subject invoices paid in FLAIR to the available MFMP edit checks.

Our limited analytical procedures of selected transactions disclosed that some invoices were erroneously paid twice, some because agencies failed to follow the process outlined above, some because invoices were not properly defaced. Specifically:

- At DVA, our test of 55 applicable transactions disclosed 3 duplicate payments. The first duplicate payment occurred because DVA neglected to follow the process outlined above when paying directly in FLAIR, thus allowing the charge to mistakenly be paid again through MFMP. Another duplicate payment resulted from DVA processing the same invoice twice in MFMP. The vendor invoice was not properly defaced during the initial processing. Additionally, the MFMP edit check did not detect the duplicate submittal for this invoice because two additional characters were added to the vendor invoice number when the Invoice eForm was erroneously completed and submitted in MFMP a second time by a DVA employee. The third duplicate payment occurred because the vendor included the same charge on 2 separate invoices. We alerted DVA of the overpayments totaling \$3,444.
- At DOR, our test of 35 applicable transactions disclosed 3 duplicate payments, resulting from DOR neglecting to follow the process outlined above when paying directly in FLAIR. At the end of our audit field work, DOR was in the process of recovering the overpayments totaling \$4,447, in some cases netting amounts owed against other invoiced amounts due to the vendors.
- At DOT, our test of 15 applicable transactions disclosed 1 duplicate payment resulting from DOT neglecting to follow the process outlined above when paying directly in FLAIR. The overpayment of \$17,381 was netted against other invoiced amounts due to the vendor.
- At DHSMV, our test of 16 applicable transactions disclosed 1 duplicate payment processed in MFMP. In May 2006, in response to our audit inquiries, DHSMV staff inquired about the cause of this duplicate payment and DMS initiated an investigation. As of September 14, 2006, the investigation was still ongoing. The overpayment of \$20,432 was returned by the vendor.

Recommendation: To capitalize on MFMP system edit checks, State agencies should process payments for MFMP transactions through MFMP whenever possible. Agency procedures should require supervisory monitoring of payments made directly in FLAIR to ensure that the Invoice eForms and Payment Update eForms are completed and submitted and the “Payment completed in FLAIR” box is checked. Also, agencies should ensure that vendor invoices are properly defaced after processing, thus mitigating the risk that they will be paid twice.

Finding No. 17: Duplicate Payments – MFMP Issues

Proper IT controls include provisions for ensuring that the appropriate data is processed by the system only once. Our audit disclosed instances of duplicate payments as a result of MFMP file processing errors. Specifically:

- Due to an error during a test of the disaster recovery plan on April 28, 2006, 25 invoice reconciliations that had been previously processed by MFMP and sent to FLAIR for payment were reprocessed in the disaster recovery test environment but inadvertently passed to the FLAIR production environment. FLAIR processed these transactions normally, resulting in 18 duplicate warrants totaling \$8,433 and 3 duplicate electronic funds transfer (EFT) payments totaling \$455, all relating to the Agency for Health Care Administration (AHCA) vendors. In response to our audit inquiries, DMS staff indicated that all 18 warrants were intercepted by AHCA and canceled prior to being sent and that the 3 EFTs had subsequently been recovered.
- MFMP receives an error file from FLAIR listing transactions that were not successfully processed. Due to a file naming error during MFMP processing, the file was inadvertently reprocessed resulting in two duplicate warrants totaling \$5,824 and one duplicate EFT payment of \$12,600 being issued between April 26, 2006, and April 28, 2006. In response to our audit inquiries, DMS staff indicated that the two duplicate warrants were intercepted prior to being sent and that the EFT had subsequently been recovered. DMS staff additionally indicated that Accenture had revised its procedures to prevent this error from recurring in the future.

Recommendation: DMS should analyze the aforementioned instances to ensure that appropriate controls are in place to preclude file processing errors affecting the integrity of MFMP data transfers to FLAIR.

Finding No. 18: Other Data Integrity Issues

Data integrity relates to the accuracy and completeness of information as well as its validity in accordance with business values and expectations. We noted the following issues with data integrity in MFMP, in addition to the matters discussed in Finding Nos. 16, 17, and 19:

- As also noted in audit report No. 2006-015, when a transaction was recorded in MFMP, the system only captured the vendor number for that transaction. For recorded transactions, MFMP provided additional vendor information associated with the vendor number such as the vendor name and address. To provide this information, MFMP looked up the vendor number associated with the transaction in the Supplier and SupplierLocation database objects. As a result, MFMP provided the current information for the vendor associated with the vendor number. If any of the vendor information associated with the vendor number in the Supplier and SupplierLocation database objects had changed subsequent to the entry of the transaction, the correct historical vendor information would not be provided for that transaction.
- Two instances were noted where the MFMP invoice reconciliation approval history inaccurately reported an individual as having performed the DFS auditor function when in reality that person was not a DFS employee and did not perform that function.

- As also noted in audit report No. 2006-015, when a transaction was entered into MFMP, the appropriate accounting information (such as fund, function, and object code) was entered along with the transaction. This accounting data was used to facilitate the automatic routing of the transaction to FLAIR to be processed for payment once all of the required approvals in MFMP were recorded. The user could subsequently edit this accounting information directly in FLAIR with a Transaction 58 (Disbursement Correction). The information from a Transaction 58 was not passed from FLAIR back to MFMP. In addition, after making the change in FLAIR, the user could not go back into MFMP and manually update the transaction to reflect the change because the system did not allow changes to transactions in paid status.
- MFMP provided selected reports for agencies to manage their usage of MFMP. Our testing noted MFMP transactions that did not appear on the appropriate MFMP report. In response to our audit inquiries, DMS staff indicated that this was due to issues with the query that was developed to generate the report and that they were in the process of resolving the issue.
- The purchase order start date and end date fields in an MFMP on-line requisition form are 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.

Data integrity problems increase the risk of errors in user decision making that could impact business operations.

Recommendation: DMS should take action regarding the above-described issues to ensure that MFMP data is consistent and accurate both within the system and when shared with external systems.

Finding No. 19: MFMP and FLAIR Reconciliation

Proper data management includes procedures to assure that data is appropriately reconciled and routinely balanced to relevant control totals. As also noted in audit report No. 2006-015, neither MFMP nor FLAIR had the capability to support reconciliations of the two systems. DMS had not performed a manual or automated reconciliation since implementation.

Additionally, our audit field work at 14 State agencies disclosed that reconciliations of MFMP and FLAIR data were not being performed. In response to our audit inquiries, DFS staff provided that, while it appears the original intent of DMS was to require all agencies to process all payments for MFMP transactions through MFMP, system functionality and performance issues compelled State agencies to request that DFS allow agencies to pay transactions directly in FLAIR. DFS agreed and modified FLAIR to allow users to pay transactions encumbered in MFMP directly in FLAIR. Subsequently, MFMP was modified to allow for update of MFMP for payments made in FLAIR, and CFO Memorandum No. 03 (2003-04) was released.

CFO Memorandum No. 03, dated December 1, 2003, addresses payments processed through MFMP, setting forth the procedures and documentation requirements for disbursement requests made through MFMP. The memorandum also provides that agencies processing encumbered transactions through MFMP and the corresponding disbursement through FLAIR must individually reconcile the transactions by entering FLAIR payment data into MFMP for the applicable transactions.

Whereas this process of reconciling MFMP and FLAIR transactions is on a transaction basis only, our audit disclosed that there were no reliable reports available to facilitate agencies' reconciliation of MFMP and FLAIR data. Reconciliations of the data within these two systems is necessary to identify and correct any changes, cancellations, or errors in the transaction data that may have occurred in one but not both of the systems and provides assurance to stakeholders and decision makers as to the completeness and reliability of the data.

Our audit disclosed that, to facilitate the reconciliation of MFMP and FLAIR, a design document was created on July 28, 2005, that described the required information and steps in the process needed to reconcile MFMP payment records to FLAIR payment records. As of August 31, 2006, DMS staff indicated that the MFMP project team, in concert with DFS, was testing an overall MFMP and FLAIR reconciliation process as well as developing agency-level reconciliation reports; however, the implementation date had not been finalized.

When proper reconciliations are not performed, the risk is increased that data within the system and between external systems will not be accurate and synchronized. Given the instances described in this report that could create discrepancies within MFMP and differences between MFMP and FLAIR, proper reconciliations are necessary to timely detect data problems, as they occur.

Recommendation: DMS should continue collaborating with DFS to provide the means to reconcile MFMP with FLAIR and the future replacement accounting system, Aspire. Further, when the reconciliation capability is implemented, DMS should initiate training for designated agency personnel and disseminate detailed instructions for performing the reconciliations.

Finding No. 20: Statistical Sampling

Section 17.04, Florida Statutes, provides that the Chief Financial Officer, using generally accepted auditing procedures for testing or sampling, shall examine, audit, adjust, and settle the accounts of all the officers of this State. MFMP contains a Statistical Sampling Module that was used by DFS to perform a preaudit of payments in accordance with its statutory responsibilities.

Our review of the Statistical Sampling Module in MFMP noted the following issues:

- According to the design specifications for invoice sampling, DFS was to provide MFMP with operating level organization (OLO) and site codes, the number of invoices predicted for the upcoming year, the number of invoices to be sampled, and the OLO/site code combinations that required all invoices to be sampled. Our testing indicated that OLO 790000, site code 00, did not have the random number files reset with new parameters requested by DFS. The request was communicated between DFS and MFMP on February 6, 2006, for a March 1, 2006, reset, but the random number file was not reset until April 6, 2006, 36 days later than the requested date. As a result, 367 transactions of \$1,000 or less that would have been subject to sampling under the new DFS parameters were not subject to selection and preaudit.
- A list of random numbers was generated in MFMP based on the sampling information provided by DFS. These random numbers were compared to the incremental numbers assigned to each invoice subject to sampling and the item was selected if they matched. As also noted in audit report No. 2006-015, some of the random number files contained a zero. Our current audit noted 17 sites for which the random number file contained a zero. The random number zero could not be selected due to the number accumulator only assigning values of one and greater. This resulted in the amount of invoices being sampled being one less than what was expected by DFS for the 17 sites. In a response to our audit inquiries, DMS staff stated that they had corrected the program on April 27, 2006, to prevent zeros from being included in the future.

The issues listed above could potentially result in a failure of the Statistical Sampling Module to perform as expected, thereby affecting the validity of DFS's sampling process.

Recommendation: Going forward, DMS should ensure the statistical sampling process adheres to the design specifications for invoice sampling and DFS instructions.

Finding No. 21: Disaster Recovery Risk Assessments

The contract between Accenture and DMS indicates that a disaster recovery plan for MFMP will include a determination of the general nature and potential range of adverse events, so the plan adequately addresses the risks. As also noted in audit report No. 2006-015, this risk assessment had not been documented as of the date of our current audit field work testing. Subsequently, Accenture submitted an updated disaster recovery plan to DMS on March 17, 2006, that included a risk assessment. Our review of the risk assessment noted that it did not document the methodology used to determine risks nor did it quantify the risks that were identified. The lack of a sufficiently detailed risk assessment increases the risk that management may overlook or fail to fully prepare for all pertinent risks.

On June 13, 2006, Accenture submitted another revised disaster recovery plan to DMS. DMS subsequently approved the plan on July 5, 2006.

Recommendation: DMS should ensure that the disaster recovery risk assessment contains sufficient information to function as intended.

Finding No. 22: MFMP Back-up

Proper policies and procedures for the back-up of program and data files ensure that regular data back-ups are made and verified, and specify the frequency of back-ups, the location of stored data, file naming conventions, media rotation frequency, and methods for transporting data off-site. Good back-up practices also include the use of off-site storage facilities that are geographically removed from the primary site.

The contract between DMS and Accenture states that the service provider's server(s) must be backed up onto tape using a back-up system. Weekly full back-ups and daily incremental back-ups must be performed for production systems. Back-ups are to be taken from the hosting or other designated tape back-up facility and stored off-site.

We noted the following deficiencies in the back-ups performed for MFMP:

- As also noted in audit report No. 2006-015, only weekly back-ups were cycled off-site. If data needed to be recovered by using the off-site back-up tapes, the data could be up to one week old. Neither DMS nor Accenture had created a formal plan addressing the issue of how a potential week-old data loss from MFMP would be restored or reconciled with FLAIR data.
- Our testing of back-ups revealed that a weekly back-up in September 2005 was skipped. Consequently, when combined with the issue noted above, had data needed recovery during this period, the restored data would have been between one and two weeks old.
- The hosting facility that housed MFMP and the off-site storage facility were located within approximately 30 miles of each other in South Florida and could both be susceptible to the same effects of a natural disaster. The MFMP back-up site that was to be used in the event of a disaster at the hosting facility was located in Tallahassee. In the event of a natural disaster in South Florida, the back-up tapes would have to be transported from within the disaster area to Tallahassee prior to the restoration of MFMP.

As a result, there is significant risk that, in the event of a system failure or other event causing a loss of stored data, sufficient back-ups would not be available to timely and completely restore the lost information.

Recommendation: DMS should ensure that off-site back-ups are available to allow for a complete and timely recovery in the event of a system loss. Additionally, DMS should consider relocating the off-site storage facility to a location more geographically removed from the hosting facility.

Finding No. 23: Environmental Controls

The contract between Accenture and DMS requires that the Service Provider's server(s) must be protected by an industry standard fire suppression system in accordance with the local fire codes. Environmental controls such as fire detection and suppression systems prevent or mitigate potential damage to facilities and interruptions in service.

The MFMP development environment, located in Tallahassee, was also the back-up site to be used in the event of a disaster at the hosting facility. There were no fire detection or suppression systems in place at the Tallahassee location. The lack of a fire detection and suppression system increases the risk of loss due to fire.

Recommendation: DMS should require Accenture to implement a fire detection and suppression solution at the Tallahassee location pursuant to the contract.

Follow-up to Management Response

In his response, DMS's Secretary stated that the referenced contract clause is within a larger set of service level requirements for the MFMP production environment and since the Tallahassee project site does not house the production environment, these requirements are not relevant to that site. However, Section 2 of Attachment D of the contract between DMS and Accenture defines the infrastructure as including, not only the production facility, but also the alternate geographically separated data management facility for development, test, and data recovery purposes. Accordingly, the fire suppression system requirements are relevant to the disaster recovery facility.

OTHER MATTERS

Functional Acceptance

In audit report No. 2006-015, we noted that DMS had not functionally accepted the MFMP system even though it had been in operation since March 24, 2003, for vendor registration and since July 1, 2003, for agency purchasing. As additionally noted, the operations plan, which described the plans, policies, procedures, processes, and tracking tools for selected business functions such as security administration, systems development, and customer service desk, had not been formally approved by DMS.

On July 22, 2005, DMS provided us with two letters, both dated June 8, 2005, in which DMS functionally accepted MFMP and approved the operations plan. As a part of this audit, we reviewed DMS's basis for accepting these deliverables.

Based on our review, we concluded that the supporting documentation provided by DMS established a reasonable basis for its acceptance of MFMP. We additionally noted that on March 23, 2006, an updated operations plan was accepted by DMS, which incorporated selected recommendations from audit report No. 2006-015.

Project Staffing

DMS had contracted with the North Highland Company (North Highland) to provide technical expertise regarding Ariba Systems and to provide third-party project monitoring functions that DMS was unable to replicate internally. The original terms of this contract included services through July 2008, but during the 2006 Legislative session, the appropriation for the North Highland contract was reduced. As a result, DMS amended the North Highland contract to conclude in August 2006. In response to our audit inquiries, DMS staff indicated that they were in the process of exploring options to create a position to internally carry out the functions that were being handled by North Highland.

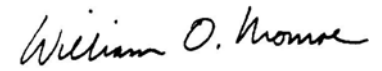
In audit report No. 2006-015, we noted that DMS had five full-time employees assigned to the MFMP project. Three of those employees have since left the project and five new employees were added to the project. As of the end of our audit field work, DMS had seven full-time employees assigned to the MFMP project. In response to our audit inquiries, DMS staff stated that the two additional positions added to the project were for business processes and that they still did not have adequate IT expertise and resources for the project.

PRIOR AUDIT FINDINGS

Finding Nos. 1, 3, 9 through 14, and 18 through 22, noted above, included issues repeated from our prior audit, report No. 2006-015. Other IT deficiencies noted in the prior audit, which were within the scope of this audit, have been corrected or were in the process of being corrected.

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 information technology audit.



William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSES

In letters dated December 12, 2006, through December 22, 2006, the heads of the applicable agencies provided responses to our preliminary and tentative findings. These letters are included in their entirety as Appendix C.

APPENDIX LIST

Appendix A MFMP Utilization Survey Summary

Appendix B MFMP Agency Liaison Survey Results

Appendix C Management Responses:

- Department of Management Services
- Department of Children and Family Services
- Department of Corrections
- Department of Education
- Department of Financial Services
- Department of Health
- Department of Highway Safety and Motor Vehicles
- Department of Law Enforcement
- Department of Revenue
- Department of State
- Department of Transportation
- Department of Veterans' Affairs
- Executive Office of the Governor
- Fish and Wildlife Conservation Commission

Appendix A
MFMP Utilization Survey Summary
As of April 30, 2006

In order to gain an understanding of the MFMP functions that State agencies were utilizing, we asked the 14 agencies included in our audit to identify on a listing of MFMP functions whether they used each function, used each function with a workaround, or did not use the function, as of April 30, 2006. Below is a summation of agency responses. Agencies reported numerous reasons for not utilizing some functions, as described in Finding No. 2 in this report.

MFMP UTILIZED TO:	YES	Y/W	NO	NA	DNR	Total
<i>Create requisitions</i>	86%	7%	0%	0%	7%	100%
<i>Establish encumbrances for direct orders</i>	71%	21%	7%	0%	0%	100%
<i>Authorize payments on direct orders</i>	71%	29%	0%	0%	0%	100%
<i>Initiate master agreements</i>	43%	0%	50%	0%	7%	100%
<i>Establish encumbrances for master agreements</i>	7%	7%	79%	7%	0%	100%
<i>Authorize payments on master agreements</i>	29%	7%	57%	7%	0%	100%
<i>Initiate construction contracts and authorize payments</i>	29%	0%	64%	7%	0%	100%
<i>Establish encumbrances for purchasing card transactions</i>	7%	0%	93%	0%	0%	100%
<i>Initiate/record approvals for purchasing card transactions</i>	7%	0%	93%	0%	0%	100%
<i>Manage encumbrances</i>	21%	14%	64%	0%	0%	100%
<i>Assist with year-end reporting of:</i>						
<i>Encumbrances</i>	36%	0%	64%	0%	0%	100%
<i>Accounts payables</i>	29%	0%	71%	0%	0%	100%
<i>Certified forwards</i>	29%	0%	71%	0%	0%	100%
<i>Track compliance issues</i>	0%	0%	79%	7%	14%	100%
<i>Report to oversight entities:</i>						
<i>EOG Office of Policy and Budget</i>	14%	0%	79%	7%	0%	100%
<i>Department of Management Services</i>	14%	0%	79%	7%	0%	100%
<i>Department of Financial Services</i>	21%	0%	71%	7%	0%	100%
<i>Search for and select vendors</i>	86%	0%	14%	0%	0%	100%
<i>Store and retrieve procurement documents</i>	79%	14%	7%	0%	0%	100%
<i>Report spend for developing budget requests</i>	7%	0%	93%	0%	0%	100%

LEGEND:

YES - Agency uses MFMP to accomplish this task.
 Y/W - Agency uses work-arounds with MFMP to accomplish task.
 NO - Agency does not use MFMP to accomplish this task.
 N/A - Agency does not perform this task with any regularity.
 DNR - Agency did not respond to this task.

Appendix B
MFMP Agency Liaison Survey Results
November 2004 and March 2006

In an effort to understand certain MFMP usage patterns and determine the level of user satisfaction with MFMP, we conducted a survey of 28 agency liaisons of agencies that had implemented MFMP. The survey was electronically sent to the agency liaisons on March 1, 2006. All 28 agency liaisons responded. Certain questions in this survey were previously asked in a similar survey of 27 agency liaisons on November 16, 2004. For these questions, both sets of responses are presented for comparison purposes. Not all questions were answered by all respondents; therefore, results may not total to 28 (for the March 2006 survey) or 27 (for the November 2004 survey). Our tabulation of the responses to the survey questions follows:

1. Question 1 asked for identification information from the person completing the survey.
2. Please rate your level of agreement or disagreement with the following statement: MFMP meets our information needs.

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Strongly Agree	0	0.0%	0	0.0%
Agree	8	30.8%	8	28.6%
Neutral	10	38.5%	6	21.4%
Disagree	8	30.8%	13	46.4%
Strongly Disagree	0	0.0%	1	3.6%

3. If you answered Question 2 as Disagree or Strongly Disagree, please elaborate on your reasons.

March 2006 – We received 15 comments. Respondents indicated numerous areas where MFMP lacked functionality or the included functionality did not work properly. Agencies also found reporting to be inadequate and remarked that the information in the system was not adequate or accurate and did not always correlate with FLAIR. Additionally, agencies indicated that the system was not paperless, required too many work-arounds, was fragmented, and caused workload issues. Finally, agencies indicated that there was a lack of consistent and reliable answers from the Help Desk.

4. What advantages did the implementation of MFMP bring to your agency?

March 2006 – We received 28 comments. Some agencies indicated that advantages included reduced processing time, better visibility, automation of processes, and paperwork reduction. Other agencies indicated that they did not see any advantages from MFMP and have had an increase in workload and longer turn-around times as a result of MFMP.

5. During a typical month, has your Agency experienced the inability to communicate (i.e., downtime) with MFMP, and if so, how frequently?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes, Once or More per Day	1	3.7%	0	0.0%
Yes, 2 to 4 Times per Week	1	3.7%	7	25.0%
Yes, Once per Week	0	0.0%	0	0.0%
Yes, Once per Two Weeks	0	0.0%	3	10.7%
Yes, Once per Month	7	25.9%	6	21.4%
No Downtime (Skip ahead to Question 7)	11	40.7%	8	28.6%
Don't Know (Skip ahead to Question 7)	7	25.9%	4	14.3%

6. If you answered yes to question 5, what is the typical length of the downtime?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
0 - 10 minutes	0	0.0%	3	18.8%
Over 10 minutes to 1 hour	4	44.4%	8	50.0%
Over 1 hour to 4 hours	3	33.3%	4	25.0%
Over 4 hours to 8 hours	1	11.1%	1	6.3%
> 1 business day	NA	NA	NA	NA
> 3 business days	NA	NA	NA	NA
> 5 business days	NA	NA	NA	NA

7. During a typical month, has your Agency experienced transaction response time greater than 6 seconds, and if so, how often?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes, Once or More per Day	11	42.3%	18	66.7%
Yes, 2 to 4 Times per Week	7	26.9%	4	14.8%
Yes, Once per Week	0	0.0%	0	0.0%
Yes, Once per Two Weeks	1	3.8%	2	7.4%
Yes, Once per Month	1	3.8%	2	7.4%
No transaction response greater than 6 seconds	0	0.0%	1	3.7%
Don't Know	6	23.1%	0	0.0%

8. During a typical month, has your Agency experienced system time-outs (system stops attempting a function you have submitted and makes you re-attempt) during a work session with MFMP, and if so, how frequently?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes, Once or More per Day	3	11.1%	7	25.0%
Yes, 2 to 4 Times per Week	5	18.5%	9	32.1%
Yes, Once per Week	4	14.8%	4	14.3%
Yes, Once per Two Weeks	0	0.0%	1	3.6%
Yes, Once per Month	3	11.1%	2	7.1%
No Timeouts	4	14.8%	4	14.3%
Don't Know	8	29.6%	1	3.6%

9. Does your Agency consider MFMP to be “user friendly”, that is, easy for staff to learn and use?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	11	40.7%	9	32.1%
No	11	40.7%	17	60.7%
No Opinion	5	18.5%	2	7.1%

10. If you answered Question 9 as No, please elaborate on your reasons.

March 2006 – We received 19 comments. Agencies indicated that the system was complex for the occasional user while being cumbersome and time consuming for the frequent user. Many processes were difficult as they were not intuitive, involved too many steps and screens, required too much scrolling, and the system had inconsistent page layouts. Agencies also reported that expected functionality was not in place, that they had difficulty with the interface to FLAIR, that there were too many work-arounds, and that the system was slow. Finally, agencies reported that training was inadequate, that there was no mechanism to get immediate help, and that help desk answers were incomplete and vague. One agency indicated the need for a user reference manual similar to what existed for SPURS.

11. Do you verify the accuracy of data entered into MFMP, and if you do, what procedures do you follow?
Answer 'Yes' or 'No' for each item.

11-1. I review periodic update reports from MFMP.

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	11	47.8%	17	73.9%
No	12	52.2%	6	26.1%

11-2. I perform routine spot checks of data.

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	19	79.2%	20	80.0%
No	5	20.8%	5	20.0%

11-3. I compare the data with other internally generated data.

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	11	44.0%	17	70.8%
No	14	56.0%	7	29.2%

11-4. I perform other procedures to verify the accuracy of the data.

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	15	62.5%	17	70.8%
No	9	37.5%	7	29.2%

11-5. I do not verify the accuracy of the data.

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	1	5.0%	2	10.5%
No	19	95.0%	17	89.5%

12. How would you rate the accuracy of the data in MFMP?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Excellent	1	3.7%	0	0.0%
Very Good	5	18.5%	5	17.9%
Good	8	29.6%	8	28.6%
Fair	2	7.4%	10	35.7%
Poor	1	3.7%	1	3.6%
No Basis to Judge	10	37.0%	4	14.3%

13. If you believe that there is inaccurate data in MFMP, please describe the areas of inaccurate data.

March 2006 – We received 20 comments. These focused on both data within MFMP as well as problems with matching data in MFMP to external systems such as FLAIR and SPURView.

November 2004 - We received 16 comments. These focused on accounting data and included comments that the analysis and data tools are insufficient.

14. If you answered question 13, what are the effects (if any) of the inaccurate data?

March 2006 – We received 19 comments. Agencies indicated that there was a poor audit trail and that reports and system searches were inaccurate, resulting in duplicate work and increased time since they could not rely on the data. Agencies also expressed audit concerns and concerns that management decisions could be based on inaccurate data. Agencies indicated that there was a possibility of duplicate payments and that transactions would fail FLAIR integration. Finally, an agency indicated that they “(w)onder what else is wrong if the basics don’t work and hasn’t been fixed as yet.”

November 2004 - We received 14 comments. Comments included concerns regarding duplicate invoices and payments, increased workload, items being shipped to the wrong location, and inaccurate financial reporting.

15. Does MFMP cause incorrect payments or other data that must be corrected?

	March 2006	
	Count	Percentage
Strongly Agree	3	11.1%
Agree	10	37.0%
Neutral	10	37.0%
Disagree	4	14.8%
Strongly Disagree	0	0.0%

16. If so, please describe the circumstances?

March 2006 – We received 18 comments. Agencies indicated difficulties in correcting or updating encumbrances and other accounting information and reported problems with double encumbrances and duplicate payments.

17. Describe any risks as related to incorrect payments even if incorrect payments have been adjusted.

March 2006 – We received 19 comments. Many agencies indicated the risk of duplicate payments as well as increased interest payments. One agency also reiterated the resulting lost time and duplication of efforts.

18. In general, how would you rate the overall quality of assistance your Agency has received from the MFMP Project staff?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Excellent	2	7.7%	0	0.0%
Very Good	9	34.6%	5	17.9%
Good	9	34.6%	11	39.3%
Fair	6	23.1%	9	32.1%
Poor	0	0.0%	3	10.7%
N/A, Never asked for or received assistance from the MFMP Project staff	0	0.0%	0	0.0%

19. In general, how would you rate the overall quality of assistance your Agency has received from the MFMP Help Desk?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Excellent	0	0.0%	0	0.0%
Very Good	3	11.5%	2	7.1%
Good	6	23.1%	5	17.9%
Fair	9	34.6%	16	57.1%
Poor	6	23.1%	5	17.9%
N/A, Never asked for or received assistance from the MFMP Help Desk	2	7.7%	0	0.0%

20. Do you believe the following about DMS's response to user reported problems?

20-1. DMS's response to user reported problems is adequate:

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	10	38.5%	9	32.1%
No	9	34.6%	15	53.6%
No Opinion	7	26.9%	4	14.3%

20-2. DMS's response to user reported problems is timely:

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	10	40.0%	11	39.3%
No	9	36.0%	13	46.4%
No Opinion	6	24.0%	4	14.3%

21. How would you rate any MFMP policies and procedures provided to your staff?

	November 2004		March 2006	
	Count	Percent	Count	Percentage
Excellent	0	0.0%	0	0.0%
Very Good	2	7.7%	1	3.6%
Good	6	23.1%	6	21.4%
Fair	7	26.9%	5	17.9%
Poor	0	0.0%	4	14.3%
No policies or procedures were provided	11	42.3%	12	42.9%

22. Does your staff have problems with MFMP supporting their daily tasks?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	14	53.8%	19	67.9%
No (Skip ahead to Question 28)	7	26.9%	8	28.6%
Don't Know (Skip ahead to Question 28)	5	19.2%	1	3.6%

23. Please describe the types of problems.

March 2006 – We received 19 comments. Comments included complaints about system response time, problems with FLAIR integration, the need for too many work-arounds, problems with system searches, contract management, approval flows, and file size limitations for attachments. Comments also reflected that agencies felt the system was overly complicated and inefficient.

November 2004 - We received 15 comments. Comments included complaints regarding the helpfulness of the help desk, a lack of applicability of training to actual work, system issues causing increased workload at the agency level, and system performance issues.

24. Do you feel these problems have resulted from the following:

24-1. Quantity of Training

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	5	31.3%	7	41.2%
No	11	68.8%	10	58.8%

24-2. Quality of Training

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	6	37.5%	7	41.2%
No	10	62.5%	10	58.8%

24-3. Timeliness of Training

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	6	37.5%	7	41.2%
No	10	62.5%	10	58.8%

24-4. Applicability of Training to Required Work Tasks

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	10	62.5%	9	52.9%
No	6	37.5%	8	47.1%

24-5. Communication Issues

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	10	62.5%	12	70.6%
No	6	37.5%	5	29.4%

24-6. Design of System

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	16	94.1%	16	84.2%
No	1	5.9%	3	15.8%

24-7. Hardware/Network Configurations

	November 2004		March 2006	
Question	Count	Percentage	Count	Percentage
Yes	6	46.2%	8	50.0%
No	7	53.8%	8	50.0%

24-8. Hardware/Network Capacity

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	7	50.0%	11	64.7%
No	7	50.0%	6	35.3%

24-9. Other (Please describe in question 25)

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	4	66.7%	2	28.6%
No	2	33.3%	5	71.4%

25. If you answered question 24 as Other reasons, please specify the reasons here.

March 2006 – We received 7 comments. Comments included a variety of reasons, including system slowness, lack of training, and problems with system design and FLAIR integration. An agency also commented that the system was very complicated and after 2 years none of their staff would claim to be experts.

November 2004 - We received 7 comments. Respondents expressed concerns that their business processes were not considered during system design, that many issues in the system were not addressed prior to go-live, and that MFMP was designed as a one size fits all system requiring agencies to develop workarounds. Additionally, an agency expressed concerns regarding MFMP implementation and design staff's lack of experience with government procurement and accounting.

26. Has your staff had to work overtime as a result of these problems?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	7	36.8%	11	57.9%
No (Skip ahead to Question 28)	12	63.2%	8	42.1%

27. During a typical month, how many hours of overtime has your Agency worked as a result of these problems?

March 2006 – We received 11 comments. Agency estimates of resulting overtime ranged as high as 200 hours during a typical month. An agency commented that no overtime is involved because most participants are selected exempt and their extra hours are not paid overtime.

November 2004 - We received 15 comments. Agency estimates of resulting overtime ranged as high as 100 hours during a typical month. An agency commented that no overtime is involved because most participants are selected exempt and their extra hours are not paid overtime.

28. Has your staff had to create internal processes outside of MFMP for the procurement or payment process to address MFMP functionality?

	March 2006	
	Count	Percentage
Yes	21	75.0%
No (Skip ahead to Question 30)	7	25.0%

29. If so, please describe.

March 2006 – We received 21 comments. Responses indicated that processes outside of MFMP had been created to handle items such as credits, auditing, warrant envelopes, receiving, manual payments, purchases containing the addresses of law enforcement officers, P-card purchases, non-registered vendors, journal transfers, subpoenaed records, leases, contracts, conferences, information technology review processes, two-party contracts, after-the-fact transactions, manual encumbrances, reconciliations to FLAIR, emergency purchases, and accounting.

30. Is your agency making use of any shadow systems (in-house system that is not the official system, but is used internally for certain functions) containing the some of the same information as MFMP?

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	10	38.5%	13	48.1%
No (Skip ahead to Question 33)	16	61.5%	14	51.9%

31. To what do you attribute the need for dual systems? Answer 'Yes' or 'No' for each item.

31-1. Availability of Reports

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	7	70.0%	11	84.6%
No	3	30.0%	2	15.4%

31-2. Ease of Data Entry

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	8	80.0%	10	83.3%
No	2	20.0%	2	16.7%

31-3. Need to capture additional data elements

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	9	90.0%	12	85.7%
No	1	10.0%	2	14.3%

31-4. Integration with financial tracking

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	8	88.9%	10	83.3%
No	1	11.1%	2	16.7%

31-5. Federal Reporting

	March 2006	
	Count	Percentage
Yes	2	18.2%
No	9	81.8%

31-6. Other reason (Please specify in question 32)

	November 2004		March 2006	
	Count	Percentage	Count	Percentage
Yes	5	71.4%	4	57.1%
No	2	28.6%	3	42.9%

32. If you answered question 31 as Other reasons, please specify the other reason(s) you need the shadow systems.

March 2006 – We received 5 comments. The comments indicated the need to interface with other systems and the lack of certain functionality in MFMP.

November 2004 - We received 9 comments. Comments included the following:

- Items procured outside of MFMP due to exemptions or reluctant vendors must be obtained or housed by other systems.
- Users found it easier to use the Pcard system.
- There are certain procurement related functions that MFMP does not handle or does not handle well. These include performance monitoring, contract management, and deliverable tracking.
- There has been difficulty in obtaining data downloads and useful reports from MFMP.
- Users have experienced training issues and feel that MFMP is not user friendly and does not meet their unique needs.

33. Does your agency receive security reports from MFMP?

	March 2006	
	Count	Percentage
Yes	6	21.4%
No (Skip ahead to Question 36)	22	78.6%

34. What types of information is contained in these reports (if possible, please include the report name)?

March 2006 – We received 8 comments. These comments indicated a variety of reports the agencies used for assessing MFMP security.

35. Does your agency feel that the provided security reports provide adequate information to allow you to properly monitor your employees and assure that adequate controls such as segregation of duties are in place?

	March 2006	
	Count	Percentage
Yes	6	66.7%
No	3	33.3%

36. Does MFMP provide the necessary functionality to allow your agency to establish the necessary procedures and controls to ensure proper authorization, documentation, recording, and compliance of procurement and payment transactions? Answer 'Yes' or 'No' for each item.

36-1. Authorization

	March 2006	
	Count	Percentage
Yes	23	82.1%
No	5	17.9%

36-2. Documentation

	March 2006	
	Count	Percentage
Yes	20	71.4%
No	8	28.6%

36-3. Recording

	March 2006	
	Count	Percentage
Yes	22	81.5%
No	5	18.5%

36-4. Compliance

	March 2006	
	Count	Percentage
Yes	19	70.4%
No	8	29.6%

37. If you answered any part of the previous question as 'No', what, if any, compensating control do you have in place outside of MFMP?

March 2006 – We received 14 comments. Agencies indicated a variety of compensating controls, including retention of all documentation in hard copy form and use of external reports and procedures.

38. Has MFMP caused your agency to have issues with prompt payment compliance?

	March 2006	
	Count	Percentage
Yes	17	60.7%
No (Skip ahead to Question 40)	11	39.3%

39. Please describe the nature of the prompt payment issues your agency has experienced.

March 2006 – We received 19 comments. Agencies indicated that prompt payment issues were caused by a variety of issues, including problems with approval processes and program deficiencies. Responses indicated that MFMP reported incorrect dates, causing them to appear as overdue for prompt payment purposes. Multiple agencies indicated that they made payments outside of MFMP to avoid prompt payment issues.

40. In regard to your responses to questions 22/27 (problems with MFMP supporting daily tasks) and questions 30/32 (shadow systems), have you requested modifications or enhancements be made to MFMP to rectify the problems or preclude the future need for shadow systems?

	March 2006	
	Count	Percentage
Yes	14	53.8%
No (Skip ahead to Question 42)	12	46.2%

41. If such requests have been made, have MFMP staff indicated whether they would be considered for enhancements?

	March 2006	
	Count	Percentage
Yes	7	43.8%
No	9	56.3%

42. Regarding modifications and enhancements that have been requested for the system, do you feel that MFMP staff... (Answer 'Yes' or 'No' for each item)

42-1. Are dealing with the issues in a timely manner?

	March 2006	
	Count	Percentage
Yes	6	24.0%
No	19	76.0%

42-2. Are correctly prioritizing the issues?

	March 2006	
	Count	Percentage
Yes	6	26.1%
No	17	73.9%

43. Regarding the MFMP Analysis Tool, does your agency find the tool to be... (Answer 'Yes' or 'No' for each item)

43-1. Useful?

	March 2006	
	Count	Percentage
Yes	10	40.0%
No	15	60.0%

43-2. Accurate?

	March 2006	
	Count	Percentage
Yes	9	39.1%
No	14	60.9%

43-3. User Friendly?

	March 2006	
	Count	Percentage
Yes	2	8.0%
No	23	92.0%

44. Where do you currently store the documents that are not stored in MFMP but are needed to support the transactions that flow through MFMP? How are these documents referenced within MFMP?

March 2006 – We received 28 comments. Agencies indicated a variety of methods for storing these documents. Some maintained hard copies while others imaged the documents. One agency commented that they kept hard copies because they lacked scanners. Electronic documents were stored on shared drives or in shadow systems. Some agencies referenced the locations of these documents from within MFMP while others did not.

45. Does your agency currently have procedures to redact nonpublic information from documents electronically stored in MFMP pursuant to DMS Scanning and File Attachment Guidelines dated 10/7/2005?

	March 2006	
	Count	Percentage
Yes	10	37.0%
No	17	63.0%

46. To what extent does your agency stop the workflow on procurements initiated in MFMP and record the expense directly in FLAIR?

	March 2006	
	Count	Percentage
Never	3	11.5%
Rarely	0	0.0%
Several times a month, 1% to 5% of monthly MFMP procurements	7	26.9%
Frequently, > 5% of monthly MFMP procurements	NA	NA

47. If so, please describe how your agency identifies the status of such items in MFMP and how applicable encumbrances are recorded and reduced.

March 2006 – We received 18 comments. The agencies provided a variety of responses, including that they couldn't identify the status or that they used FLAIR, a manual process, or shadow systems.

48. Does your agency use MFMP to record blanket encumbrances for P-Card expenditures?

	March 2006	
	Count	Percentage
Yes	3	10.7%
No	25	89.3%

49. If so, please describe how your agency identifies the status of such items in MFMP and how applicable encumbrances are recorded and reduced.

March 2006 – We received 3 comments. Respondents indicated that they did not or could not identify the status, or that they used a manual process to do so.

50. Does your agency have a policy requiring that similar items requisitioned within the same time period be combined for competitive procurement?

	March 2006	
	Count	Percentage
Yes	20	71.4%
No	8	28.6%

51. Does your agency have a policy requiring the coordination and monitoring of procurements made through separate procurement processes, i.e., MFMP, P-Card, FLAIR?

	March 2006	
	Count	Percentage
Yes	19	67.9%
No	9	32.1%

52. If you have any additional comments related to MFMP, please enter them in the space provided.

March 2006 – We received 11 comments. These comments generally reiterated the comments made throughout the survey.

November 2004 - We received 21 comments. These comments reflected other concerns that were not directly addressed in the survey. Some responses expressed a satisfaction with the system. Others expressed concerns that prompt payment compliance may have dropped. Others noted that the commodity codes (class/group) agencies are using to identify commodities/services being purchased are outdated and lack the specificity of newer standard code systems. Agencies indicated that this was brought to the attention of DMS and Accenture during the conference room pilots. Another concern was that the Purchase Order to Invoice Flip functionality that was indicated as a primary feature is not being used for the most part due to a lack of vendor participation. Another comment indicated that there was too strong of a push by DMS to go-live on the system and indicated that they should have worked through all issues with the pilot agencies rather than relying on agencies to identify issues after they had implemented.

**Appendix C
Management Responses**



DEPARTMENT OF MANAGEMENT
SERVICES

"We serve those who
serve Florida"

JEB BUSH
Governor

Tom Lewis, Jr.
Secretary



Office of the
Inspector General
4050 Esplanade Way
Tallahassee, Florida
32399-0950

Telephone:
850-488-5285

Fax:
850-921-3066

Internet:
www.MyFlorida.com

December 22, 2006

Mr. William O. Monroe, CPA
Auditor General
Office of the Auditor General
Claude Denson Pepper Building
111 West Madison Street
Tallahassee, Florida 32301

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, following is the Department of Management Services (DMS) response to your preliminary and tentative audit report, *Department of Management Services and Other Selected State Agencies, MyFloridaMarketPlace System, Information Technology Audit*. The attached response corresponds with the order of your preliminary and tentative audit findings and recommendations.

As noted in your report, agencies continue to use manual processes, workarounds and alternative systems for many of the business functions offered by MFMP. As recently as June 2006, changes to the Florida Accounting Information Resource (FLAIR) System allowed agencies to manage encumbrances established in MFMP directly in FLAIR, thereby circumventing MFMP financial controls. By using alternatives, agencies have diminished the benefits of MFMP financial controls, visibility into enterprise-wide spend, and accountability and have impeded our ability to reconcile MFMP and FLAIR, as noted in previous audits. We have been working with agencies to try and eliminate this and plan to meet with the new CFO to request that she reconsider allowing agencies to manage encumbrances outside of MFMP.

DMS agrees that all agencies should be using all functionality elements of MFMP. Likewise, we understand and respect that many real and perceived challenges, including system performance, resistance to change and system training, contribute to agencies not using the system as required by law. To continue to encourage and expand agency use of MFMP, DMS remains committed to ensuring that MFMP is responsive to the needs of our agency customers. We have made measurable progress in improving system performance in the past year. DMS has proactively engaged and has been working closely with our agency customers, including those who are not using the system, to evaluate their use, needs, and challenges related to the system. DMS and Accenture have used that input to cooperatively develop a comprehensive Quality Improvement Plan that proactively addresses all facets of MFMP including Procurement Business Process Improvement, Invoicing

Mr. William O. Monroe
December 22, 2006
Page 2

Business Process Improvement, System Performance Management, Reporting, Sourcing Improvement, Agency Productivity Measurement Program and Customer Service Focus.

It is important to remember that MFMP is still a very new system and like any new system, it is evolving. We see improvements in performance, greater engagement of users, and expanded training particularly in the area of security. The steady increase in the overall acceptance of the system by its users is evidenced by the continued increase in transactional volume generated by the system. For example, the overall number of purchase orders issued in fiscal year 2006 was almost double that generated in fiscal year 2005. And the MFMP system is currently on pace to issue five percent more purchase orders in fiscal year 2007 as compared to fiscal year 2006. We know we still have much to do and are confident that with implementation of our new Quality Improvement Plan, anticipated software upgrade (Ariba 8.2) in spring 2007 and the intended integration into Aspire, MFMP will continue on its path of quality improvement.

The Auditor General, OPPAGA and others audit entities help DMS do a better job. Your audits are important and provide valuable information and insight into our programs. However, DMS and the MFMP Project Team, in particular, have been in a constant state of audit for the last three years. I realize it takes substantial staff and time to conduct an audit. It takes equal, if not more staff and time, for us to properly prepare for the audit, assist during the audit and respond to your findings. With our limited staff, each minute spent focusing on audit preparation and response takes away from valuable time that could be spent improving system security, performance, accountability and user satisfaction.

Despite the competing demands on their time, our MFMP Project Team has successfully implemented the majority of prior audit recommendations while maintaining day-to-day operation of a Statewide procure to pay system used by over 30 State of Florida Agencies. For example, the MFMP Project Team supports a system that has generated over 71,000 purchase orders for State Purchasing professionals for \$600 million dollars of goods and services in Fiscal year 2007 alone. To date, the MFMP system has issued over 340,000 purchase orders for \$2.8 billion dollars. Finance and administration professionals have already processed 85,000 invoices in fiscal year 2007, totaling over 400,000 invoices processed for \$1.8 billion dollars in payments to State of Florida vendors since the project began. Finally, the Customer Service Desk has handled over 175,000 customer inquires from the roughly 13,000 users and 80,000 suppliers that comprise the system.

To allow us to focus our limited resources on making MFMP better, we sincerely appreciate your consideration in scheduling your next follow-up after the upgrade has been fully implemented and agencies have concluded their year-end processing.

If further information is needed concerning our response, please contact Steve Rumph, Inspector General, at 488-5285.

Mr. William O. Monroe
December 22, 2006
Page 3

Sincerely,

A handwritten signature in black ink, appearing to read "Tom Lewis, Jr.", followed by a long horizontal line extending to the right.

Tom Lewis, Jr.
Secretary

Attachment

cc: Colleen Englert, Chief of Staff, Department of Management Services
Ken Granger, Deputy Secretary, Department of Management Services
Josh Yaffin, MFMP Project Manager, Department of Management Services

Mr. William O. Monroe
December 22, 2006
Attachment Page 1

Finding No. 1: System Performance

Proper management of system performance is an important aspect of IT service delivery. We observed, and MFMP users reported, instances of MFMP system performance problems throughout the audit period. DMS has taken steps to address system performance, but we continued to note aspects of DMS's management of system performance that needed improvement.

Recommendation 1:

DMS should continue with efforts to resolve system performance issues. DMS should also ensure that periodic load and stress testing is performed and that verifiable performance metrics are maintained.

Response:

Concur: Next to security, improving system performance and customer satisfaction is our highest priority. On August 10, 2006, DMS and Accenture cooperatively implemented a new, comprehensive performance management strategy, which involves a proactive approach to load testing of the system and an ongoing capacity planning effort that includes agency input. It also addresses the set of metrics that best indicate degradation in end user experience with the application so that trends can be analyzed and issues proactively identified and remediated before the impact becomes significant. In addition, DMS is independently verifying the performance metric number 6 - System Response Time, from March 2006 forward. This process will be completed by March 2007.

Finding No. 2: Policies, Procedures, and Systems Documentation

Our audit field work at the 14 State agencies disclosed that few agencies were fully utilizing all the functional capabilities available in MFMP. Agencies gave various reasons for not using certain MFMP functions and some agencies relied on workarounds or alternate systems in lieu of MFMP functionality

Recommendation 2a and 2b:

- a. In addition to resolving the performance problems, as discussed in Finding No. 1, DMS should continue to communicate and work with State agencies to increase user awareness and expertise regarding MFMP functionality.
- b. Furthermore, DMS should conduct a complete survey of all State agencies, subject to the Florida Financial Management Information System Act (Section 215.90 through 215.96, Florida Statutes), to identify the MFMP functionality used by each and, for the functions not employed, explanations as to why MFMP is not being used. This information should be provided to the Financial Management Information Board for its use in ensuring that the Florida Financial Management Information System operates efficiently as an

Mr. William O. Monroe
December 22, 2006
Attachment Page 2

integrated financial management information system and provides accurate and complete financial information necessary to the effective operation of State government.

Response:

- a. **Concur:** Over the last 12 months, DMS has proactively engaged its agency customers to evaluate their use, needs and challenges related to the system and increase user awareness, understanding and use of the system. DMS is committed to continuing this effort. Plans are already underway to fulfill this commitments over the next 12 months include:
- agency process evaluation sessions for both purchasing and Finance and Accounting staff;
 - agency refresher training on system functionality;
 - overall process review for enterprise business processes;
 - improvement initiatives for key areas of the system including catalogs, eQuote, master agreements and electronic invoicing; and
 - the implementation of an overall agency scorecard that will help identify best practices among agencies in order to improve the enterprise utilization of MFMP as a tool for purchasing and invoice processing.

In April 2006, DMS established a Change Review Board (CRB) comprised of representatives from 13 different agencies. This board has thus far been an excellent forum for ensuring awareness and input from our user agencies. For example, as a part of the upgrade to Ariba 8.2 the Project Team is working closely with the CRB to incorporate five significant functional enhancements. The enhancements were evaluated, prioritized, and the designs reviewed by CRB members. These enhancements address major agency productivity areas including approval workflows, end of year processing, payment processing and correcting procurement receiving issues. We are proud of our progress in involving our customers in bringing continued increases in quality to MFMP. Their experience and input will continue to receive major focus from DMS as the 2007 Quality Improvement Plan is executed.

- b. **Concur:** DMS agree it is essential to survey our customers on a regular basis. The MFMP team conducts an annual customer satisfaction survey to gauge user satisfaction with the MFMP system. This annual survey is distributed to 200 of our frequent users across all agencies. It provides helpful feedback to the project team in addressing concerns with the system. In addition, over the past six months, DMS has met with user agencies, individually and collectively and at every level from Agency Secretaries, Purchasing Directors, Finance and Accounting Directors to general users, to gain a more thorough understanding of their current use, needs and challenges related to the system. DMS has used that input to develop a Technical Performance Management Plan and a more comprehensive 2007 MFMP Quality Improvement Plan that proactively address all facets of MFMP including Procurement Business Process Improvement, Invoicing Business Process Improvement, System Performance Management, Reporting, Sourcing

Mr. William O. Monroe
December 22, 2006
Attachment Page 3

Improvement, Agency Productivity Measurement Program and Customer Service Focus. In order to gauge the effectiveness of the plan, DMS has also established a tailored survey that will baseline user feedback on all areas addressed in the Improvement Plan. That survey was distributed on December 12th to a broad set of our frequent users, including more than 1,600 individuals across all agencies. DMS will reissue the survey every six months to measure progress against the baseline. While the previous annual surveys referenced above have provided valuable insight, this survey will be more indicative of user satisfaction and project improvement, since it is more comprehensive, addresses specific customer feedback issues and covers a larger sample of the user population than previous surveys, including the survey conducted by the Auditor General.

Finding No. 3 Monitoring of Transaction

Florida law and administrative rules provide that DMS may collect fees from vendors for the use of MFMP. While transactions may be exempt for a number of reasons, agency transactions involving commodities and contractual services are generally assessed a one-percent transaction fee, which the vendor shall pay to the State. We noted that improvements were needed in DMS's review and follow-up process for the appropriateness of the application of transaction fees and exemptions.

Recommendation 3:

DMS should enhance its monitoring of exemptions to the one-percent transaction fee to include a thorough and documented review of exemptions to provide further assurance that exemptions are appropriately applied and fees appropriately assessed for past and future transactions. DMS should also determine whether other findings in this report, for example Findings Nos. 2, 15, 16, 17, and 19, have any potential impact on the one-percent transaction fee.

Response:

Concur: Due to the mass correction of the Vendor Registration Verification Process, instituted by the MFMP project team, verification of the one percent transaction fee was temporarily suspended. DMS is resuming the Transaction Fee Exemption verification. Furthermore, the associated procedures for the Verification Process will be developed by February 2007.

At your suggestion, DMS will evaluate findings nos. 2,15,16,17, and 19, to determine whether any of these findings have any potential impact on the one-percent transaction fee. We are sure you realize that these findings reference the MFMP system itself, the support of that system by DMS and Accenture, and agencies' use of the system. The one-percent transaction fee is applied irrespective of MFMP system usage. The fee is applied to all state agency purchases except for those explicitly exempted by Rule 60A-1.032, Florida Administrative Code. The fee is also applied to all purchases made off of the State Term Contracts by entities other than state agencies, including local governments, public universities etc. As such, system usage or

Mr. William O. Monroe
December 22, 2006
Attachment Page 4

function and agency processes do not directly dictate the application of the one-percent transaction fee.

Finding No. 4: Risk Assessments

IT risk assessment is a process of identifying and evaluating information risks that are relevant to the achievement of entity business objectives. The MFMP project team had not been tracking project risks as described in the approved Risk Management Process for MFMP.

Recommendation 4:

Consistent with the approved Risk Management Process, DMS should ensure that risks relevant to the successful operation of MFMP, and the business objectives dependent thereon, are regularly identified and assessed. DMS should use the risk assessment information to identify cost-effective risk reduction solutions, and monitor and report on the progress of risk reduction actions.

Response:

Concur: DMS is ensuring that risks relevant to the successful, secure operation of MFMP are regularly identified and assessed. In June 2006, MFMP Project Management resumed the approved Risk Management Process. The project management team meets at least monthly to identify and remove risks, evaluate current probability and impact of each risk, and monitor and report on the progress of risk reduction actions identified. The project management team uses the RISC (Risks, Issues, System Investigation Requests - SIRs, and Change Request) application as the vehicle to document the results of this process. On an annual basis, we will evaluate our risk management process to confirm its effectiveness.

Finding No. 5 through 10: Security of Data and IT Resources

IT security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that the management of MFMP security continued to need improvement in the areas of conducting background checks of Accenture personnel; controlling access at the application system, operating system, and database levels; ensuring the appropriateness of project staff and user access privileges; providing comprehensive security policies and procedures; and other specific areas not disclosed in detail in this report to avoid jeopardizing MFMP security.

Recommendation No. 5:

DMS should obtain and review documentation of the performance and results of all background checks performed for contractor employees.

Mr. William O. Monroe
December 22, 2006
Attachment Page 5

Response:

Concur: Accenture conducts background checks for all employees at the beginning of their tenure with Accenture. Furthermore, any Accenture agreements with DMS approved subcontractors also require background checks to be completed for all employees staffed on the MFMP project. Accenture project management will provide DMS with documentation confirming the completion of background checks for all current project team members by January 31, 2007 and will continue to provide this confirmation for any new team members through the quarterly access review process. DMS Office of Inspector General will review and maintain confirmation documentation provided by Accenture on all current and new project team members. In addition, DMS Office of Inspector General will conduct random reviews of the background documentation on at least an annual basis.

Recommendation No. 6:

DMS should strengthen MFMP logical access controls to reduce the risk of compromise to MFMP information.

Response:

Concur: As noted in the AG report, a change request was implemented in May 2006 to force users to change their password upon initial log-in to the MFMP application and are automatically prompted to change their password every 45 days. For Accenture employees, the inherent security at the database and operating system levels do not require such a change. Accenture employees are required, by procedure, to change their password on initial log-on. The Accenture user ids and passwords are limited to technical project team personnel and the risk of unauthorized access given the process controls, isolated system access, and infrequency of new user ids being established is minimal.

Recommendation No. 7:

DMS should periodically analyze the functions of MFMP project staff to ensure that access privileges are appropriate and commensurate with individuals' job duties. In addition, DMS should ensure that MFMP access for terminated, transferred, or reassigned Accenture personnel is removed in a timely manner. Additionally, database administrators should immediately cease the sharing of user IDs and each designated individual should be assigned a unique user ID with a corresponding password.

Response:

Concur: Beginning in July 2006, the project management team began a quarterly access review process to review Accenture user access reports generated by MFMP. Quarterly, the team reviews Accenture and MFMP project staff user accounts to verify access privileges are appropriate. The team also conducts quarterly reviews to determine that terminated, transferred,

Mr. William O. Monroe
December 22, 2006
Attachment Page 6

or reassigned personnel are removed from the system. In addition, the database administrators that were sharing a user ID will be assigned unique user IDs by January 31, 2007.

Recommendation No. 8:

Agencies should periodically analyze the functions of their employees to ensure that MFMP user access privileges are appropriate and commensurate with users' job duties. Additionally, agencies should immediately cease the sharing of user IDs or passwords and assign each designated system user a unique user ID with a corresponding password. Further, agencies should regularly review the weekly Buyer Adoption Report and immediately remove any user accounts deemed no longer appropriate.

Response:

Concur: We agree that agencies should periodically analyze the functions of their employees to ensure that MFMP user access privileges are appropriate and commensurate with users' job duties. Regarding DMS, in November our Security Administrator began running and reviewing the Buyer Adoption report weekly. The Security Administrator will also begin meeting in December 2006, with each Division within the Department to review MFMP user access privileges. This process should be completed by the end of January 2007 and will be done annually.

Recommendation No. 9:

DMS should ensure that its newly implemented security administration policies and procedures are followed. Additionally, in future system development projects of this nature, DMS should establish relevant policies and procedures more timely upon system implementation.

Response:

Concur: DMS has provided agencies with the security administration policies and has held training with the agency system administrators. The project team will continue to provide yearly system administrator training sessions so agencies are reminded of the security policies and procedures that need to be followed when administering application access for MFMP Users. As for Accenture access to the system, as mentioned in response to Finding No. 7, the project staff is now reviewing staff access on a quarterly basis. In addition, DMS will annually request a certification, signed by a senior agency executive, verifying that security administration policies and procedures are being followed.

Additionally, if DMS has another major system implementation, we will establish security policies and procedures more timely.

Mr. William O. Monroe
December 22, 2006
Attachment Page 7

Recommendation No. 10:

DMS should improve the deficient security control features and enhance the safeguarding of DMS IT resources.

Response:

Concur: DMS will implement the appropriate security controls for MFMP system in regards to this confidential finding. The MFMP upgrade 2.0 estimated to be release in April 2007 will identify specific dates for implementation as appropriate.

Finding Nos. 11 and 12: Application Systems Change Management

Effective management of application system changes helps ensure that the ongoing integrity of a system is preserved over time as the system is changed. Our audit disclosed instances where neither DMS nor end-user approval of system changes and operational data updates (data changes made by Accenture on behalf of users) had been obtained prior to the changes becoming operational. We also noted instances where the MFMP design specifications had not been updated to reflect system changes or contained inaccuracies.

Recommendation No. 11:

DMS should ensure that the program change process incorporates adequate user involvement and written approval for all system enhancements and changes.

Response:

Concur: The MFMP application maintenance process calls for end user involvement for significant changes to the system. Users are asked to provide input and review design specifications, participate in testing of coded modifications before implementation, and submit a satisfaction survey post implementation. This process is now being coordinated with the MFMP Change Review Board. In July 2006, the project team began a more structured sign-off process before migrating code changes to the production environment. The approval process requires Accenture to submit all supporting documentation supporting testing and the Change Review Board and DMS' project management must sign-off on all changes prior to migrating the change to the production system.

Recommendation No. 12:

In addition to maintaining a historical copy of the original design documents, DMS should maintain updated versions of the documents to serve as documentation of the current state of the system.

Mr. William O. Monroe
December 22, 2006
Attachment Page 8

Response:

Concur: As noted in the report, the project team maintains a crosswalk to tie system documentation for enhancements and ongoing changes to the original design documentation. Operationally, the project team has found that this approach provides the application maintenance team with a clear and concise method of representing changes to MFMP functionality over time. If particular misstatements are identified in previous MFMP design documentation, they can be overridden by subsequent design documents that are recorded in the overall system documentation crosswalk. The system documentation crosswalks for the reported identified designs, DLFD002 and FLDD072, will be updated by March 31, 2007.

Finding Nos. 13, 14, 17, 18 and 19: Data Management

Effective data management controls help ensure the integrity of information stored within a system. We continued to note deficiencies in the management of electronic documents within MFMP that serve as attachments to procurement records. Additionally, DMS had not established maintenance procedures to ensure the ongoing retention and usability of electronic records pursuant to Department of State Rules. We also noted instances of duplicate payments initiated from MFMP and processed by FLAIR for payment. We noted other data integrity issues within MFMP and we continued to find data inconsistencies between MFMP and FLAIR. Further, DMS had not established a mechanism for reconciling MFMP and FLAIR transaction data.

Recommendation No. 13:

DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to assure that the rule is being followed. Also, DMS should ensure that all confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Response:

Concur: Effective October 15, 2006, rule 60A-1.033 – MyFloridaMarketPlace Information Security and Electronic Attachments - was promulgated as part of the Florida Administrative Code. The rule outlines procedures and guidelines to purge confidential information from the system. It should also be noted that two change requests were implemented in May and July 2006 to further encourage agencies to follow the MFMP Attachment and Scanning Guidelines. These changes entail additional text throughout the application reminding users that no confidential information should be included in the application, and requiring that users check a checkbox before adding an attachment to the system to confirm that any confidential information that may have been contained in that specific attachment has been removed.

Mr. William O. Monroe
December 22, 2006
Attachment Page 9

As noted in the Auditor General's report, DMS implemented an audit process to monitor and control inappropriate data. This process began in December 2006. Furthermore, in June 2006, DMS distributed a model security policy to user agencies.

Recommendation No. 14:

DMS should implement procedures to ensure compliance with Department of State Rule 1B-26.003, Florida Administrative Code.

Response:

Concur: The project management team will evaluate the Department of State Rule and will request guidance from both the Department of State and Auditor General to determine the appropriate policies and procedures for MFMP. This should be completed no later than September 15, 2007.

Recommendation No. 17:

DMS should analyze the aforementioned instances to ensure that appropriate controls are in place to preclude file processing errors affecting the integrity of MFMP data transfers to FLAIR.

Response:

Concur: To prevent a reoccurrence of the file processing errors affecting the integrity of MFMP data transfers to FLAIR, the operational procedures and documentation along with the Disaster Recovery Plan were updated in June 2006.

Recommendation No. 18:

DMS should take action regarding the described issues to ensure that MFMP data is consistent and accurate both within the system and when shared with external systems.

Noted issues follow:

- a. *As also noted in audit report No. 2006-015, when a transaction was recorded in MFMP, the system only captured the vendor number for that transaction. For recorded transactions, MFMP provided additional vendor information associated with the vendor number such as the vendor name and address. To provide this information, MFMP looked up the vendor number associated with the transaction in the Supplier and SupplierLocation database objects. As a result, MFMP provided the current information for the vendor associated with the vendor number. If any of the vendor information associated with the vendor number in the Supplier and SupplierLocation database objects had changed subsequent to the entry of the transaction, the correct historical vendor information would not be provided for that transaction.*

Mr. William O. Monroe
December 22, 2006
Attachment Page 10

- b. *Two instances were noted where the MFMP invoice reconciliation approval history inaccurately reported an individual as having performed the DFS auditor function when in reality that person was not a DFS employee and did not perform that function.*
- c. *As also noted in audit report No. 2006-015, when a transaction was entered into MFMP, the appropriate accounting information (such as fund, function, and object code) was entered along with the transaction. This accounting data was used to facilitate the automatic routing of the transaction to FLAIR to be processed for payment once all of the required approval in MFMP were recorded. The user could subsequently edit this accounting information directly in FLAIR with a Transaction 58 (Disbursement Correction). The information from a Transaction 58 was not passed from FLAIR back to MFMP. In addition, after making the change in FLAIR, the user could not go back into MFMP and manually update the transaction to reflect the change because the system did not allow changes to transactions in paid status.*
- d. *MFMP provided selected reports for agencies to manage their usage of MFMP. Our testing noted MFMP transactions that did not appear on the appropriate MFMP report. In response to our audit inquiries, DMS staff indicated that this was due to issues with the query that was developed to generate the report and that they were in the process of resolving the issue.*
- e. *The purchase order start date and end date fields in an MFMP on-line requisition form are 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.*

Response:

Per your noted issues please find our response.

- a. As noted in the AG report, the system will show a vendor's current, up-to-date information as opposed to the historical vendor information for a given transaction. The core Ariba software supporting MFMP does not provide a mechanism to maintain and display the historical information. The MFMP team will submit a product enhancement request to the software provider Ariba, as this is not a reasonable change that Accenture can make to the Ariba software.
- b. These instances were recorded in SIR #393 as a system defect and was resolved in the production environment on August 31, 2006.
- c. As part of the interface design between MFMP and FLAIR, this transaction was not identified as one that should be interfaced back to MFMP for updates in the approved and implemented MFMP design. Therefore, if a user chooses to complete a Transaction 58 in FLAIR, this information is not automatically transferred back to MFMP.

Mr. William O. Monroe
December 22, 2006
Attachment Page 11

- d. The reporting data omission referenced was recorded as a customer incident (ticket number 232545) and impacted the *All Received Orders* and *All Open Orders* reports. The issue was resolved on June 29, 2006.
- e. The Department will submit a change request to Accenture for a correction to the PO start and end date fields.

Recommendation No. 19:

DMS should continue collaborating with DFS to provide the means to reconcile MFMP with FLAIR and the future replacement accounting system, Aspire. Further, when the reconciliation capability is implemented, DMS should initiate training for designated agency personnel and disseminate detailed instructions for performing the reconciliations.

Response:

Concur: As stated in the report, the MFMP project team, in concert with DFS, has designed and is currently testing an overall MFMP and FLAIR payment reconciliation process. The objective of this process is to confirm that payments made through FLAIR for MFMP-initiated transactions are properly recorded on the associated MFMP transaction. The team is targeting to have the payment reconciliation process operational by January 2007, but that schedule is dependent upon DFS resources that also have to support DFS operations and Aspire project activities. Furthermore, a similar reconciliation process will be built into the Aspire interface effort for eventual implementation. When the reconciliation process is operational, communication and training will be provided to the necessary Finance and Accounting personnel responsible for this function in the agencies. Further, this process will be added to the Finance and Accounting refresher training course available via the MFMP Toolkit, located on the MFMP website.

Finding No. 15: Agency Procedural Deficiencies

Effective procedures and guidelines are necessary to promote end-users' complete understanding and proper use of MFMP. Our audit field work at the 14 State agencies disclosed instances where written procedures or guidelines for key MFMP processes were lacking and where procedural deficiencies existed regarding the issuance of direct orders (purchase orders), invoice reconciliations (the process whereby invoices are compared to direct orders), and processing of payments.

Recommendation No 15:

To ensure that transactions are consistently and properly reviewed and processed, State agencies should establish written procedures and guidelines for key MFMP processes utilized. These written procedures should specifically:

Mr. William O. Monroe
December 22, 2006
Attachment Page 12

- Require that approved direct orders are obtained prior to the receipt of any goods or services.
- Enhance procedures to ensure that MFMP is appropriately updated for invoices paid directly in FLAIR.

Response:

Concur: We agree that State agencies should establish written procedures and guidelines for key MFMP processes. Regarding DMS, Section 5.1 of the Departmental Purchasing's Policies and Procedure manual, already directs that purchase orders will not be processed for goods or services that are acquired after-the-fact. In addition, Finance and Accounting will provide procedures for their staff on updating MFMP for invoices paid directly in FLAIR. These procedures are expected to be completed by January 15, 2007.

Finding No. 20: Statistical Sampling of Payments for Preauditing

MFMP's Statistical Sampling Module was used by DFS to perform a preaudit of payments. Improvements were needed in the operation of the sampling process to provide increased assurance of its validity.

Recommendation:

Going forward, DMS should ensure the statistical sampling process adheres to the design specifications for invoice sampling and DFS instructions.

Response:

Concur: The random number zero problem was corrected in the production environment in April 2006. In addition, the confusion regarding the routing and approval of the DFS request to reset the OLO 790000 site code 00, in February 2006 has been corrected. This was corrected by the project team working with DFS and subsequently refined and confirmed the approval process for OLO site code resets to include DMS approval and this change should avoid the delays noted in the report.

Finding Nos. 21 through 23: Continuity of Service

IT service continuity is protected through such measures as disaster recovery planning and appropriate provisions for making and safeguarding copies of software and data. Risk assessment elements within the MFMP disaster recovery plan needed enhancement. Additionally, improvements were needed in MFMP program and data back-up provisions and in environmental controls at the Tallahassee facility that housed the MFMP development environment and served as a back-up site to the primary hosting facility.

Mr. William O. Monroe
December 22, 2006
Attachment Page 13

Recommendation No. 21:

DMS should ensure that the disaster recovery risk assessment contains sufficient information to function as intended.

Response:

Concur: The Disaster Recovery Application Risk Analysis document provided to DMS, by Accenture, in June 2006 as a part of the revised Disaster Recovery Plan documents the risk associated with losing one or more of the components of the MFMP application in the event of a disaster. The document also provides the business process workaround to be utilized in the event that a component is lost that is not included in the scope of the Disaster Recovery Plan. The existence of the executable workarounds outlined provides the rationale used to determine which components of MFMP are covered in the Disaster Recovery Plan.

Recommendation No. 22a and 22b:

- a. DMS should ensure that off-site back-ups are available to allow for a complete and timely recovery in the event of a system loss.
- b. Additionally, DMS should consider relocating the off-site storage facility to a location more geographically removed from the hosting facility.

Response:

- a. **Concur:** The Department agrees that we should ensure that off-site back-ups are complete and available in the event of a system loss and currently have a monitoring program in place. The monitoring program was enhanced with the update to the Operations Plan in April 2006.
- b. **Concur:** While the Department believes the risk of the off-site storage facility is acceptable, based on the Auditor General's input we will again consider relocating the off-site storage facility to a location more geographically removed from the hosting facility.

Recommendation No. 23: Environmental Controls

DMS should require Accenture to implement a fire detection and suppression solution at the Tallahassee location pursuant to the contract.

Response:

Concur: The referenced contract clause, Attachment D Section 4.0 (g), is within a larger set of service level requirements for the MFMP production environment that is accessed by State of Florida users. Since the Tallahassee project site does not house the production environment, these requirements are not relevant to that site. Nonetheless, the Department and Accenture recently investigated the opportunity to move the MFMP production environment from Miami

Mr. William O. Monroe
December 22, 2006
Attachment Page 14

where it is protected by a fire detection and suppression system to the State's SRC in Tallahassee, in an effort to support the Department's initiative to further utilize the SRC for State of Florida production applications. Efforts to analyze this move identified the need to simultaneously move the disaster recovery site away from Tallahassee if the production site were to be moved to Tallahassee, in order to maintain appropriate geographic separation of the production and disaster recovery sites. Legislative funding was allocated in this year's budget to support such application environment moves. However, funding could not be obtained in time to move the MFMP environment before the testing phase of the in process upgrade effort began. As such, to minimize risk, the Department and Accenture agreed to reconsider this move at some point after July 2007.



State of Florida
Department of Children and Families

Jeb Bush
Governor

Lucy D. Hadi
Secretary

December 14, 2006

Mr. William Monroe
Auditor General
State of Florida
111 West Madison Street
G74 Claude Pepper Building
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

The Department of Children and Families (DCF) is in receipt of the preliminary and tentative findings and recommendations of the Auditor General's report for the period of July 1, 2005 through June 30, 2006. DCF has reviewed the report findings and recommendations of the Auditor General's audit, and would like to specifically address the following issues related to this agency.

Finding No. 2: Agency Utilization of MyFloridaMarketPlace (MFMP) Functions

At the present time, DCF has a need to continue the use of the Automated Requisition Tracking System (ARTS) due to the capability and ease to the users of the system, which is currently unavailable within the MFMP system. Within the ARTS System, requisitions may be moved from one requestor to another, which cannot be done in the MFMP system. Also, due to the simplicity of the ARTS system, less intense training is required for new users, which is a concern due to current turnover rates. For example, a district staff person who is a new, inexperienced user of ARTS, is able to conduct business through ARTS by simple coaching via phone if needed, however, with MFMP, hands on training will be required before a user is able to utilize the system, due to the complexity of the MFMP system.

To address the aforementioned issues, DCF staff participated in a conference call with MFMP staff in November, to discuss difficulties experienced with the use of MFMP. Since that time, DCF re-implemented the use of MFMP (beginning Nov. 13), for several districts and zones. MFMP staff have also agreed to conduct refresher training for users of the system, which will include training on the use of new enhancements within MFMP, intended to increase the speed of the system, as well as improve the overall functionality of the system to be one that is more user-friendly.

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: Protect the Vulnerable, Promote Strong and Economically Self-Sufficient Families, and Advance Personal and Family Recovery

Mr. William Monroe
December 14, 2006
Page Two

Finding No. 13 Management of Attachments- DCF has historically followed all state and federal laws referenced in the report under this finding, and will continue to do so. Additionally, the agency will adopt a written policy and procedure to specifically address confidential information issues within MFMP. A policy will be developed by January 31st, related to preserving confidential information within MFMP; which will be followed by the development and implementation of specific procedures, in accordance with the policy. We will also continue to perform monitoring activities of all information entered into the MFMP system, as well as provide on-going training to users of MFMP, to ensure confidentiality of all clients served by the agency.

Lastly, DCF would like to thank the Auditor General for their review and we look forward to the continued partnership with DMS, DFS, and other agencies, as we all strive to provide the best services to the citizens of our great State of Florida.

If you should have any further inquiries pertaining to the issues addressed in this response, please contact Mr. Thomas Towns, Purchasing Administrator, at (850) 487-1951.

Sincerely,



Lucy D. Hadi
Secretary



FLORIDA
DEPARTMENT of
CORRECTIONS

An Equal Opportunity Employer

2601 Blair Stone Road • Tallahassee, FL 32399-2500
Phone: (850) 488-7480

Governor
JEB BUSH

Secretary
JAMES R. McDONOUGH

<http://www.dc.state.fl.us>
Fax: (850) 922-2848

December 22, 2006

The Honorable William O. Monroe, CPA
Auditor General
Office of the Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

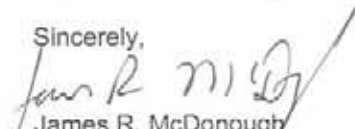
RE: Preliminary and Tentative Audit Findings, Audit of Department of Management Services and other Selected Agencies, MyFloridaMarketPlace System

Dear Mr. Monroe:

We have reviewed the preliminary and tentative findings and recommendations included with your letter dated November 20, 2006. As required by Section 11.45(4)(d), Florida Statutes, our response is attached. This response reflects the specific actions taken or contemplated to address Findings No. 2 and No. 13.

Thank you for your continued cooperation and presentation of recommendations for the improvement of our operations.

Sincerely,



James R. McDonough
Secretary

JRM/DM/dm

Attachment

cc: Laura E. Bedard, Ph.D., Deputy Secretary
Richard Prudom, Chief of Staff
Paul C. Decker, Inspector General
Millie Seay, Director of Administration
Donald L. Miller, Chief Internal Auditor

**FLORIDA DEPARTMENT OF CORRECTIONS
RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS
AUDIT OF DEPARTMENT OF MANAGEMENT SERVICES AND OTHER
SELECTED AGENCIES, MYFLORIDAMARKETPLACE SYSTEM**

Finding No. 2 Agency Utilization of MFMP Functions

The department utilizes most of the functionality available in MFMP but, for various reasons, do not use, or have ceased using, some of the functions of the system. Some of these reasons are:

- 1) E-quote – We have periodically reviewed this function and determined that it is not user friendly, the vendor can “cherry-pick”, but the buyer cannot split the award, the process is cumbersome and time consuming and it stifles competition. Many vendors have decided against participating in this function and several have withdrawn their support, making the vendor base very limited and restrictive.
- 2) Master Agreements – We do not enter formal contracts as Master Agreements (MA's) in MFMP because of the functional limitations of the system. One of the major concerns is the requirement for the Contract Manager to approve all invoices and the system only allows one Contract Manager, which is not feasible for an agency our size with the magnitude of invoices that we process. Some other concerns are that M.A.'s are not electronically submitted to the vendor; the “comments” field in the requisition does not transfer (print) onto the M.A.; if the M.A. is for a commodity, purchase orders must be issued against the M.A. in order for the products to be received in MFMP, which is duplicative and time consuming; and the correct “ship to” address does not print on the MA.
- 3) Sourcing – The sourcing tool has never been rolled out to the agencies.

For those procurements made through MFMP, the transactions are encumbered by procurement staff, with the exception of blanket or term purchase orders, which are encumbered by F&A staff, and payments are processed in MFMP unless problems are encountered that would jeopardize compliance with the prompt payment law, Chapter 215.422.

The department will continue to review these functions for consideration as improvements to the system are implemented.

Utilization of an Alternative In-House System: The department's Purchase Request System (PRS) was developed prior to MFMP implementation and the decision to maintain this shadow system was based on several factors, including but not limited to:

- 1) PRS is not internet-based and can contain specific confidential information that cannot be entered in MFMP and is visible and available internally to staff who may need this information.
- 2) Internet access within a prison setting is available in controlled settings only.
- 3) DMS instructed agencies to have a contingency plan for issuing PO's when MFMP is not available or cannot be used. Our PRS is used for this purpose, primarily for the creation and issuance of emergency purchase orders.
- 4) PRS contains additional data that is not duplicated in MFMP.
- 5) All information in PRS is entered into MFMP by procurement staff, in compliance with Section 215.93, Florida Statutes.
- 6) Use of PRS reduces the workload.
- 7) Because MFMP is cumbersome and time-consuming, the department chose not to roll out the requisitioning and approval functionality of the system to end users in the field, based on workload and training issues. System performance is slow, especially at year-end, and attempts to rectify this problem have failed. The number of MFMP users in our agency is less than 725. PRS has over 4500 users. Adding this vast amount of users to MFMP would, most likely, substantially affect the system performance for all agencies.

Finding No. 13 Management of Attachments

The department includes confidentiality requirements during initial training of the MFMP system to all new users. In addition, periodic reminders have been issued to MFMP users via e-mail. However, the department agrees with the audit recommendation and will develop a written procedure that specifically addresses confidential information issues within MFMP.

FLORIDA DEPARTMENT OF EDUCATION



John L. Winn
Commissioner of Education

STATE BOARD OF EDUCATION

T. WILLARD FAIR, *Chairman*

F. PHILIP HANDY, *Vice Chairman*

Members

DONNA G. CALLAWAY

ROBERTO MARTINEZ

PHOEBE RAULBERGSON

KATHLEEN SHANAHAN

LINDA K. TAYLOR

December 21, 2008



Mr. William O. Monroe
Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Attached is the Department's response to the preliminary and tentative findings from your Multi-Agency Audit of *MyFloridaMarketPlace System*.

If you have any questions, please contact John M. Franco, Inspector General, at 245-0403 or email john.franco@fldoe.org.

Sincerely,

A handwritten signature in cursive script, appearing to read "John L. Winn".

John L. Winn
Commissioner

JLW/jmf/br

Attachment

**Florida Department of Education
Auditor General
Preliminary and Tentative Findings Response
Multi-Agency MyFloridaMarketPlace
December 21, 2006**

Finding # 2, Agency Utilization of MFMP Functions. (DOE did not process encumbrances in MFMP.)

Auditor General Recommendation:

In addition to resolving the performance problems, as discussed in Finding No. 1, DMS should continue to communicate and work with State agencies to increase user awareness and expertise regarding MFMP functionality. We also recommend that State agencies reconsider their utilization of MFMP functionality and the necessity of maintaining alternative systems.

Department of Education Response:

As we informed audit staff prior to the release of the report, this issue was resolved September 1, 2006, when DOE implemented a procedure to encumber all MFMP transactions.

Finding #13, Management of Attachments

Auditor General Recommendation:

DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to assure that the rule is being followed. Also, DMS should ensure that all confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Department of Education Response

The Department of Education (DOE) was aware of the concern about confidential information contained in MFMP attachments and implemented all actions recommended by DMS to address this issue in a timely fashion. These recommendations did not include the development of written policies and procedures by each agency. During the course of this audit, DOE has requested and received guidance from DMS and has drafted a set of procedures. The procedures are undergoing review and will be finalized and implemented by January 31, 2007.



CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

TOM GALLAGHER

December 18, 2006

Mr. William O. Monroe
Auditor General
State of Florida
Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's preliminary report for the Information Technology Audit of Department of Management Services and Other Selected State Agencies MyFloridaMarketPlace System.

If you have any questions or would like to discuss the matter further, please contact David Harlan, Inspector General at (850) 413-4960.

Sincerely,

A handwritten signature in blue ink that reads "Tom Gallagher".

Tom Gallagher

TG:Hc

Enclosures

Florida Department of Financial Services
Audit Response
Department of Management Services
And Other Selected State Agencies
MyFloridaMarketPlace System
For the Period July 1, 2005 through June 30, 2006
And Selected Actions Taken Through September 14, 2006
Preliminary and Tentative Audit Findings

Finding No. 8: Management of User Access Privileges

Recommendation: Agencies should periodically analyze the functions of their employees to ensure that MFMP user access privileges are appropriate and commensurate with users' job duties. Additionally, agencies should immediately cease the sharing of user IDs or passwords and assign each designated system user a unique user ID with a corresponding password. Further, agencies should regularly review the weekly Buyer Adoption Report and immediately remove any user accounts deemed no longer appropriate.

Response: We concur. Employees have been assigned individual user IDs and passwords. Department policies and procedures reiterate that authorized users are responsible for the security of their passwords and accounts and that personal passwords should not be shared or disclosed.

Finding No. 13: Management of Attachments

Recommendation: DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to assure that the rule is being followed. Also, DMS should ensure that all confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Response: We concur. We have reminded all agency staff of this requirement and are in the process of revising Department policies and procedures.



Jeb Bush
Governor

M. Rony François, M.D., M.S.P.H., Ph.D.
Secretary

December 15, 2006

Mr. William O. Monroe, C.P.A.
Auditor General
Room G74, Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe:

This letter is in response to your November 20, 2006 correspondence regarding the preliminary and tentative findings of your report entitled, *Department of Management Services And Other Selected State Agencies MyFloridaMarketPlace System*. The agency's response and corrective action plans to your findings and recommendations may be found in the enclosed document.

We appreciate the work of your staff and will diligently pursue appropriate resolution to the findings.

If I may be of further assistance, please let me know.

Sincerely,

A handwritten signature in black ink, appearing to read "M. Rony François".

M. Rony François, M.D., M.S.P.H., Ph.D.
Secretary, Department of Health

MRF/kir
Enclosure

Department of Management Services and Other Select Agencies, MyFloridaMarketPlace System Information Technology Audit

Para. # Finding:	Recommendation:	Management Response:	Corrective Action Plan:
<p>13 Effective data management controls help ensure the integrity of information stored within a system. We continued to note deficiencies in the management of electronic documents within MFMP that serve as attachments to procurement records. Additionally, DMS had not established maintenance procedures to ensure the ongoing retention and usability of electronic records pursuant to Department of State Rules. We also noted instances of duplicate payments initiated from MFMP and processed by FLAIR for payment. We noted other data integrity issues within MFMP and we continued to find data inconsistencies between MFMP and FLAIR. Further, DMS had not established a mechanism for reconciling MFMP and FLAIR transaction data.</p>	<p>DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to assure that the rule is being followed. Also, DMS should ensure that all confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.</p>	<p>DOH has an existing written policy (revised 7/6/06) addressing confidential information within MFMP in its Purchasing Policies and Procedures Manual (COHP-250-9-06, Section VII.B.7-Confidentiality)</p>	<p>Completed.</p>

Para. # Finding:

Recommendation:

Management Response:

Corrective Action Plan:

15	<p>Effective procedures and guidelines are necessary to promote end-users' complete understanding and proper use of MFMP. Our audit field work at the 14 State agencies disclosed instances where written procedures or guidelines for key MFMP processes were lacking and where procedural deficiencies existed regarding the issuance of direct orders (purchase orders), invoice reconciliations (the process whereby invoices are compared to direct orders), and processing of payments.</p>	<p>To ensure that transactions are consistently and properly reviewed and processed, State agencies should establish written procedures and guidelines for key MFMP processes utilized. These written procedures should specifically:</p> <ul style="list-style-type: none"> -Require that approved direct orders are obtained prior to the receipt of any goods or services. -Enhance procedures to ensure that MFMP is appropriately updated for invoices paid directly in FLAIR. 	<p>DCH has an existing written policy (revised 7/6/06) addressing the procurement of goods and services within MFMP in our Purchasing Policies and Procedures Manual (DDMP 250-9-05, Section V B-Purchase Order/Direct Order).</p> <p>DCH will develop written policies that provide appropriate guidance with processing payments in MFMP and update MFMP records when DCH finds it necessary to process payments directly in FLAIR that were generated from MFMP Direct Orders and Master Agreements.</p>	<p>Develop written policies that provide appropriate guidance with processing payments in MFMP and maintaining payment history</p>
----	---	---	---	--

<i>Para. # Finding:</i>	<i>Recommendation:</i>	<i>Management Response:</i>	<i>Corrective Action Plan:</i>
<p>2. Our audit field work at the 14 State agencies disclosed that few agencies were fully utilizing all the functional capabilities available in MFMP. Agencies gave various reasons for not using certain MFMP functions and some agencies relied on workarounds or alternate systems in lieu of MFMP functionality.</p>	<p>In addition to resolving the performance problems, as discussed in Finding No. 1, DMS should continue to communicate and work with State agencies to increase user awareness and expertise regarding MFMP functionality. We also recommend that State agencies reconsider their utilization of MFMP functionality and the necessity of maintaining alternative systems.</p> <p>Furthermore, DMS should conduct a complete survey of all State agencies, subject to the Florida Financial Management Information System Act (Sections 215.90 through 215.96, Florida Statutes), to identify the MFMP functionality used by each and, for the functions not employed, explanations as to why MFMP is not being used. This information should be provided to the Financial Management Information Board for its use in ensuring that the Florida Financial Management Information System operates efficiently as an integrated financial management information system and provides accurate and complete financial information necessary to the effective operation of State government.</p>	<p>The Department of Health (DOH) has been and remains a strong advocate of streamlining processes and cutting costs while improving accuracy and timeliness through the utilization of automation with such systems as MFMP. As noted in the audit report, MFMP has experienced performance and functional deficiencies which in May 2005 prompted DOH to suspend processing payments through MFMP and revert back to using payment processing functionality in Department of Financial Services' state accounting system FLAIR. Since then, DOH has been working with DMS to provide end-user perspective on best ways to enhance MFMP. As a result, DOH has started the process of transitioning specific county health departments and program offices back to processing their payments through MFMP. As DOH experiences improvements in MFMP performance and functionality through its transitioning back to payment processing in MFMP and DMS's continuance to make DOH recommended enhancements to MFMP, DOH may then return to processing all payments through MFMP.</p>	<p>Transitioning back to payment processing through MFMP.</p>



State of Florida
DEPARTMENT OF
HIGHWAY SAFETY AND MOTOR VEHICLES

FRED O. DICKINSON
Executive Director

JEB BUSH
Governor

CHARLIE CRIST
Attorney General

TOM GALLAGHER
Chief Financial Officer

CHARLES H. BRONSON
Commissioner of Agriculture

December 20, 2006

Mr. William O. Monroe, CPA
Auditor General
State of Florida
111 West Madison Street
Tallahassee, Florida 32302-1735

Dear Mr. Monroe:

Enclosed is a copy of this agency's response to the preliminary and tentative audit findings regarding your operational audit of:

Department of Management Services
And Other Selected State Agencies
MyFloridaMarketPlace System
For the period July 1, 2005, Through June 30, 2006,
And Selected Actions Taken Through September 14, 2006.

The professionalism exhibited by your staff during this audit was evident and appreciated. If you should need additional information, please contact Mr. Laurence W. Noda, Inspector General, at 617-3104.

Sincerely,

Fred O. Dickinson
Executive Director

FOD/gc
Enclosure

Preliminary and Tentative Audit Findings
Department of Management Services
And Other Selected State Agencies
MyFloridaMarketPlace System
For the period July 1, 2005, Through June 30, 2006,
And Selected Actions Taken Through September 14, 2006.

Finding No. 13: Management of Attachments

Recommendation: DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to assure that the rule is being followed. Also, DMS should ensure that all confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Response:

DHSMV has established written policy and procedures for handling confidential information in the MFMP system. The information was distributed to all MFMP users in June 2006. One memorandum describes the confidential information policy, which was incorporated into the Department's purchasing manual. A second memorandum gives detailed instructions regarding required documentation needed for processing invoices.

Finding No. 16: Duplicate Payments – Agency Issues

Recommendation: To capitalize on MFMP system edit checks, State agencies should process payments for MFMP transactions through MFMP whenever possible. Agency procedures should require supervisory monitoring of payments made directly in FLAIR to ensure that the Invoice eForms and Payment Update eForms are completed and submitted and the "Payment completed in FLAIR" box is checked. Also, agencies should ensure that vendor invoices are properly defaced after processing, thus mitigating the risk that they will be paid twice.

Response:

Our current policy is to process all payments for MFMP transactions through MFMP when possible. However, if processing through MFMP is not possible and the invoice is to be paid in FLAIR, we use agency assignment of the voucher number, record it in the comments field, and check the "Payment completed in FLAIR" box. Additionally, we reconcile outstanding encumbrances and open orders in MFMP to ensure payments being made directly in FLAIR are properly recorded in MFMP. After our vouchers (which include the vendor invoice) are scanned for retention the original documentation is destroyed.



Florida Department of
Law Enforcement

Gerald M. Bailey
Commissioner

Post Office Box 1489
Tallahassee, Florida 32302-1489
(850)410-7001
www.fdle.state.fl.us

Jeb Bush, Governor
Charlie Crist, *Attorney General*
Tom Gallagher, *Chief Financial Officer*
Charles H. Bronson, *Commissioner of Agriculture*

December 18, 2006

Mr. William O. Monroe, CPA
Auditor General
G74 Claude Pepper Building
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

We have received the preliminary and tentative findings and recommendations from the following audit of:

**DEPARTMENT OF MANAGEMENT SERVICES
AND OTHER SELECTED STATE AGENCIES
MYFLORIDAMARKETPLACE SYSTEM
Information Technology Audit**

Your recommendations and our related explanation or our description of actual or proposed corrective actions initiated by the Florida Department of Law Enforcement (FDLE) are enumerated below:

FINDING #2: Except for three field offices, FDLE staff used e-mail for initiating and assigning purchase requisitions to Purchasing staff. Alternatively, requesters completed a hardcopy requisition form and submitted the form to the Purchasing staff for approval and entry of the information into MFMP.

RECOMMENDATION: In addition to resolving the performance problems, as discussed in Finding No. 1, DMS should continue to communicate and work with State agencies to increase user awareness and expertise regarding MFMP functionality. We also recommend that State agencies reconsider their utilization of MFMP functionality and the necessity of maintaining alternative systems.

FDLE Response: Currently, all FDLE Direct Orders are initiated by a requisition in MFMP. FDLE does not require a hardcopy requisition but uses an approval driven e-mail identifying requested items which is electronically forwarded to either Headquarters FDLE Central Purchasing Mail Box or to the assigned regional procurement staff. Once a regionally generated MFMP requisition is received by Headquarters FDLE Central Purchasing, it is electronically processed via MFMP and a subsequent Direct Order is issued. Once approval driven e-mails are received from Headquarters' members, FDLE Central Purchasing staff prepares a MFMP requisition and then issues the subsequent Direct Order. Regardless of the source of the MFMP requisition, FDLE Central Purchasing staff issues the Direct Order.

We met with DMS staff to discuss the MFMP encumbrance and invoice payment functional shortcomings. FDLE will continue to work closely with DMS to recommend improvements with MFMP functionality.

*Committed to
Service • Integrity • Respect • Quality*

Mr. William O. Monroe, CPA
December 18, 2006
Page Two

FINDING #8: At FDLE, purchasing staff used a common password to accommodate workload sharing. The sharing of a user ID or password limits the ability to assign responsibility for a transaction to an individual employee, thereby overriding a basic control of any IT system.

RECOMMENDATION: Agencies should periodically analyze the functions of their employees to ensure that MFMP user access privileges are appropriate and commensurate with users' job duties. Additionally, agencies should immediately cease the sharing of user IDs or passwords and assign each designated system user a unique user ID with a corresponding password. Further, agencies should regularly review the weekly Buyer Adoption Report and immediately remove any user accounts deemed no longer appropriate.

FDLE Response: Currently, all FDLE MFMP users are assigned an individual MFMP user ID and password. When FDLE began to utilize MFMP in February of 2005, a pilot group of FDLE members in FDLE Central Purchasing shared a common password - with individual user IDs - in order to document the receipt of services that were ordered by other FDLE members. As the pilot continued to roll out to the field offices, the pilot purchasing members continued this practice with the new users. This practice was discontinued in November of 2006.

FINDING #13: During our audit field work at the 14 State agencies, including DMS, we inquired whether each agency had developed policies and procedures that addressed preventing the introduction of confidential information into MFMP, monitoring documents stored as attachments into MFMP for confidential information, and redacting any confidential information so discovered. While some agencies described measures taken to address confidential information, none of the agencies provided written policies and procedures that specifically addressed confidential information issues within MFMP.

RECOMMENDATION: . . . Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

FDLE Response: On July 24, 2006 FDLE updated Policy 1.5 PURCHASING to read: "Confidential member information will not be entered into the MyFloridaMarketPlace purchasing system. Please refer to the Office of General Services, General Services Manual Section C, Subsection 4, MyFloridaMarketPlace Confidential Member Information for the detailed procedures and training plans."

The recommendations in your audit report are appreciated. If you require further information regarding the actual or proposed corrective actions, please contact me or Inspector General Al Dennis at 410-7225.

Sincerely,



Electra T. Bustle
Assistant Commissioner

ETB/ALD/dkk



JIM ZINGALE
EXECUTIVE DIRECTOR

DEPARTMENT OF REVENUE
TALLAHASSEE, FLORIDA 32399-0100

December 12, 2006

Mr. William O. Monroe, CPA
Auditor General
Office of the Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

As required by section 11.45(4)(d), Florida Statutes, attached is the Department's response to the preliminary and tentative findings and recommendations relating to Finding Nos. 2, 13 and 16 of your audit of the Department of Management Services And Other Selected State Agencies MyFloridaMarketPlace System For the Period July 1, 2005, Through June 30, 2006, And Selected Actions Taken Through September 14, 2006.

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact Sharon Doredant, Acting Inspector General, at 487-1037.

Sincerely,

A handwritten signature in black ink that reads "Jim Zingale".

Jim Zingale

JZ/bs0

Attachment

Department of Revenue
Response to Preliminary and Tentative Findings and Recommendations
MyFloridaMarketPlace System
For the period July 1, 2005, Through June 30, 2006,
And Selected Actions Taken Through September 14, 2006

Finding No. 2: Agency Utilization of MFMP Functions

Recommendation: In addition to resolving the performance problems, as discussed in Finding No. 1, DMS should continue to communicate and work with State agencies to increase user awareness and expertise regarding MFMP functionality. We also recommend that State agencies reconsider their utilization of MFMP functionality and the necessity of maintaining alternative systems.

Response: The Department of Revenue began a full implementation of MFMP in November 2004 and attempted to utilize all available system functionality. In addition to the cited system performance problems, we discovered that basic functionalities such as encumbering, receiving, and payment processing did not work effectively even with attempted work-arounds in order to stay on the system. Our decision to return to FLAIR for payment processing was prompted by our inability to maintain compliance with the prompt payment law (s. 215.422, F.S.) using MFMP. We then decided to use only the MFMP functionalities that provided an operational benefit to DOR. We continue to use the requisitioning and purchase order (direct order) generation features of MFMP.

Although we recognize that some improvements have been made to MFMP since we discontinued usage of some of its functionalities, we are hesitant to expand our current use of the system again until we are confident that MFMP will provide a comprehensive and effective procurement system solution. We will continue to work with DMS and our sister agencies to that end.

Finding No. 13: Management of Attachments

Recommendation: Agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Response: The Florida Department of Revenue has an extensive and comprehensive Information Security Policy that meets the confidential information requirements of sections 119.071(4)(d)1. and 119.071(5)(a)3., Florida Statutes. Due to the broad reaching nature of our regulatory duties, all DOR employees are required to read and acknowledge their understanding of this policy and their adherence to it, inclusive of MFMP issues. Section V.D. of the DOR Information Security Policy (#DOR-SEC-004) states that employees are not authorized to grant access to use any information resource or computer without specific permission. Section VI.A.4. of the policy requires that all confidential or sensitive information be accessible only to persons who are authorized by the owner on the basis of his/her duties.

In addition to our standard policy on confidentiality, our MFMP Security Administrator released a bulletin on April 10, 2006, and again on December 1, 2006, reminding all MFMP users of this

requirement. Each requisition that is created at the Department of Revenue is monitored for confidential information by the Purchasing Office. Requisitions that are found to contain confidential or sensitive information are declined and sent back to the creator for correction or the information is redacted in the Purchasing Office.

Finding No. 16: Duplicate Payments

Recommendation: To capitalize on MFMP system edits, State agencies should process payments for MFMP transactions through MFMP whenever possible. Agency procedures should require supervisory monitoring of payments made directly in FLAIR to ensure that the Invoice eForms and Payment Update eForms are completed and submitted and the "Payment completed in FLAIR" box is checked.

Response: The three cited duplicate payments have been fully recovered. We concur with the auditor's finding that having the capability to process payments either as a MFMP transaction or directly through FLAIR increases the risk that an invoice may be paid twice, without detection. Our decision to process non-electronic payments exclusively through FLAIR (see DOR response to Recommendation No. 2) not only allows us to remain in compliance with the State's prompt payment law but also ensures a more effective payment process by eliminating this risk. An added benefit of using one payment system is that the need to reconcile two overlapping systems is eliminated as well. Although the FLAIR payment controls that we currently use for detecting duplicate payments are mostly manual processes, we believe that they are adequate to avoid material duplicate payments.

STATE OF FLORIDA
DEPARTMENT OF STATEJEB BUSH
*Governor*SUE M. COBB
Secretary of State

December 13, 2006

Mr. William O. Monroe, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe:

Thank you for the opportunity to respond to Auditor General's multi-agency report titled: *Department of Management Services and Other Selected State Agencies MyFloridaMarketPlace*.

Pursuant to your instructions, we have enclosed the Department's response to Findings No. 13 and No. 15.

If you require additional information in this regard, please contact JuDee Pettijohn at (850)-245-6500.

Sincerely,

Handwritten signature of Sue M. Cobb in blue ink.

Sue M. Cobb, Secretary of State

Enc.

cc. JuDee Pettijohn, Deputy Secretary of State
Heidi Hughes, Chief of Staff/General Counsel
Kathy McCullars, Human Resource Manager, Bureau of Departmental Services
Kirby J. Mole, Inspector GeneralR. A. Gray Building • 500 South Bronough Street • Tallahassee, Florida 32399-0250
Telephone: (850) 245-6500 • Facsimile: (850) 245-6125 • <http://www.dos.state.fl.us>

FLORIDA DEPARTMENT OF STATE
RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS
DEPARTMENT OF MANAGEMENT SERVICES AND OTHER SELECTED STATE
AGENCIES MYFLORIDAMARKETPLACE SYSTEM

Finding No. 13: Management of Attachments.

Recommendation: DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to assure that the rule is being followed. Also, DMS should ensure that all confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Effective August 23, 2006, the Department adopted a "MyFloridaMarketPlace Confidential Information Policy" that identifies types of information considered to be confidential and establishes procedures to ensure that confidential information is not entered into MyFloridaMarketPlace. The Department's policy provides management and employees with guidelines to edit or redact confidential information from supporting documentation scanned into MyFloridaMarketPlace and establishes purge process procedures for information accidentally introduced. The Department trains all employees that use MyFloridaMarketPlace and monitors their activities for policy compliance. The Department's policy is on file with the Department of Management Services.

Finding No. 15: Agency Procedural Deficiencies.

Recommendation: To ensure that transactions are consistently and properly reviewed and processed, State agencies should establish written procedures and guidelines for key MFMP processes utilized. These written procedures should specifically:

- Require that approved direct orders are obtained prior to the receipt of any goods and services.
- Enhance procedures to ensure that MFMP is appropriately updated for invoices paid directly in FLAIR.

The Department will expedite the enhancement of comprehensive agency specific procedures for MyFloridaMarketPlace transaction processing that includes current order processing procedures and procedures related to invoice reconciliations. The Department's procedures will include timely processing of payments and updating invoices paid directly in FLAIR. Upon completion of the MFMP Enhanced User Support Materials by the Department of Management Services – Special Projects Office targeted for July 2007, the Department will incorporate relevant portions into Department guidelines.



Florida Department of Transportation

JEB BUSH
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

DENVER J. STUTLER, JR.
SECRETARY

December 18, 2006

William O. Monroe, CPA
Auditor General
Office of the Auditor General
Room G74, Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

We are pleased to respond to the preliminary and tentative audit findings and recommendations concerning the audit of:

**MyFloridaMarketPlace
July 2005 through June 2006**

As required by Section 11.45(4)(d), Florida Statutes, our response to the findings is enclosed.

We appreciate the efforts of you and your staff in assisting to improve our operations. If you have any questions, please contact our Inspector General, Cecil Bragg, at 410-5823.

Sincerely,

A handwritten signature in blue ink, appearing to read "Denver J. Stutler, Jr.", written over a horizontal line.

Denver J. Stutler, Jr., P.E.
Secretary

DJS:hmt

Enclosure

cc: Cecil Bragg, Inspector General

FLORIDA DEPARTMENT OF TRANSPORTATION

**Response to the Auditor General's
Preliminary and Tentative Audit Findings and Recommendations**

**MyFloridaMarketPlace
July 2005 through June 2006**

Finding No. 2: Agency Utilization of MFMP Functions

- DOT staff ceased using MFMP for processing encumbrances on March 15, 2004, utilizing an in-house information system.
- In January 2006, DOT Central Office discontinued paying for all purchases through MFMP, suggesting that MFMP system performance issues jeopardized meeting the 20-day invoice filing requirements mandated by Section 215.422, Florida Statutes. To enhance workload efficiencies, DOT discontinued processing payments for services requiring master agreements in MFMP in February 2006.
- DOT staff utilized an in-house information system to manage encumbrances indicating that they encountered numerous difficulties in trying to process encumbrances in MFMP and that MFMP's encumbrances function did not facilitate compliance with the statutory requirements of Section 339.135(2)(a), Florida Statutes.

Recommendation: We recommend that State agencies reconsider their utilization of MFMP functionality and the necessity of maintaining alternative systems.

Management Response: MFMP's encumbrance function did not facilitate compliance with statutory requirements. Specifically, MFMP does not have the edits necessary to verify that the encumbrance is for a financial project within the Department's adopted Work Program plan and to allow DOT's Comptroller to state that funds are available in accordance with Florida Statutes 339.135(6)(a). We use the encumbrance process to meet these statutory requirements and our existing CFM system has the additional edits in place to verify the project's encumbrances.

Paying for MFMP purchases directly through FLAIR is an official MFMP system option supported by DMS and DFS as long as the appropriate MFMP Invoice eForm function/process is followed appropriately. Accordingly, we consider this to be a choice of using one MFMP option over another MFMP option, not a decision to not use a required MFMP function.

Our long resisted decision to change options during the January/February 2006 timeframe was necessitated due to the General Payment Accountants being required to consistently work excessive overtime while their prompt payment compliance rate had dropped to an unacceptable level. Comparing the General Payment Accountant staffing and average prompt payment compliance rates for the seven months leading up to the change against the seven months since the change shows results that speak for themselves. While reducing the number of General Payment Accountant FTEs by one or 11.1%, their non-compliance with prompt payment statute (Section 215.422, F.S.) has decreased by 80.6%.

At a point when the negative systemic workload impact and the negative systemic impact on prompt payment compliance is corrected in MFMP/FLAIR, which may occur after implementation of ASPIRE, we will reconsider using the MFMP payment option.

Finding No. 13: Management of Attachments

Effective data management controls help ensure the integrity of information stored within a system. We continued to note deficiencies in the management of electronic documents with MFMP that serve as attachments to procurement records.

Recommendation: Agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Management Response: The Department adopted a policy on confidential information in MFMP on July 19, 2006. The policy included the procedures for identifying and redacting potentially exempt of confidential data prior to entering it in the system, and established the responsibility and process for monitoring compliance. All current users of MFMP were required to certify that they had read and understood the policy and all new users will be required to sign a similar certification.

Finding No. 16: Duplicate Payments – Agency Issues

At DOT, our test of 15 applicable transactions disclosed 1 duplicate payment resulting from DOT neglecting to follow the process outlined above when paying directly in FLAIR. The overpayment of \$17,381 was netted against other invoiced amounts due to the vendor.

Recommendation: To capitalize on MFMP system edit checks, State agencies should process payment for MFMP transactions through MFMP whenever possible. Agency procedures should require supervisory monitoring of payments made directly in FLAIR to ensure that the Invoice eForms and Payment Update eForms are completed and submitted and the "Payment completed in FLAIR" box is checked. Also, agencies should ensure that vendor invoices are properly defaced after processing, thus mitigating the risk that they will be paid twice.

Management Response: DOT's standard practice was to follow the process outlined. This was an oversight by one General Payment Accountant on one payment, versus a practice to not follow the outlined process. Additional training and emphasis has been provided to all General Payment Accountants on following the proper procedures.



Rocky McPherson
Executive Director

State of Florida
DEPARTMENT OF VETERANS' AFFAIRS
Office of the Executive Director
4040 Esplanade Way, Suite 152
Tallahassee, FL 32399-0950
850-487-1533 850-488-4001 (Fax)
www.floridavets.org

Jeb Bush
Governor
Charlie Crist
Attorney General
Tom Gallagher
Chief Financial Officer
Charles Bronson
Commissioner of Agriculture

December 20, 2006

Mr. William O. Monroe
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-0950

Dear Mr. Monroe,

In response to Auditor General's letter of November 20, 2006, a list of preliminary and tentative audit findings and recommendations which may be included in a report on the Department of Management Services and other Selected State Agencies MyFloridaMarketPlace System, the following comments on findings specific to the Department of Veterans' Affairs are provided.

Audit Finding #13: Recommendation: DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to assure that the rule is being followed. Also, DMS should ensure that all confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

Agency Response: FDVA has implemented procedures to comply with the DMS Rule. To codify these, a modification to FDVA Policy 5030.300B has been drafted and is currently under staff review. This modification encompasses the use and management of confidential information within MFMP.

Audit Finding #16: Recommendation: To capitalize on MFMP system edit checks, State agencies should process payments for MFMP transactions through MFMP whenever possible. Agency procedures should require supervisory monitoring of payments made directly in FLAIR to ensure that the Invoice eForms and Payment Update eForms are completed and submitted and the "Payment completed in FLAIR" box is checked. Also, agencies should ensure that vendor invoices are properly defaced after processing, thus mitigating the risk that they will be paid twice.

Agency Response: FDVA hosted a MFMP Refresher Training in November 2006 and has stressed the importance as to the correct procedures for making a payment directly in FLAIR to each of the accountants. These procedures will be added to the payment processing procedure documentation the FDVA Fiscal Department will send to each of the accountants in late December 2006."

Thank you for the opportunity to review our procedures. Audits are a beneficial tool in the proper function of a department. If there are any further questions, please do not hesitate to contact me or any of my staff.

Sincerely,

Warren R. McPherson
Colonel, U. S. Marine Corps (Ret.)
Executive Director



JEB BUSH
GOVERNOR

STATE OF FLORIDA

Office of the Governor

THE CAPITOL
TALLAHASSEE, FLORIDA 32399-0001

www.flgov.com
850-488-7146
850-487-0801 fax

December 20, 2006

Mr. William O. Monroe, Auditor General
111 West Madison Street
Claude Pepper Building
Tallahassee, Florida 32399

*Audit of the Department of Management Services and Other Selected State Agencies:
MyFloridaMarketPlace System*

Dear Mr. Monroe:

Thank you for the opportunity to review and comment on the preliminary and tentative findings and recommendations in the above referenced report; specifically to *Finding 13: Management of Attachments*. We generally concur with your finding related to written policies and procedures regarding MyFloridaMarketplace attachments and have implemented your recommendation of adopting written policies and procedures that specifically address confidential information issues. These written policies and procedures were submitted to and reviewed by the Department of Management Services.

We appreciate your office's courtesy and professionalism during the conduct of this review. Should you have any questions, please do not hesitate to contact Dawn Hanson, Director of Administration at 487-1011.

Regards,

Mark Kaplan
Chief of Staff

cc: Kim Mills, Director of Auditing
Dawn Hanson, Director of Administration



FLORIDA FISH AND WILDLIFE CONSERVATION COMMISSION



RODNEY BARRETO
Miami

SANDRA T. KAUPF
Palm Beach

H.A. "HERKY" HUFFMAN
Enterprise

DAVID K. MEEHAN
St. Petersburg

KATHY BARCO
Jacksonville

RICHARD A. CORBETT
Tampa

BRIAN S. YABLONSKI
Tallahassee

KENNETH D. HADDAD, Executive Director
VICTOR J. HELLER, Assistant Executive Director

OFFICE OF THE EXECUTIVE DIRECTOR
(850)487-3796 TDD (850)488-9542

December 15, 2006

Mr. William O. Monroe
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

RE: Preliminary and Tentative Audit Findings for the Department of Management Services and Other Selected State Agencies MyFloridaMarketPlace System

Dear Mr. Monroe:

We have reviewed the preliminary and tentative audit findings and recommendations included with your letter dated November 20, 2006. Please find enclosed our responses to the two audit findings related to our agency.

We appreciate the constructive comments and technical assistance provided by your staff. If further information is required, please contact our Director of Auditing, Trevor Phillips, at 488-6068.

Sincerely,

For Kenneth D. Haddad
Executive Director

kh/tp

Enclosures

INFORMATION TECHNOLOGY AUDIT
DEPARTMENT OF MANAGEMENT SERVICES (DMS)
AND OTHER SELECTED STATE AGENCIES
MYFLORIDAMARKETPLACE SYSTEM (MFMP)

FLORIDA FISH AND WILDLIFE CONSERVATION COMMISSION (FWC) RESPONSE

Finding No. 8: Management of User Access Privileges¹

Access privileges must be appropriately managed for end-users of an application system to ensure that users can only perform those system functions needed for their job duties, to enforce a proper segregation of duties, and to enable management to monitor employees' system activity.

In MFMP, users are designated certain roles authorized by management, based upon the agency's workflow and other access needs. Within roles, management grants users permissions to perform various functions. Roles and permissions comprise the user's profile and, when used appropriately, provide an effective means of internal control over Web-based procurement.

Our audit field work disclosed the following end-user access control deficiencies in MFMP:

- At DFS, we noted that an unusually large number of expenditure transactions (30 to 40 tested) were requisitioned under the same user ID. In response to our audit inquiries, DFS staff informed us that the user ID was shared by two employees. At DLE, purchasing staff used a common password to accommodate workload sharing. The sharing of a user ID or password limits the ability to assign responsibility for a transaction to an individual employee, thereby overriding a basic control of any IT system.
- At DMS and FWCC, staff did not routinely review the weekly Buyer Adoption Report (a listing of current users and their respective roles and permissions) during the audit period. Without routinely reviewing the report, agencies may be unaware of user accounts that are no longer appropriate and that should be inactivated.
The above-listed deficiencies increase the risk that inappropriate transactions could be processed without timely detection and assets could be misappropriated.

Recommendation: Agencies should periodically analyze the functions of their employees to ensure that MFMP user access privileges are appropriate and commensurate with users' job duties. Additionally, agencies should immediately cease the sharing of user IDs or passwords and assign each designated system user a unique user ID with a corresponding password. Further, agencies should

¹ The text of the finding is summarized to include only the portion applicable to FWC

regularly review the weekly Buyer Adoption Report and immediately remove any user accounts deemed no longer appropriate.

FWC Response: FWC has a single System Administrator who manages the users' access and authorities within MFMP. A regular analysis of user functions will be provided to FWC management by the System Administrator on a monthly basis, and there will be a weekly review of the Buyer Adoption Report. Both of these duties will be included in the System Administrator's position description.

FWC has developed a comprehensive password policy into the Internal Management Policies and Procedures Manual, (Chapter 3, Section 3.3) which includes a prohibition of password sharing. To the best of our knowledge, there are no FWC employees currently sharing a user ID or password for access to MFMP. Any workload sharing in FWC is performed by using the "delegation" function provided by MFMP, and this occurs only for short durations during an employee annual leave or sick leave absence.

Finding No. 13: Management of Attachments²

MFMP has the ability to store documents electronically as attachments to procurement records, and these documents may at times contain information deemed nonpublic pursuant to various provisions of State and Federal laws. Sections 215.93(5) and 215.94(4), Florida Statutes, provide that DMS, as functional owner of MFMP, is legally responsible for the security and integrity of all data records existing within or transferred from its Information subsystems. Furthermore, Section 119.07(b), Florida Statutes, provides that the custodian of public records shall provide safeguards to protect the contents of public records from unauthorized remote electronic access or alteration, and to prevent the disclosure or modification of those portions of public records which are exempt or confidential.

During our audit field work at the 14 State agencies, including DMS, we inquired whether each agency had developed policies and procedures that addressed preventing the introduction of confidential information into MFMP, monitoring documents stored as attachments into MFMP for confidential information, and redacting any confidential information so discovered. While some agencies described measures taken to address confidential information, none of the agencies provided written policies and procedures that specifically addressed confidential information issues within MFMP.

Recommendation: DMS should ensure that an appropriate rule is promulgated regarding MFMP attachments. Additionally, it should proceed with its planned audit process to ensure that the rule is being followed. Also, DMS should ensure that all

² The text of the finding is summarized to include only the portion applicable to FWC

confidential and unusable information currently in the system is purged. Finally, agencies should adopt written policies and procedures that specifically address confidential information issues within MFMP.

FWC Response: Upon review of the new DMS rule, FWC will adopt written policies and procedures that will prevent the introduction of confidential information into MFMP. FWC will continue to monitor MFMP for confidential information, and will coordinate with DMS to purge any such confidential information that may still remain in the system.