REPORT NO. 2011-193
JUNE 2011

DEPARTMENT OF HEALTH

MANAGEMENT INFORMATION AND PAYMENT SYSTEM (MIPS)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

STATE SURGEON GENERAL AND STATE HEALTH OFFICER

Pursuant to Section 20.43(2)(a), Florida Statutes, the head of the Department of Health is the State Surgeon General and State Health Officer, who is appointed by the Governor, subject to confirmation by the Senate. During the period under audit, the following individuals served as State Surgeon General and State Health Officer:

Dr. Ana Viamonte Ros	January 25, 2007, through January 3, 2011
Dr. Shairi Turner, Acting	March 16, 2011, through April 3, 2011
Dr. H. Frank Farmer, Jr.	From April 4, 2011

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

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF HEALTH

Management Information
and
Payment System (MIPS)

SUMMARY

The Department of Health (Department) uses the Management Information and Payment System (MIPS) to calculate monthly Child and Adult Care Food Program (CACFP) claims, provide management information, and prepare Federal reports. The Division of Information Technology within the Department operates and maintains MIPS.

Our audit focused on evaluating selected information technology (IT) controls applicable to MIPS. The results of our audit are summarized below:

Finding No. 1: Authorization documentation for some employees' MIPS access privileges did not exist or was incomplete or inaccurate.

Finding No. 2: The access privileges of some MIPS users were not appropriate for the users' assigned job responsibilities and did not enforce an appropriate separation of duties.

Finding No. 3: The Department's review of the appropriateness of MIPS user access privileges did not include some privileges and was not conducted on a sufficiently frequent basis.

Finding No. 4: Contrary to the requirements of the State of Florida, *General Records Schedule* for the retention of access control records, the Department did not retain certain access control records. Additionally, Department policy provided guidance that conflicted with the retention requirements set forth in the *General Records Schedule*.

Finding No. 5: Certain security controls related to user authentication needed improvement.

Finding No. 6: The Department's systems modification controls for MIPS needed improvement.

BACKGROUND

The Department of Health (Department) was created pursuant to Section 20.43, Florida Statutes, which states, in part, that the Department is to promote and protect the health of all residents and visitors in the State through organized State and community efforts, including cooperative agreements with counties. The Department is organized into 11 divisions, as listed in Section 20.43(3), Florida Statutes. The Division of Family Health Services includes the Bureau of Childcare Food Programs that administers the Child and Adult Care Food Program (CACFP). CACFP benefits consist of nutritious meals and snacks served to eligible children and adults who are enrolled for care at participating child care centers, adult day care centers, outside-school-hours care centers, at-risk afterschool programs, family and group day care homes, and emergency shelters. The United States Department of Agriculture, Food and Nutrition Service, administers CACFP through grants-in-aid to states.

The Bureau of Childcare Food Programs utilizes the Management Information and Payment System (MIPS) to receive CACFP claims from pre-approved contractors who provide meals and snacks under the program. MIPS calculates monthly program claims, provides management information, and prepares Federal reports.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Documentation of User Access Authorizations

Effective security controls include logical (electronic) access controls that restrict legitimate and appropriate users to the specific IT resources needed and prevent others from accessing the resources. Access controls include, among other things, documentation of management authorization of the access privileges granted to system users. According to the Department's *Information Security and Privacy Policy*, the Department's workforce will be provided a user account to access Department IT resources. This access will be based on the documented need as provided by the appropriate hiring authority.

According to the Department's *Process for Assigning Employee Access to MIPS*, MIPS user account administration (creating or changing user access privileges to MIPS) is the responsibility of the Operations and Management Consultant Manager. The *Process* states further that the user's supervisor must e-mail a request to the Operations and Management Consultant Manager to add or change a MIPS user account.

We requested authorization documentation for a sample of 10 of the 44 active MIPS users as of March 23, 2011. For 5 of the 10 users included in our sample, authorization documentation for the user access privileges did not exist. Our review of the 5 authorization documents that were on file disclosed the following:

- The access privileges that had been requested were not specified on 2 documents.
- Access privileges shown as authorized on 1 additional document did not match the access privileges actually granted in MIPS. The access granted, however, did not appear excessive for the job duties of the MIPS user listed on the form.

The Department implemented a new practice for issuing access to MIPS in July 2010 that included the use of a *MIPS Account Rights Request Form* for requesting access. As of March 23, 2011, only one new user had been granted access after July 2010 and a *MIPS Account Rights Request Form* was used to authorize the user's access. Without accurate authorization forms to document approved user access privileges, management's ability to monitor the appropriateness of access privileges may be limited.

Recommendation: The Department should ensure that authorization documentation is accurately maintained for all granted access privileges.

Finding No. 2: Appropriateness of Access Privileges

Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, or destruction. Additionally, the Department's *Information Security and Privacy Policy* provides that the Department's workforce shall have unique user accounts.

We reviewed the access privileges of the ten active MIPS user accounts as of March 23, 2011. Our review disclosed some instances in which user access to MIPS was not appropriate for the users' assigned job responsibilities and did not enforce an appropriate separation of duties. Specifically:

- The Operations and Management Consultant Manager had been given complete update access to MIPS, exceeding the access privileges the Manager needed for the performance of assigned job responsibilities. Some of these privileges were described as incompatible in the Department's *Process for Assigning Employee Access to MIPS* because the privileges created a separation of duties concern. Specifically, the combination of some of the access privileges allowed the Manager the ability to both enter a new contractor into MIPS and

approve claims. Additionally, the Manager was given an access privilege to perform system modifications in the production environment, potentially bypassing established system modification controls.

- The Department had also issued a generic user account that provided the above-described complete update access privileges assigned to the Operations and Management Consultant Manager plus three additional privileges. According to Department management, the generic user account was being utilized by the MIPS Programmer to perform back-up security administration duties for the Operations and Management Consultant Manager. Because the generic user account was not assigned to one person, the Department's ability to establish accountability for actions performed with the account may be limited.

These conditions increased the risk of unauthorized disclosure, modification, or destruction of MIPS data. In response to audit inquiry, Department management modified the Operations and Management Consultant Manager's account by removing some of the unnecessary access privileges and changing 20 access privileges from read, add, and update to read only.

Recommendation: The Department should limit access privileges to MIPS to only what is needed for the performance of assigned job responsibilities to enforce an appropriate separation of duties. Additionally, the Department should assign unique user accounts to all individual authorized MIPS users.

Finding No. 3: Periodic Review of MIPS Access Privileges

Periodic review of user access privileges helps ensure that user access privileges remain appropriate. The Department's *Information Security and Privacy Policy* provides that supervisors will regularly review the access privileges of staff and ensure that access is appropriate for the performance of assigned job responsibilities. AEIT Rule 71A-1.007, Florida Administrative Code, provides that agency information owners shall review access rights periodically based on risk, access account change activity, and error rate.

According to Department management, applicable supervisors of employees having read, add, and update access privileges in MIPS receive employee listings periodically to verify that the access privileges are appropriate. In response to audit inquiry, Department management indicated that the reviews are conducted every two years and that the last review of MIPS user access privileges was performed in October 2009. Although the reviews were being conducted, the reviews did not include the read and add, read and create, or read and update privileges. Additionally, the importance of MIPS to the Child and Adult Care Food Program and the existence of excessive MIPS access privileges as described in Finding No. 2 indicate the need for the Department to review MIPS access privileges more frequently than every two years. Under these conditions, the risk was increased that MIPS data and IT resources may be subject to unauthorized disclosure, modification, or destruction.

Recommendation: The Department should reassess the frequency by which MIPS access privileges are reviewed by supervisors and consider a more frequent review. Additionally, the Department should ensure that all levels of MIPS access privileges are subject to the review.

Finding No. 4: Access Control Records

According to the Department's *Information Security and Privacy Policy*, all Department information must be retained, archived, and destroyed in accordance with the State of Florida, *General Records Schedule GS1-SL for State and Local Government Agencies (General Records Schedule)*, revised by the Department of State effective August 2010, and the retention requirements of the Department. The *General Records Schedule* provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment.

Our audit disclosed that the Department did not retain certain access control records, contrary to the requirements of the *General Records Schedule*. Access records of former employees with access to the network or MIPS and nonclaiming contractors (contractors who require read-only access to the application to review claim and application information and to download program forms) with access to MIPS were not retained upon being deleted when the access was no longer needed. Also, when modifications were made to existing employee access privileges in MIPS, the previous access privilege records were deleted.

Additionally, conflicting Department guidance existed within the *Information Security and Privacy Policy, Access Security – Termination of Access Rights*. Specifically, contrary to the requirements of the *General Records Schedule*, the *Policy* provided that access accounts must be deleted 60 days after termination of employment. The *Policy* did not provide for the timely disabling of unneeded access privileges and retention of the related access control records as provided in the *General Records Schedule*.

Without adequate retention of access control records, the risk increases that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur. Additionally, the Department is not in compliance with the State's record retention requirements. Furthermore, the risk of access privileges being misused by former employees or others would be reduced if the *Policy* were enhanced to require the disabling of access privileges within 24 hours of termination.

Recommendation: The Department should retain access control records in accordance with the requirements of the *General Records Schedule* and update its *Policy* to provide for the disabling, but not deleting, of former employee access privileges within 24 hours of employee termination.

Finding No. 5: Security Controls – User Authentication

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to user authentication that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising Department data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls related to user authentication, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The Department should improve security controls related to user authentication to ensure the confidentiality, integrity, and availability of data and IT resources.

Finding No. 6: Systems Modification

Effective systems modification controls are intended to ensure that all systems modifications are properly authorized, tested, and approved for implementation. According to the Department's *IT Change Management Standard Operating Procedure*, the following components are required for modifications to applications: impact analysis, testing, rollback plan, and customer notification.

Our audit disclosed that the impact analyses and rollback plans for the two systems modifications included in our test were not documented, contrary to Department procedure. Additionally, systems modifications to the MIPS

production environment (i.e., production programs) were logged; however, the logs were not being reviewed to ensure that unauthorized systems modifications had not been made.

The absence of impact analyses and rollback plans increases the risk that systems modifications may be implemented with unintended results to the system or data and that the unintended results may not be easily reversed. Additionally, without supervisory review of systems modifications to the MIPS production environment, the risk is increased that unauthorized or erroneous systems modifications may be moved into the production environment without timely detection, jeopardizing the ongoing integrity of MIPS.

Recommendation: The Department should ensure compliance with established procedure to provide for the proper documentation of all MIPS systems modifications. Additionally, to ensure that systems modifications to MIPS are made in a consistent manner, the Department should review all systems modifications to the MIPS production environment to detect the implementation of any unauthorized or erroneous programs, should they occur.

OBJECTIVES, SCOPE, AND METHODOLOGY

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

We conducted this IT operational audit from March 2011 through April 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to MIPS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, and reliability of data; and the safeguarding of IT resources.

The scope of our audit focused on evaluating selected IT controls applicable to MIPS. The audit included selected general IT controls over systems modification and logical access to programs and data. The audit also included selected application IT controls and selected user controls relevant to MIPS. Our audit included examinations of various Department records and transactions (as well as events and conditions) occurring from July 2010 through April 2011.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of MIPS; including the purpose of the system; recent changes to Federal reporting compliance requirements; computing platform and related software; access paths to view, modify, or delete data; system modification process; and the user account administration process.
- Tested the effectiveness of MIPS password settings to evaluate the effectiveness of the settings in adequately protecting resources.
- Tested the effectiveness of Department network password settings to evaluate the effectiveness of the settings in adequately protecting resources.

- Evaluated on a sample basis the effectiveness of procedures for authorizing user access privileges to MIPS. Specifically, we reviewed a sample of 10 user accounts to determine whether the access was authorized in writing.
- Evaluated on a sample basis the appropriateness of the access privileges granted. Specifically, we reviewed a sample of 10 MIPS user accounts to determine whether the access levels granted were appropriate.
- Tested the effectiveness of MIPS input, processing, and output control procedures relating to two Federal requirements.
- Tested the effectiveness of systems modification procedures followed by the Department for the authorization, design, testing, and approval of two MIPS modifications resulting from two recent changes in Federal requirements.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

AUTHORITY

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

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated June 22, 2011, the State Surgeon General provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

EXHIBIT A
MANAGEMENT'S RESPONSE

FLORIDA DEPARTMENT OF HEALTH

Rick Scott
Governor

H. Frank Farmer, Jr., M.D., Ph.D.
State Surgeon General

June 22, 2011

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

Dear Mr. Martin:

We are pleased to respond to the preliminary and tentative audit findings and recommendations concerning the Auditor General's Information Technology Audit of Management Information and Payment System (MIPS). Our response to the findings is enclosed as required by section 11.45(4)(d), *Florida Statutes.*

We appreciate the effort of you and your staff in assisting to improve our operations. If you have any questions, please contact our Director of Auditing, Michael J. Bennett by calling (850) 245-4444 extension 2150.

Sincerely,

H. Frank Farmer, Jr., M.D., Ph.D.
State Surgeon General

HFF/kir
Enclosure

cc: James D. Boyd, C.P.A., M.B.A.
Inspector General
Michael J. Bennett, C.I.A.
Director of Auditing

Office of the State Surgeon General
4052 Bald Cypress Way, Bin A00 • Tallahassee, Florida 32399-1701
Phone: (850) 245-4444 • Fax: (850) 922-9453 • http://www.floridashealth.com

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Health Management Information and Paymnet System (MIPS) Information Technology Operational Audit

Para. #	*Finding:*	*Recommendation:*	*Management Response:*	*Corrective Action Plan:*
1	Authorization documentation for some employees' MIPS access privileges did not exist or was incomplete or inaccurate.	The Department should ensure that authorization documentation is accurately maintained for all granted access privileges.	We concur with this finding and have updated the process for assigning employee access to MIPS whereby a supervisor sends a signed and completed MIPS Account Rights Request form authorizing the Project Manager to assign rights in MIPS for all users.	We will collect MIPS Account Request forms for all MIPS users. Completed April 2011.
2	The access privileges of some MIPS users were not appropriate for the users' assigned job responsibilities and did not enforce an appropriate separation of duties.	The Department should limit access privileges to MIPS to only what is needed for the performance of assigned job responsibilities to enforce an appropriate separation of duties. Additionally, the Department should assign unique user accounts to all individual authorized MIPS users.	We concur with this finding.	We have adjusted the Operations and Management Consultant Manager's rights to reflect those rights needed for the performance of assigned job responsibilities to address the separation of duties concern. Also, we have removed the generic user account in MIPS. Completed April 2011.
3	The Department's review of the appropriateness of MIPS user access privileges did not include some privileges and was not conducted on a sufficiently frequent basis.	The Department should reassess the frequency by which MIPS access privileges are reviewed by supervisors and consider a more frequent review. Additionally, the Department should ensure that all levels of MIPS access privileges are subject to the review.	We concur with this finding.	We have set up a system of checking privileges annually that includes supervisor's approval. Completed June 2011.

Page 1

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Para. #	Finding:	Recommendation:	Management Response:	Corrective Action Plan:
4	Contrary to the requirements of the State of Florida, General Records Schedule for the retention of access control records, the Department did not retain certain access control records. Additionally, Department policy provided guidance that conflicted with the retention requirements set forth in the General Records Schedule.	The Department should retain access control records in accordance with the requirements of the General Records Schedule and update its Policy to provide for the disabling, but not deleting, of former employee access privileges within 24 hours of employee termination.	Program Office: We concur with this finding. DOH IT: We concur with this finding.	Program Office: With the rewrite of MIPS into .net, all user accounts will be retained after account disabling and until then, we will keep paper documentation of all employee and non-claiming contractor accounts that are disabled or have a change in privilege. Information Techonology Office: The DOHP 50-10-10 policy conflict with the General Records Schedule will be addressed and corrected in the next policy revision cycle which is tentatively scheduled to begin in Fall 2011. Also during this revision cycle, DOHP 50-10-10 will be updated so that it clearly supports the current DOH IT practice of disabling but not deleting former employee access privileges within 24 hours of employee termination/separation. Anticipated Completion Date: February 2012.
5	Certain security controls related to user authentication needed improvement.	The Department should improve security controls related to user authentication to ensure the confidentiality, integrity, and availability of data and IT resources.	We concur. We will implement the required changes and the majority of the recommended improvements..	Required security controls related to user authentication are being addressed. Anticipated completion date: August 2011.

Page 2

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Para. #	*Finding:*	*Recommendation:*	*Management Response:*	*Corrective Action Plan:*
6	The Department's systems modification controls for MIPS needed improvement.	The Department should ensure compliance with established procedure to provide for the proper documentation of all MIPS systems modifications. Additionally, to ensure that systems modifications to MIPS are made in a consistent manner, the Department should review all systems modifications to the MIPS production environment to detect the implementation of any unauthorized or erroneous programs, should they occur.	Program Office: We concur. DOH IT: A) PROGRAM OFFICE AREA OF RESPONSIBILITY. DOH IT has a Change Management standard operating procedure in place. In regard to this procedure and the MIPS application, specifically the impact analysis and roll back plans, which the AG indicated are not being documented 100% of the time, it's the understanding of DOH IT that the Program Office is responsible for developing the impact analysis and roll back plans for the MIPS application. DOH IT can work with the Program Office using the DOH IT Change management procedures and/or Customer Service Center ticketing system to help them develop a way to document their the impact analysis and roll back plans more efficiently. B) DOH IT AREA OF RESPONSIBILITY: it's the understanding of DOH IT that the MIPS system modifications logs were present and intact, but they were not being reviewed by a supervisor for unauthorized or erroneous system modifications. After discussions with the Acting Chief of the Bureau of Applications and Development (DOH IT) and that Bureau's Data Center Work Request Manager Liaison, DOH IT concurs that this is not occurring and that DOH IT should be the program office providing this service.	Program Office: We will implement process to address impact analysis and roll back plans. The FootPrints change management process addresses the need for review of systems modifications. DOH IT: DOH IT already has a Change Management standard operating procedure in place. As part of the Change Management procedure, the Data Center Work Request Manager Liaison opens up a Courtesy Notice about the specific with the Southwood Shared Resource Center (SSRC) staff. After the change has been effected, the Courtesy Notice is closed. This Courtesy Notice sub-routine of the Change Management procedure could be used to accommodate the required third party (delegated supervisory third party) review of the MIPS systems modifications logs. This proposed new business process would be done by the Data Center Work Request Manager Liaison opening up the Courtesy Notice to the SSRC as usual, then the SSRC staff would join the process by reviewing the MIPS systems modifications logs (to the MIPS production environment) and reporting any detected unauthorized implementations and/or erroneous programs (should they occur) to the Data Center Work Request Manager Liaison who would then use established DOH IT procedures to address the reported information. Anticipated completion date: February 2012.

Page 3