



CHARLIE CRIST
GOVERNOR

Better Health Care for all Floridians

THOMAS W. ARNOLD
SECRETARY

March 31, 2010

Thomas W. Arnold, Secretary
Agency for Health Care Administration
2727 Mahan Drive
Tallahassee, FL 32308

Dear Secretary Arnold,

Please find enclosed our six-month status report on the Auditor General's Audit of *Agency for Health Care Administration Florida Medicaid Management Information System (FMMIS) and Decision Support System (DSS)* Report Number 2010-025, issued October 2009. This status report is issued in accordance with the statutory requirement to report on corrective actions resulting from the Auditor General's recommendations six months from the report date.

If you have any questions about this status report, please contact Mike Blackburn at 412-3977.

Sincerely,

Pete Williams
Inspector General

PW/mb
Enclosure

cc: Terry L. Shoffstall, Legislative Auditing Committee
Roberta Bradford, Secretary, Division of Medicaid

RECEIVED
APR 6 - 2010



**Six-Month Status on Auditor General Report:
IT Audit of FMMIS and DSS
Report #2010-025 Issued: October 2009
Six-Month Status as of: March 2010**

Finding #1	Recommendation	Management Response as of October 2009	Management Response as April 2010	Anticipated Completion Date & Contact
<p>The Agency and EDS lacked appropriate access control documentation to demonstrate the business justification for access privileges granted within FMMIS, DSS, and the related software.</p>	<p>The Agency, with the assistance of EDS, should develop documentation of user roles and access privileges to guide in the assignment of employee and contractor access. In addition, access authorization records should be consistently maintained to document the access privileges requested, approved, and granted.</p>	<ul style="list-style-type: none"> The various user roles within the FMMIS and DSS applications, server operating systems, and databases and the access privileges that each user role provided. <p>AHCA Response: The roles in MEUPS (FMMIS/DSS application) have been updated with the appropriate clarification to assist in the understanding of the functionality that the role provides.</p> <ul style="list-style-type: none"> The correlation of user roles for the FMMIS and DSS applications, server operating systems, database, and program change management software with specified job functions. In response to audit inquiry, EDS created a Role Definition by Position document to help guide the assignment of FMMIS user roles based on job functions. <p>AHCA Response: As noted in</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Stroud, David Powers, and Jennifer Weeks</p>

*****MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.**

**Six-Month Status on Auditor General Report:
IT Audit of FMMIS and DSS
Report #2010-025 Issued: October 2009
Six-Month Status as of: March 2010**

Finding #1	Recommendation	Management Response as of October 2009	Management Response as April 2010	Anticipated Completion Date & Contact
		<p>position (job title) there will always be exceptions. There are various functions a user may perform based on skill set and/or assignment; these exceptions are documented on the request form.</p> <ul style="list-style-type: none"> • Authorization for the FMMIS and DSS user roles granted to 4 of the 5 Agency employees included in our tests. <p>AHCA Response: We acknowledge this finding; there has been a refined business process implemented to maintain the Agency user request forms and approvals in a central location.</p> <ul style="list-style-type: none"> • Authorization for server operating systems and database user roles. In response to audit inquiry, EDS staff stated that procedures have been revised to retain documentation of server operating system and database access authorization. 	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009</p> <p>Alan Stroud, David Powers, and Jennifer Weeks</p>

*****MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.**

**Six-Month Status on Auditor General Report:
IT Audit of FMMS and DSS
Report #2010-025 Issued: October 2009
Six-Month Status as of: March 2010**

Finding #2	Recommendation	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
<p>In some instances, system access privileges were inconsistent with employee or contractor job functions. In addition, neither the Agency nor EDS performed periodic reviews of the appropriateness of access privileges.</p>	<p>The Agency, together with EDS, should review, and adjust as appropriate, the above-listed access privileges in question. In addition, the Agency should ensure that periodic reviews are conducted of the ongoing appropriateness of system access privileges to facilitate the timely detection and correction of excessive or unnecessary capabilities.</p>	<p>For 19 of 57 users included in our sample with access to server operating systems, the access granted was not necessary based on the users' job functions. AHCA Response: We acknowledge the finding; however there will always be examples outside the norm based on the specialty job functions that are limited to specific users. These exceptions are now being documented on the Security Request form within the business justification section. • For 25 of 61 users included in our test with access to program change control software, the access granted was not necessary based on the users' job functions. AHCA Response: We acknowledge the finding; however there will always be examples outside the norm based on the specialty job functions that are limited to specific users. These</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Strowd, David Powers, and Jennifer Weeks</p>
		<p>AHCA Response: We acknowledge the finding; however there will always be examples outside the norm based on the specialty job functions that are limited to specific users. These</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Strowd, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

**Six-Month Status on Auditor General Report:
IT Audit of FMMS and DSS
Report #2010-025 Issued: October 2009
Six-Month Status as of: March 2010**

Finding #2	Recommendation	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>exceptions are now being documented on the Security Request form within the business justification section.</p> <ul style="list-style-type: none"> • Thirty-four of the 61 users had the ability to both modify source program code and move the changes into the production environment without detection, contrary to an appropriate separation of duties. <p>AHCA Response: Access to promote changes is limited to users with Super Users (SU) access. This access has been reviewed and limited to 19 users. Technical Support staff has been briefed on the process and will continue to receive periodic refresher training, as needed. All support staff are required to review the Change Order (CO) Programming Checklist detailing these requirements. Each Systems Manager is responsible for ensuring employees within their</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Stroud, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

Six-Month Status on Auditor General Report:
 IT Audit of FMMIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010

Finding #2	Recommendation	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>areas of responsibility follow these guidelines and documentation requirements.</p> <ul style="list-style-type: none"> • FMMIS users with the Help Desk role had the ability to assign themselves the System Administrator role, thereby gaining inappropriate and unnecessary access privileges. In response to audit inquiry, EDS initiated changes to FMMIS to prevent Help Desk users from inappropriately assigning themselves the System Administrator Role. <p>AHCA Response: July 27 2009, EDS removed the capability of Help Desk users to assign themselves as a System Administrator.</p> <ul style="list-style-type: none"> • Neither the Agency nor EDS performed periodic reviews of the appropriateness of access privileges within the applications, operating systems, database, or program change management 	<p>As stated in the original response, this is completed.</p>	<p>July 27, 2009 Alan Strowd, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

Six-Month Status on Auditor General Report:
 IT Audit of FMMIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010

Finding #2	Recommendation	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>software. Such periodic reviews could enable the Agency or EDS to detect and more timely adjust inappropriate access privileges such as those described above. In response to audit inquiry, EDS implemented new procedures in February 2009 for the review of FMMIS access privileges.</p> <p>AHCA Response: EDS has refined the procedures around reviewing the appropriateness of access. Super User access for Databases/ Servers/VCTL is reviewed weekly by the Project Managers. MEUPS (FMMIS application) roles are reviewed monthly by the Security Officer. EDS has developed a schedule to review all users for all databases and servers. The target date to begin this effort is October 2009.</p>	<p>As stated in the original response, this is completed.</p> <p>However, it is important to note effective December 2009 MCM approved a request from HP to move the MEUPS access review to a quarterly process.</p> <p>Also, when reviewing/ following up on the schedule that HP provided for reviewing all users' access to all servers and databases, it was determined they have</p>	<p>October 2, 2009</p> <p>Alan Strowd, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

**Six-Month Status on Auditor General Report:
 IT Audit of FMFIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010**

Finding #2	Recommendation	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
			failed to adhere to the schedule. MCM has initiated a Corrective Action Plan.	

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

**Six-Month Status on Auditor General Report:
IT Audit of FMMIS and DSS
Report #2010-025 Issued: October 2009
Six-Month Status as of: March 2010**

Finding #3	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
Some former contractor access privileges were not removed in a timely manner.	The Agency should work with EDS to ensure that the access privileges of former contractors are promptly removed.	<p>AHCA Response: The agency acknowledges all of the documented findings. The NACO's (Network Application Control Online System) identifications (IDs) (i.e. EDS VPN IDs) control all areas. In order to access to the before mentioned areas a VPN connection must be established first. There is a system report card SLA to monitor that all ids are terminated within 4 hours of an employees' termination. However, EDS has implemented procedures improving the timeliness of removal of the terminated users and the database/server levels.</p>	As stated in the original response, this is completed.	October 2, 2009 Alan Stroud, David Powers, and Jennifer Weeks

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

**Six-Month Status on Auditor General Report:
IT Audit of FMMIS and DSS
Report #2010-025 Issued: October 2009
Six-Month Status as of: March 2010**

Finding #4	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
<p>Generic user identifications (IDs) for database administration were being shared by contractor staff.</p>	<p>The Agency should require EDS to assign unique user IDs to all individual users authorized to perform database administration functions for FMMIS and DSS.</p>	<p>AHCA Response: I t was discovered that database administration roles have been performed with these three IDs. As a result of this finding EDS is changing the privileges associated to the IDs and educating the users. EDS will include these IDs in their ongoing auditing procedures.</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Stroud, David Powers, and Jennifer Weeks</p>

****MCM Note:** The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

**Six-Month Status on Auditor General Report:
IT Audit of FMMIS and DSS
Report #2010-025 Issued: October 2009
Six-Month Status as of: March 2010**

Finding #5	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
<p>Certain access controls were deficient in the areas of user authentication, session controls, and logging of system activity.</p>	<p>The Agency should implement the appropriate access controls in the areas of user authentication, session controls, and logging of system activity to ensure the continued confidentiality, integrity, and availability of Agency data and IT resources.</p>	<p>AHCA Response: We have carefully reviewed the findings and have implemented some of your recommendations. However some of the recommendations will not be implemented because they may be covered via another medium. We are preparing a response for each of the reported findings for internal documentation purposes.</p>	<p>As stated in the original response, this is completed</p>	<p>October 2, 2009 Alan Stroud, David Powers, and Jennifer Weeks</p>

*****MCM Note:** The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

**Six-Month Status on Auditor General Report:
 IT Audit of FMMIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010**

Finding #6	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
<p>Program and data change controls for FMMIS and DSS needed improvement.</p>	<p>The Agency, with the assistance of EDS as applicable, should accurately document and enforce effective program and data change controls that provide for the involvement of the end user; timely testing and approval of changes; and an appropriate separation of duties for programming, testing, approval, and implementation of program and data changes.</p>	<ul style="list-style-type: none"> Written EDS program change control procedures did not reflect actual EDS practices. For example, Agency staff indicated that procedures for the use of the User Acceptance Region and the specific requirements for testing and management approval of system changes were documented prior to EDS becoming the Medicaid fiscal agent and were no longer reflective of actual practice. In addition, no written Agency or EDS procedures existed to govern the change control process for FMMIS and DSS batch programs. <p>AHCA Response: Cycle Monitoring Procedures, the Customer Service Request (CSR)</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

Six-Month Status on Auditor General Report:
 IT Audit of FMMS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010

Finding #6	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>Process, and the CO Process documentation have been updated and can be found on iTrace.</p> <ul style="list-style-type: none"> • According to EDS staff, program changes were to be implemented and documented within production software releases. However, we identified instances where program changes were moved into the production environment without being documented as part of a production software release. Under these conditions, it could be more difficult for Agency management to track the changes made and ensure that the changes were approved prior to implementation. <p>AHCA Response: According to procedures, our SE can no longer release code. The Cycle Monitors do this with the Project Manager's approval. There is an exception to this process in order to allow a few selected SE's the ability to promote code in emergency</p>	<p>As stated in the original response, this is completed.</p>	<p>Alan Stroud, David Powers, and Jennifer Weeks</p> <p>October 2, 2009</p> <p>Alan Stroud, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

Six-Month Status on Auditor General Report:
 IT Audit of FMMIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010

Finding #6	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>situations normally related to nightly cycles. These special code promotions are tracked in FIP with the cycle monitoring CO type and ultimately approved by the State, after the fact.</p> <ul style="list-style-type: none"> The program change management software used by EDS did not provide automatic logging and reporting of program changes moved into the production environment, limiting Agency management's ability to ensure that all program changes were authorized. <p>AHCA response: The Agency acknowledges the finding. The code promotion process has been changed, requiring EDS release teams and configuration managers to review all objects for promotion to ensure everything is tied to a CO and the CO has been approved. There are reports available to identify what was released for any particular week.</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Strowd, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

Six-Month Status on Auditor General Report:
 IT Audit of FMMIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010

Finding #6	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<ul style="list-style-type: none"> • Changes to FMMIS and DSS data by EDS technical staff using utility software that bypassed normal FMMIS application edits and controls were sometimes performed by one EDS employee without independent testing or approval of the changes. <p>AHCA Response: The Florida Interactive Portal (FIP) has been modified to prevent this from reoccurring. The defect CO type is no longer available.</p> <ul style="list-style-type: none"> • According to Agency and EDS staff, Agency management authorization was required for program changes other than those to correct program defects. <p>However, Agency management authorization was lacking for 7 of the 10 EDS program changes that were made for purposes other than correcting defects.</p> <p>AHCA Response: The Change Order (CO) workflow has now been updated to ensure AHCA</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009</p> <p>Alan Strowd, David Powers, and Jennifer Weeks</p>
			<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

Six-Month Status on Auditor General Report:
 IT Audit of FMMIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010

Finding #6	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>approval before a CO can be closed.</p> <ul style="list-style-type: none"> • Programmer testing was not documented for 6 EDS program changes. <p>AHCA response: We acknowledge this finding. The examples provided were during a time period when many procedural changes were occurring. The current promotion process will avoid future occurrences of this finding.</p> <ul style="list-style-type: none"> • For 4 EDS changes, the dates that testing were completed preceded the dates that the program changes were coded. <p>AHCA Response: This is contrary to our procedures. Management has reemphasized the appropriate procedures to EDS and AHCA staff and further clarified within the promotions procedures.</p> <ul style="list-style-type: none"> • Agency policy provided that program changes were to be independently tested by EDS 	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009</p>
			<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Stroud, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

Six-Month Status on Auditor General Report:
 IT Audit of FMMS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010

Finding #6	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>business analysts. However, 7 EDS program changes lacked documentation of testing by the EDS business analysts and testing of 1 EDS change was documented as having occurred after the change was implemented in the production environment.</p> <p>AHCA Response: The Agency acknowledges the eight occurrences mentioned above were examples in which business analyst documentation was necessary. However, it is important to note that the various business areas within FMMS have unique testing requirements regarding the code promotion. Therefore, not all COs will have Business Analyst testing.</p> <ul style="list-style-type: none"> • Agency management approval for implementation was not documented for 8 EDS program changes and 3 EDS program changes were documented as having been approved after 	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009</p> <p>Alan Strowd, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

Six-Month Status on Auditor General Report:
 IT Audit of FMMIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010

Finding #6	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>implementation. AHCA Response: The Agency acknowledges the above mentioned examples were not emergency situations. However, there will continue to be situations for which documentation after the fact or limited documentation will occur i.e., cycle monitor promotions and specific coding promotion that do not fit into the normal documentation requirements.</p> <ul style="list-style-type: none"> • For 4 EDS program changes, the same individual was documented as having developed and implemented the changes in the production environment, contrary to an appropriate separation of duties. <p>AHCA Response: The Agency acknowledges the findings. Although the above referenced examples were not emergency situations, it is important to note that instances of this nature will</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Strowd, David Powers, and Jennifer Weeks</p>
		<p>AHCA Response: The Agency acknowledges the findings. Although the above referenced examples were not emergency situations, it is important to note that instances of this nature will</p>	<p>As stated in the original response, this is completed.</p>	<p>October 2, 2009 Alan Strowd, David Powers, and Jennifer Weeks</p>

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

**Six-Month Status on Auditor General Report:
 IT Audit of FMMIS and DSS
 Report #2010-025 Issued: October 2009
 Six-Month Status as of: March 2010**

Finding #6	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
		<p>continue to occur for emergency situations. EDS and the Agency have defined such scenarios when this would be appropriate and also set up a procedure in which the developer is required to perform a walk through with another senior developer prior to promoting the code.</p>		

***MCM Note: The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.

**Six-Month Status on Auditor General Report:
IT Audit of FMMIS and DSS
Report #2010-025 Issued: October 2009
Six-Month Status as of: March 2010**

Finding #7	Recommendation(s)	Management Response as of October 2009	Management Response as of April 2010	Anticipated Completion Date & Contact
<p>Agency reconciliation documentation of FMS data with DSS data was incomplete and contained discrepancies, limiting the Agency's ability to demonstrate the accuracy and completeness of DSS data.</p>	<p>The Agency should address the inaccuracies in the DSS Claims Balance Reports and maintain appropriate documentation to demonstrate that complete reconciliations of FMMIS data with DSS data are performed.</p>	<p>AHCA Response: AHCA acknowledges the finding and DSS team is working on refining the reconciliation process. The DSS team is anticipating completing this effort by close of business November 27, 2009.</p>	<p>The DSS Team created an on-demand report within Business Objects that balances claim payment totals, expenditures, and accounts receivable every week to the corresponding OnBase BAC-Y report. The new balancing report was completed and implemented on November 9, 2009 and directly queries the detailed claims data instead of aggregate tables. This report is also available online as a public report.</p>	<p>November 9, 2009 Alan Stroud, David Powers, Jennifer Weeks and Matt Kline</p>

*****MCM Note:** The date provided for items completed prior to the final response will show as October 2, 2009, which was the date of the final response.