REPORT NO. 2010-025
OCTOBER 2009

AGENCY FOR HEALTH CARE ADMINISTRATION

FLORIDA MEDICAID MANAGEMENT INFORMATION SYSTEM (FMMIS)

AND

DECISION SUPPORT SYSTEM (DSS)

Information Technology Operational Audit

For the Period
October 2008 Through April 2009
and Selected Actions Through June 2009

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF HEALTH CARE ADMINISTRATION

Pursuant to Section 20.42(2), Florida Statutes, the Secretary of Health Care Administration is appointed by the Governor, subject to confirmation by the Senate. Ms. Holly Benson served as Secretary during the audit period.

The audit team leader was Art Wahl, CPA, 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) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

AGENCY FOR HEALTH CARE ADMINISTRATION

Florida Medicaid Management Information System (FMMIS)
and
Decision Support System (DSS)

SUMMARY

Sections 409.901(2) and (15), Florida Statutes, designate the Agency for Health Care Administration (Agency) as the single State agency that administers or supervises the administration of the State Medicaid plan under Federal law. Electronic Data Systems (EDS) became the Medicaid fiscal agent on June 26, 2008, and developed and operates the Florida Medicaid Management Information System (FMMIS) and Decision Support System (DSS). FMMIS is used to enroll providers, process Medicaid claims, adjudicate claims, accept and process encounter claims for data collection, and reimburse providers. FMMIS data is imported into DSS to enable efficient reporting and data analysis. The Medicaid Program is highly dependent on the security, integrity, and proper functioning of FMMIS and DSS.

Our audit focused on evaluating the effectiveness of selected Information Technology (IT) controls applicable to FMMIS and DSS during the period October 2008 through April 2009 and selected actions through June 2009. Our audit disclosed numerous instances where FMMIS and DSS IT controls were deficient or needed improvement. These control issues limit the Agency's assurance of the security and reliability of Medicaid Program data and the Agency's accountability over the Medicaid Program. Our findings are summarized below:

Finding No. 1: 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.

Finding No. 2: 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.

Finding No. 3: Some former contractor access privileges were not removed in a timely manner.

Finding No. 4: Generic user identifications (IDs) for database administration were being shared by contractor staff.

Finding No. 5: Certain access controls were deficient in the areas of user authentication, session controls, and logging of system activity.

Finding No. 6: Program and data change controls for FMMIS and DSS needed improvement.

Finding No. 7: Agency reconciliation documentation of FFMIS data with DSS data was incomplete and contained discrepancies, limiting the Agency's ability to demonstrate the accuracy and completeness of DSS data.

BACKGROUND

Medicaid is a partnership between the State and Federal Government to provide health coverage for selected categories of people with low incomes. The Agency is designated by Section 409.902, Florida Statutes, as the single State agency authorized to make Medicaid payments. EDS, as the fiscal agent for the State, uses FMMIS to enroll providers, process Medicaid claims, adjudicate claims, accept and process encounter claims for data collection, and reimburse providers. FMMIS data is imported into DSS to enable efficient reporting and data analysis. The Agency uses FMMIS and DSS for Medicaid Program oversight and analysis.

The Agency and EDS were each responsible for security administration functions for their respective users of FMMIS. Server operating system and database user account management was performed by EDS system and database administrators. EDS managed the development and promotion of FMMIS and DSS program changes using change control software.

FINDINGS AND RECOMMENDATIONS

The Medicaid Program is highly dependent on the security, integrity, and proper functioning of FMMIS and DSS to ensure the accurate payment of Medicaid benefits in accordance with Federal and State law and to facilitate timely and accurate reporting for Federal oversight purposes. According to Agency staff, approximately $14.4 billion in Medicaid benefits were processed in FMMIS during the 2008-09 fiscal year. In addition, FMMIS and DSS contain significant confidential information, including, for example, Medicaid recipient names, dates of birth, and medical services received. Given the importance of FMMIS and DSS to the Medicaid Program; the significance of the benefit payments processed therein; the extensive Federal Medicaid reporting requirements; and the need to capture, retain, and use confidential information in the administration of the Medicaid Program; effective IT controls over FMMIS and DSS are critical.

Our audit disclosed numerous instances where IT controls applicable to FMMIS and DSS were deficient or needed improvement as discussed in the following paragraphs.

Access Controls

Effective security controls include access controls that limit user access privileges to only the data and IT resources that are needed to perform authorized job duties. By restricting users from performing incompatible system functions, access controls help enforce an appropriate separation of incompatible duties.

Our audit disclosed that access controls within the FMMIS and DSS applications; databases; operating systems for the servers hosting FMMIS, DSS, and their respective databases; and program change management software needed strengthening as discussed in the following findings.

Finding No. 1: Access Control Documentation

Effective access controls include maintaining appropriate documentation of entity actions to authorize, establish, and monitor system access privileges. Examples of appropriate access control documentation include records of authorization of user access privileges requested, approved, and granted by applicable management or system owners; descriptions of user roles and the access privileges provided by the user roles; and documentation that correlates user roles with job functions.

Our audit disclosed that the Agency and EDS lacked appropriate access control documentation. Specifically, the Agency and EDS were unable, upon audit request, to provide documentation of:

- The various user roles within the FMMIS and DSS applications, server operating systems, and databases and the access privileges that each user role provided.
- 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.

- Authorization for the FMMIS and DSS user roles granted to the 52 EDS contractors included in our tests. In addition, the user roles granted to the 52 EDS contractors did not correspond to their job functions based on the guidelines in the Role Definition by Position document created by EDS.
- Authorization for the FMMIS and DSS user roles granted to 4 of the 5 Agency employees included in our tests.
- 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.
- Authorization for the access levels granted within the program change management software.

Absent the above-described documentation, the Agency and EDS could not demonstrate the business justification for access privileges granted within the FMMIS and DSS applications, server operating systems, database, and program change management software. These conditions limit the Agency's ability to control and monitor the appropriateness of access controls in protecting the confidentiality, integrity, and availability of data and IT resources.

Recommendation: 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.

Finding No. 2: Appropriateness of Access Privileges

As previously discussed, access controls include the assignment of system access privileges according to authorized job functions. Our audit disclosed instances where access privileges were inconsistent with employee or contractor job functions, increasing the risk of unauthorized disclosure, modification, and destruction of data and IT resources. Specifically:

- 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.
- 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.
- 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.
- 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.

Neither the Agency nor EDS performed periodic reviews of the appropriateness of access privileges within the applications, operating systems, database, or program change management 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.

Recommendation: 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.

Finding No. 3: Removal of Former Contractor Access Privileges

Effective access controls include provisions for timely removing or adjusting contractor access privileges when contract terminations and reassignments occur. Prompt action is necessary to ensure that access privileges are not misused by the former contractor or others.

The Agency had established policies for removing access privileges upon the termination or reassignment of contractors. However, our audit disclosed that, contrary to Agency policy, certain former or reassigned contractors retained access to the FMMIS and DSS server operating systems and databases after their dates of contract termination or reassignment. Specifically, as of the dates on which access privilege data was extracted for our testing:

- Five of 57 contractors included in our sample with server operating system access privileges retained server operating system privileges after their dates of termination or reassignment. In response to audit inquiry, Agency staff stated that 3 of the 5 contractors had been terminated or reassigned to other EDS projects. Agency staff could not determine the dates that the contractual services were terminated or reassigned or the length of time that the access privileges remained active after termination or reassignment. The remaining 2 contractors retained active operating system access privileges for 224 and 599 days, respectively, after their dates of termination.
- One of 22 database users included in our sample, a contractor, retained access privileges for 11 days after the date of contract termination.
- Three of 61 change control software users included in our sample were contractors who retained access privileges for 5, 25, and 37 days, respectively, after their dates of contract termination.

Under these conditions, the risk is increased that the access privileges could be misused by the former contractors or others. In response to audit inquiry, Agency staff indicated that the inappropriate access privileges noted above were removed.

Recommendation: The Agency should work with EDS to ensure that the access privileges of former contractors are promptly removed.

Finding No. 4: User Identification

The effectiveness of access controls is dependent, in part, on the ability to uniquely identify system users. Unique identification of individual users assists in the assignment of access privileges and provides a mechanism for attributing system actions to the responsible user.

Our audit disclosed that EDS used three generic user IDs for database administration. The generic user IDs were shared by two users. Database administration access privileges provide, among other capabilities, the capability to change data with utility software bypassing normal application edits and controls. Without the ability to uniquely identify database administrators, the ability of the Agency and EDS to establish accountability for database administration actions is limited.

Recommendation: The Agency should require EDS to assign unique user IDs to all individual users authorized to perform database administration functions for FMMIS and DSS.

Finding No. 5: Other Security Controls

Our audit disclosed certain access controls that were deficient in the areas of user authentication, session controls, and logging of system activity. We are not disclosing specific details of the deficiencies in this report to avoid the possibility of compromising the Agency's data and IT resources. However, we have notified appropriate Agency management of the specific deficiencies. Without adequate access controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Agency data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: 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.

Other IT Controls

Finding No. 6: Program and Data Change Controls

Effective controls over changes to application programs and data changes made by IT staff using database utility software rather than the FMMIS application are intended to ensure that only authorized and properly functioning changes are implemented. Program and data change controls include procedures to ensure that all changes are properly authorized, tested, approved for implementation, and documented. Additionally, an appropriate separation of duties with regard to program change controls includes provisions for the movement of programs into the production environment being controlled by persons independent of the programmer making the program changes.

Our audit disclosed aspects of the Agency's program and data change controls for FMMIS and DSS that needed improvement, increasing the risk that unauthorized or erroneous program and data changes could be implemented into the production environment. Specifically:

- 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.
- 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.
- 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.
- 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.

Additionally, our inspection of EDS program change management records for 27 FMMIS program changes disclosed instances where authorization for programming work, testing of program changes, and approval to implement

program changes either were not documented or were documented as having not been performed in an appropriate sequence. Specifically:

- According to Agency and EDS staff, Agency management authorization was required for program changes other than those to correct program defects. However, Agency management authorization was lacking for 7 of the 10 EDS program changes that were made for purposes other than correcting defects.
- Programmer testing was not documented for 6 EDS program changes.
- For 4 EDS changes, the dates that testing was completed preceded the dates that the program changes were coded.
- Agency policy provided that program changes were to be independently tested by EDS 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.
- 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 implementation.
- 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.

Recommendation: 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.

Finding No. 7: Reconciliations of FMMIS with DSS

User controls, such as reconciliations, are intended to ensure that data is processed as intended. The Agency performed weekly reconciliations of FMMIS data with DSS data to ensure the accuracy and completeness of information extracted from FMMIS and imported into DSS. In performing the reconciliations, the Agency used system-generated summary totals reports, including FMMIS Financial Balance Reports and DSS Claims Balance Reports, along with separate queries of DSS data and manually-prepared spreadsheets.

Our tests of Agency reconciliations of FMMIS data with DSS data for 13 weeks disclosed that Agency reconciliation documentation did not always demonstrate that FMMIS and DSS data totals were in agreement. In response to audit inquiry, Agency staff stated that there were inaccuracies in the DSS Claims Balance Reports utilized in the reconciliation process. Because of the report inaccuracies, the Agency relied on separate queries run against the DSS data and manually-prepared spreadsheets to assist in the reconciliation process. However, Agency reconciliation documentation provided upon audit request did not always include the separate query results or other system-generated totals and contained discrepancies. Although Agency staff provided explanations for the reconciliation differences noted in our tests, under these conditions, the Agency's ability to demonstrate the accuracy and completeness of DSS data is limited and the risk is increased that inaccurate or incomplete information in DSS, should it exist, will not be timely detected by the Agency.

Recommendation: 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.

OBJECTIVES, SCOPE, AND METHODOLOGY

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

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

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls relating to FMMIS and DSS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources. Additional objectives were to determine the effectiveness of selected Agency controls over the conversion and loading of historical data into FMMIS and the effectiveness of selected Agency controls over the loading of FMMIS data into DSS upon the change in Medicaid fiscal agent in June 2008.

The scope of our audit focused on evaluating selected IT controls applicable to FMMIS and DSS during the period October 2008 through April 2009 and selected actions through June 2009. Other aspects of FMMIS functionality will be addressed in our forthcoming audits of compliance with Federal laws, rules, and regulations and operational audits regarding selected Medicaid payment types.

In conducting our audit, we:

- Interviewed Agency and EDS personnel.
- Obtained an understanding of the Agency's and EDS's data conversion controls; program and data change controls; FMMIS, DSS, database, and operating system access and security controls, and FMMIS application controls.
- Observed, documented, and tested the effectiveness of selected controls over the conversion and loading of historical data into FMMIS.
- Observed, documented, and tested the effectiveness of selected controls over the loading of FMMIS data into DSS.
- Evaluated the appropriateness of selected controls surrounding the backup of FMMIS and DSS data.
- Observed, documented, and tested the effectiveness of selected logical access controls in ensuring that access to FMMIS and DSS applications, programs, databases, and operating systems were appropriately restricted.
- Observed, documented, and tested the effectiveness of selected controls over the authorization, testing, approval, and documentation of FMMIS and DSS application programs.
- Evaluated the effectiveness of selected controls over the authorization, testing, approval, and documentation of FMMIS and DSS data modifications.
- Evaluated the effectiveness of selected controls over the encryption of FMMIS and DSS data during selected transmissions and storage.
- Observed, documented, and tested the effectiveness of selected input and processing controls for FMMIS.

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 August 17, 2009, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

CHARLIE CRIST
GOVERNOR

Better Health Care for all Floridians

HOLLY BENSON
SECRETARY

August 17, 2009

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

Dear Mr. Martin:

Thank you for the opportunity to respond to the preliminary and tentative audit findings and recommendations from the Information Technology Audit of the Agency for Health Care Administration (Agency), Florida Medicaid Management Information System (FMMIS) and Decision Support System (DSS), for the period October 2008 through April 2009 and selected actions through June 2009. We appreciate the efforts of your staff and have included our response to the recommendation noted in your report. The Agency continuously looks for opportunities to improve operations and is committed to providing cost-effective and efficient health care services to the citizens of Florida.

In accordance with your request, we have emailed you the preliminary and tentative findings document with our response incorporated therein. If you have any questions regarding our response, please contact Mike Blackburn, Audit Director, at (850) 414-5419.

Sincerely,

Holly Benson
Secretary

HB/mb
Enclosure: Response to the P&T Information Technology Audit of FMMIS and DSS
cc: Carlton D. Snipes, Deputy Secretary for Medicaid
Alan Strowd, Bureau Chief, Medicaid Contract Management

2727 Mahan Drive • Mail Stop #1
Tallahassee, FL 32308

Visit AHCA online at
http://ahca.myflorida.com

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

CHARLIE CRIST
GOVERNOR

Better Health Care for all Floridians

HOLLY BENSON
SECRETARY

Agency for Health Care Administration
Response to Auditor General's P&T audit findings for the Information Technology Audit of the Agency for Health Care Administration, Florida Medicaid Management Information System (FMMIS) and Decision Support System (DSS), for the period October 2008 through April 2009 and selected actions through June 2009.

Finding No. 1: Access Control Documentation
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.

Recommendation:
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.

Agency Response:

- The various user roles within the FMMIS and DSS applications, server operating systems, and databases and the access privileges that each user role provided.

  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.

- 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.

  AHCA Response: As noted in the finding above, EDS created a Role Definition by Position to help guide the assignment of FMMIS/DSS user roles.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

- Authorization for the FMMIS and DSS user roles granted to the 52 EDS contractors included in our tests. In addition, the user roles granted to the 52 EDS contractors did not correspond to their job functions based on the guidelines in the Role Definition by Position document created by EDS.

  AHCA Response: In response to this audit and acknowledged in a memorandum dated April 23, 2009, EDS updated the Security Access forms and procedures to include a clear justification of the requested roles. However, it is important to note that even though a document was created to guide requesters and reviews in the basic roles for a particular 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.

- Authorization for the FMMIS and DSS user roles granted to 4 of the 5 Agency employees included in our tests.

  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.

- 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.

  AHCA Response: EDS has implemented a centralized location for all Security Request forms. The new centralized location is being maintained by the helpdesk.

- Authorization for the access levels granted within the program change management software.

  AHCA Response: EDS has refined the Security Request form and procedures. The form now requires a clarification for requested roles to include all Databases, Servers, and Applications.

Finding No 2: Appropriateness of Access Privileges
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.

Recommendation:
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.

Agency Response:

- 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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

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 exceptions are now being documented on the Security Request form within the business justification section.

- 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.

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 areas of responsibility follow these guidelines and documentation requirements.

- 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.

AHCA Response: July 27 2009, EDS removed the capability of Help Desk users to assign themselves as a System Administrator.

- Neither the Agency nor EDS performed periodic reviews of the appropriateness of access privileges within the applications, operating systems, database, or program change management 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.

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.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 3: Removal of Former Contractor Access Privileges
Some former contractor access privileges were not removed in a timely manner.

Recommendation:
The Agency should work with EDS to ensure that the access privileges of former contractors are promptly removed.

Agency 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.

Finding No.4: User Identification:
Generic user identifications (IDs) for database administration were being shared by contractor staff.

Recommendation:
The Agency should require EDS to assign unique IDs to all individual users authorized to perform database administration functions for FMMIS and DSS.

Agency Response:
It 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.

Finding No.5: Other Security Controls
Certain access controls were deficient in the areas of user authentication, session controls, and logging of system activity.

Recommendation:
The Agency should implement the appropriate access controls in the areas of user authentication, session controls, and logging of the system activity to ensure the continued confidentiality, integrity, and availability of Agency data and IT resources.

Agency 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.

Finding No.6: Program and Data Change Controls
Program and data change controls for FMMIS and DSS needed improvement.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation:

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.

Agency Response:

- 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.

  AHCA Response: Cycle Monitoring Procedures, the Customer Service Request (CSR) Process, and the CO Process documentation have been updated and can be found on iTrace.

- 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.

  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 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.

- 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.

  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.

- 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.

  AHCA Response: The Florida Interactive Portal (FIP) has been modified to prevent this from reoccurring. The defect CO type is no longer available.

- According to Agency and EDS staff, Agency management authorization was required for program changes other than those to correct program defects. However, Agency management authorization was lacking for 7 of the 10 EDS program changes that were made for purposes other than correcting defects.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

AHCA Response: The Change Order (CO) workflow has now been updated to ensure AHCA approval before a CO can be closed.

- Programmer testing was not documented for 6 EDS program changes.

  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.

- For 4 EDS changes, the dates that testing were completed proceeded the dates that the program changes were coded.

  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.

- Agency policy provided that program changes were to be independently tested by EDS 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.

  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 FMMIS have unique testing requirements regarding the code promotion. Therefore, not all COs will have Business Analyst testing.

- 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 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.

- 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.

  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 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.

Finding No. 7: Reconciliation of FMMIS with DSS

Agency reconciliation documentation of FFMIS data with DSS data was incomplete and contained discrepancies, limiting the Agency's ability to demonstrate the accuracy and completeness of DSS data.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation:
The Agency should address inaccuracies in the DSS Claims Balancing Reports and maintain appropriate documentation to demonstrate that complete reconciliations of FMMIS data with DSS data are performed.

Agency 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.

CDS/as