STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2017-093
January 2017

AGENCY FOR HEALTH CARE ADMINISTRATION

Fraud and Abuse Case Tracking System

Sherrill F. Norman, CPA
Auditor General

Secretary of Health Care Administration

The Agency for Health Care Administration is established by Section 20.42, Florida Statutes. The head of the Agency is the Secretary of Health Care Administration who is appointed by the Governor, subject to confirmation by the Senate. Elizabeth Dudek served as Secretary during the period of our audit.

The team leader was Arthur Wahl, CPA, CISA, and the audit was supervised by Tina Greene, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

AGENCY FOR HEALTH CARE ADMINISTRATION

Fraud and Abuse Case Tracking System

SUMMARY

This operational audit of the Agency for Health Care Administration (Agency) focused on evaluating selected information technology (IT) controls applicable to the Fraud and Abuse Case Tracking System (FACTS). Our audit disclosed the following:

Finding 1: The Agency's *Information Technology Security Plan* needs improvement to provide for comprehensive and current Agencywide security controls to protect the Agency's IT resources.

Finding 2: The Agency had not developed written security administration procedures for authorizing and assigning user access accounts to FACTS.

Finding 3: Complete and accurate FACTS access authorization documentation was not maintained thereby limiting management's assurance that FACTS user access privileges were authorized and appropriately assigned.

Finding 4: User access roles for FACTS were not adequately correlated to users' assigned job duties.

Finding 5: The access privileges for some FACTS users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for their assigned job duties.

Finding 6: The Agency had not established procedures for the periodic review of FACTS user access privileges and did not perform such periodic reviews.

Finding 7: The Agency did not timely deactivate the access privileges of FACTS user accounts for users who separated from Agency employment or transferred into positions that did not require access to FACTS.

Finding 8: Agency configuration management controls for FACTS need improvement to ensure that controls are in place to provide reasonable assurance that all configuration changes moved into the production environment follow an established configuration management process and are properly authorized, tested, and approved.

Finding 9: Certain security controls related to user authentication, logging, and access controls for FACTS and related IT resources need improvement to ensure the confidentiality, integrity, and availability of FACTS data and related IT resources.

BACKGROUND

The Agency for Health Care Administration (Agency) is responsible for, among other things, health facility licensure, inspection, and regulatory enforcement; investigation of consumer complaints related to health care facilities and managed care plans; and administration of the State's Medicaid Program.[1] The Office

[1] The State's Medicaid Program is a joint Federal and State-funded program that pays for health care services provided to recipients who meet the Program's eligibility criteria.

of Medicaid Program Integrity (MPI) audits and investigates providers suspected of overbilling or defrauding the State's Medicaid Program, recovers overpayments, issues administrative sanctions, and refers cases of suspected fraud for criminal investigation. The Agency contracted with Imager Software, Inc. (ISC) on April 17, 2014, to develop and maintain the Fraud and Abuse Case Tracking System (FACTS) which replaced an outdated case management system of the same name. FACTS was implemented in May 2015 and allows staff to track and manage the MPI work process from the time a complaint is recorded in the system to the time the related case is closed.

FINDINGS AND RECOMMENDATIONS

Finding 1: Information Security Program Plan

Agency for State Technology (AST) rules[2] require each agency to establish an information security program that includes information security policies, procedures, standards, and guidelines; an information security awareness program; an information security risk management process; a Computer Security Incident Response Team; and a disaster recovery program. Additionally, an information security program plan describes the controls that need to be in place or planned to meet the security requirements for an Agencywide information security program.

The Agency established an *Information Technology Security Plan* (*Plan*) with the stated purpose of ensuring that the security of the information and communication processing resources of the Agency was sufficient to minimize the risk of loss, theft, improper use, or unauthorized destruction, disclosure, or modification of the information and communication processing resources of the Agency. Our review of the *Plan* disclosed that although the *Plan* included a policy, standards, and directives and referenced a security awareness program and a disaster recovery program, the *Plan* did not include an information security risk management process. Additionally, the *Plan* did not describe the controls in place or planned to meet the security requirements for an Agencywide information security program. Furthermore, our review disclosed that the *Plan* had not been updated since March 23, 2010, or reviewed since April 19, 2010.

A comprehensive and current information security program plan that provides an overview of the security requirements for an Agencywide information security program and describes the controls in place or planned to meet those requirements provides a mechanism for the successful implementation of Agencywide security controls necessary to protect the Agency's IT resources.

Recommendation: We recommend that the Agency improve security controls that protect the Agency's IT resources by ensuring that the Agency's *Information Technology Security Plan* is kept current and includes an information security risk management process. Additionally, we recommend that the *Information Technology Security Plan* describe the controls in place or planned to meet the security requirements for the Agencywide information security program.

[2] AST Rule 74-2.002(1)(f)8.c., Florida Administrative Code. Although AST Rules were not effective until March 10, 2016, rules promulgated by the Agency for Enterprise Information Technology (AEIT), AST's predecessor agency, included similar requirements. Specifically, AEIT Rule 71A-1.003(1) and (3), Florida Administrative Code.

Finding 2: Security Administration Procedures

Security standards, guidelines, and procedures are developed to provide users, managers, and others a method for implementing security policies and meeting organizational goals. Standards and guidelines specify technologies and methodologies to be used to secure systems, and procedures provide details regarding how to implement the security policies, standards, and guidelines. Procedures are the detailed steps to be followed to accomplish particular security-related tasks such as security administration procedures for assigning appropriate access privileges. Effective security control policies and procedures are documented and approved by management, periodically reviewed and updated, and ensure that users can be held accountable for their actions.

Our audit procedures disclosed that the Agency had not developed documented and approved security administration procedures for authorizing and assigning user access accounts to FACTS. In response to our audit inquiry regarding security administration procedures, Agency management indicated that there were no written security administration procedures for FACTS. Agency management did provide a document for our review that addressed FACTS access; however, that document only specified who to notify for new hires, separations, and changes in group assignments related to FACTS users.

Without documented and approved security administration procedures for authorizing and assigning user access accounts to FACTS, there is no assurance that the Agency is appropriately controlling access privileges to FACTS according to management's expectations.

Recommendation: We recommend that Agency management develop documented and approved security administration procedures for authorizing and assigning user access accounts to FACTS to ensure that access privileges granted are appropriately controlled according to management's expectations.

Finding 3: Access Authorization Documentation

Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. Additionally, appropriately maintained access authorization documentation facilitates the complete and accurate assignment of user access privileges. AST rules[3] require each agency to manage identities and credentials for authorized devices and to implement control measures that, at a minimum, address responsibilities of information stewards, including responsibilities for administering access to systems and data based on documented authorizations.

As part of our audit, we requested access authorization documentation for 16 of the 162 FACTS users with active access privileges as of April 12, 2016, to determine whether the access privileges granted were authorized and appropriately assigned. Agency management indicated that separate access authorization forms were not used for authorizing FACTS access privileges. We also requested network access authorization documentation for the 16 selected FACTS users to determine whether any FACTS access privileges were specified in the network access authorization documentation. In response to our

[3] AST Rule 74-2.003(1)(a)6., Florida Administrative Code. Although AST Rules were not effective until March 10, 2016, AEIT Rule 71A-1.007(1), Florida Administrative Code, required agency owners to be responsible for authorizing access to information.

audit request, Agency staff were only able to provide network access authorization documentation for 10 of the 16 FACTS users and the network access authorization documentation provided did not authorize the level of FACTS access privileges granted. Therefore, without appropriate documentation authorizing FACTS access privileges, we could not determine whether the access privileges granted to the 16 FACTS users were authorized and appropriately assigned.

Use of access authorization documentation provides evidence demonstrating that access privileges for FACTS and the network are authorized and appropriately assigned.

Recommendation: We recommend that Agency management use access authorization forms to document authorized user access privileges granted to FACTS and the network.

Finding 4: Access Control Alignment

Effective access controls include limiting access privileges to individuals with a valid business purpose. Computer resource owners should identify the specific user or class of users authorized to obtain direct access to each resource for which they are responsible. This process can be simplified by developing standard roles that describe access needs for groups of users with similar duties. The effectiveness of access controls is enhanced by correlating access roles with specified job duties.

Our audit procedures disclosed that the user access roles for FACTS were not adequately correlated to users' assigned job duties. The Agency was using four user access roles for FACTS: standard administrator, AHCA administrator, standard user, and standard viewer. However, the access roles were not defined to a granular level to restrict user access privileges to only what the user needed to perform his or her assigned job duties.

Detailed access roles that are based on users' needs decrease the risk that users may inappropriately gain access to confidential data or make unauthorized changes to FACTS data.

Recommendation: We recommend that the Agency develop FACTS user roles that reflect the required level of FACTS access privileges based on users' assigned job duties.

Finding 5: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure. FACTS user access roles were used to group and control access privileges to FACTS. The four FACTS user access roles included standard user, standard viewer, standard administrator, and AHCA administrator.

Through our audit procedures related to access control alignment noted in Finding 4, we determined that the FACTS standard user access role erroneously provided users inappropriate update access privileges to security administrative functions. As of April 12, 2016, there were 127 FACTS users assigned the standard user role and, therefore, had excessive and inappropriate update access privileges to perform security functions.

Our evaluation of 71 of the 162 FACTS users with active access privileges as of April 12, 2016, disclosed that all 71 users had inappropriate access privileges, excessive access privileges, incorrect role assignments, or role assignments that allowed the performance of incompatible duties as shown in Table 1.

Table 1

Number of FACTS Users with Inappropriate FACTS Access Privileges by Access Role

	Access Role				
Category	**Standard User**	**Standard Viewer**	**Standard Administrator**	**AHCA Administrator**	**Category Totals**
Inappropriate – no business need for access	8	10	2	-	**20**
Correct role assigned, but role provided excessive access privileges	11	2	-	12	**25**
Incorrect role assigned	17	-	5	2	**24**
Performing incompatible duties using role	-	-	2	-	**2**
Total Number of FACTS Users by Role	**36**	**12**	**9**	**14**	**71**

In response to our audit inquiries, Agency management indicated that a programming change was implemented on May 27, 2016, to correct the access privileges assigned to the standard user role. The existence of inappropriate and unnecessary user access privileges increases the risk that unauthorized modification, loss, or disclosure of FACTS data may occur.

Recommendation: We recommend that Agency management limit user access privileges to FACTS to promote an appropriate separation of duties and to restrict users to only those user access privileges and functions necessary for the users' assigned job duties.

Finding 6: Periodic Review of User Access Privileges

AST rules[4] require periodic review of access rights (privileges) with information owners based on system categorization or assessed risk. Our audit procedures disclosed that the Agency had not established procedures for, and did not perform, periodic reviews of FACTS user access privileges. In response to our audit inquiry, Agency management indicated that procedures had not been established and the Agency did not perform periodic reviews of FACTS user access privileges because FACTS was a new system and the FACTS security administrator had changed after FACTS implementation.

Periodic reviews of FACTS user access privileges help provide management assurance that user access privileges were authorized and appropriate.

Recommendation: We recommend that Agency management establish and implement procedures for the periodic review of FACTS user access privileges to ensure that FACTS user access privileges are authorized and remain appropriate.

[4] AST Rule 74-2.003(1)(a)6., Florida Administrative Code. Although AST Rules were not effective until March 10, 2016, AEIT Rule 71A-1.007(2), Florida Administrative Code, required agency owners to review access rights periodically based on risk, access account change activity, and error rate.

Finding 7: Timely Deactivation of Access Privileges

AST rules[5] require that each agency shall manage identities and credentials for authorized devices and users and that control measures shall, at a minimum, ensure IT access is removed when the IT resource is no longer required. Prompt action is necessary to ensure that former users or others do not misuse the former users' access privileges.

Our review disclosed that the Agency did not timely deactivate FACTS user accounts when users separated from Agency employment or transferred to positions that no longer required access to FACTS. Specifically:

- Our examination of the 20 FACTS user accounts for users who separated from Agency employment during the period July 1, 2015, through May 5, 2016, and were listed on the FACTS users access list as of March 30, 2016, (active and inactive user accounts) disclosed that 10 of the user accounts had FACTS access privileges that were not timely deactivated upon the users' separation from Agency employment. Nine of the 10 user accounts were deactivated but had remained active from 16 to 136 days after the users' separation dates. The remaining user account was in an active status although, as of May 12, 2016, 243 days had elapsed since the user's separation date.
- Our examination of 1 FACTS user account for a user who had transferred from the Agency's Office of MPI to another position within the Agency disclosed that, as of May 24, 2016, the user account had remained active for 46 days after the user's transfer date.
- Our audit procedures also disclosed that, prior to providing us the list of FACTS users as of March 30, 2016, Agency management removed 23 user accounts. These accounts were for users who had separated employment with the Agency or transferred to another position. Our evaluation of the 23 user accounts as of May 12, 2016, disclosed that 21 of the user accounts were deactivated from 60 to 409 days after the users separated from Agency employment or transferred to a position that did not require FACTS access privileges. The remaining 2 user accounts were vendor accounts and Agency records did not evidence when the 2 vendors' user accounts became unnecessary. However, the last modified date for the 2 vendor accounts prior to being deactivated was February 11, 2015.

Although we requested documentation to evidence whether any of the FACTS user accounts that were not timely deactivated were used subsequent to the dates the users separated from Agency employment or no longer needed access privileges, Agency staff did not respond to our request. Accordingly, a determination regarding any subsequent use of the FACTS user accounts could not be made.

Without the timely deactivation of FACTS user accounts for users who separate employment with the Agency or transfer to another position within the Agency that does not require FACTS access privileges, the risk is increased that the user accounts may be misused by former employees or others.

Recommendation: We recommend that Agency management ensure that FACTS user account access privileges of former users are timely deactivated to prevent former users or others from misusing the access privileges.

[5] AST Rule 74-2.003(1)(a)8., Florida Administrative Code. Although AST Rules were not effective until March 10, 2016, AEIT Rule 71A-1.007(6), Florida Administrative Code, required that access authorization be promptly removed when the user's employment is terminated or access to the information is no longer required.

Finding 8: Configuration Management Controls

Effective configuration management controls ensure that all configuration changes (program or functionality changes) follow a configuration management process such that configuration changes are appropriately authorized, tested, and approved prior to movement into the production environment. Additionally, the effectiveness of configuration management controls is enhanced by controls that ensure the configuration management process is followed when configuration changes are moved into the production environment.

The Agency's change management policy[6] defines the process for managing changes to information systems on the Agency's network. The policy requires communication among Agency IT staff, vendors, users, and departmental administrators regarding changes to production information systems. It also requires staff to follow a common process for logging, reviewing, approving, and documenting the existence, state, and outcome of material changes to information systems. The change management policy indicates that it is applicable to all Agency employees, contractors, consultants, temporary employees, and other workers including all personnel affiliated with third parties participating in Agency IT system maintenance or system development and also applies to all individuals who install, operate, or maintain the Agency's information technology.

To determine whether the Agency was using an appropriate change management process for FACTS, we examined the 11 FACTS configuration changes (workflow process changes) moved into the production environment during the period July 1, 2015, through April 6, 2016. In response to our audit request, the Agency was unable to provide documentation to evidence that the 11 FACTS configuration changes had been appropriately authorized, tested, or approved prior to movement into the production environment by the appropriate end-user functional area. Additionally, the Agency was unable to provide documentation to evidence the 11 FACTS configuration changes were moved into the production environment by someone other than the programmer who developed the configuration changes. In response to our audit inquiry, Agency management stated that the 11 FACTS configuration changes were considered workflow process changes and therefore did not follow the Agency's change management policy.

Absent controls to ensure that all configuration changes follow the Agency's configuration management process, management has limited assurance that FACTS configuration changes moved into the production environment had been appropriately authorized, tested, and approved.

Recommendation: We recommend that Agency management ensure that controls are in place to provide reasonable assurance that all configuration changes that are moved into the production environment follow an established configuration management process and are properly authorized, tested, and approved.

Finding 9: Security Controls – User Authentication, Logging, and Access Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to user authentication,

[6] *Information Technology Change Management Policy #09-IT-03.*

logging, and access controls need improvement. We are not disclosing the specific details of the issues in this report to avoid the possibility of compromising FACTS data and related IT resources. However, we have notified appropriate Agency management of the specific issues.

Without appropriate security controls related to user authentication, logging, and access controls, the risk is increased that the confidentiality, integrity, and availability of FACTS data and related IT resources may be compromised.

Recommendation: We recommend that Agency management improve certain security controls related to user authentication, logging, and access controls to ensure the confidentiality, integrity, and availability of FACTS data and related IT resources.

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 2016 through May 2016 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to FACTS during the period July 2015 through May 2016 and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input, processing, and output and selected application-level general controls applicable to FACTS. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls 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.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of this audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of the audit; obtaining an

understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed Agency personnel and reviewed FACTS-related documentation to obtain an understanding of:
  - The organizational structure and related job duties, responsibilities, and activities of the Office of Inspector General including the Office of Medicaid Program Integrity (MPI).
  - The FACTS data and business process flows, including key sources of data input, including interfaces; key application transactions and processes; and key types of application data output related to FACTS.
  - The FACTS computing platform, including the applicable hardware; operating system; database management system; and security software.
  - The Agency's information security program plan, security administration procedures, and user account management processes for authorizing, creating, modifying, and revoking access to FACTS.
  - The Agency's configuration management processes applicable to FACTS.
- Evaluated 19 of the 183 final orders related to Medicaid sanctioned providers with the "Default and Dismissals" order type rendered during the period July 1, 2015, through June 30, 2016, to determine who, prior to the Agency Secretary's approval, was performing management and decision-making functions related to sanctions imposed for Medicaid providers.
- Evaluated FACTS business process application controls related to data input and interfaces, processing, and output. Specifically, we:
  - Determined the effectiveness of seven significant control processes in FACTS as of April 28, 2016, May 16, 2016, and May 20, 2016, by observing:
    - On May 20, 2016, three drop-down boxes on the Financials screen for type, code, and sanction type edits.
    - On May 20, 2016, an example of a transaction log after a change was made on the Financials screen.
    - On April 28, 2016, an example of the error message that was received when an unauthorized person attempted to approve a formal communication.
    - On April 28, 2016, an example of the supervisory notification that was generated when a case was closed.

        - On May 11, 2016, an example of the warning message that was displayed when attempting to submit a case for a provider with a currently open case.
    - Observed Agency staff navigate through FACTS on April 7, 2016, and examined the input controls on the journal entry cases and complaints entry, complaint approval, and audit trail screens.
    - As of April 6, 2016, and April 8, 2016, inspected FACTS interface screen prints of the Interface Transmitted Report Log and the automatic message sent to database administrators when a file fails to load to determine whether procedures were in place to ensure that interfaces are processed accurately, completely, and timely.
    - On May 20, 2016, and May 25, 2016, reviewed spreadsheets used to track FACTS cases outside the FACTS application.
    - Observed Agency staff navigate through FACTS on May 10, 2016, and examined processing controls on the audit trail and complaint approval screens.
    - Inspected user listing and role descriptions on April 12, 2016, to determine whether access to output reports was based on business needs.
    - On April 18, 2016, inspected a list of 32 reports produced by FACTS that were deemed significant by the Agency.
- Inquired of vendor staff to determine whether there was a record of disposition for 128 of the 150 complaint and 91 case numbers that were missing for the period July 1, 2015, through April 29, 2016.
- Evaluated the effectiveness of FACTS application access authorization controls for 16 of the 162 users with active FACTS access privileges as of April 12, 2016.
- Conducted inquiries with Agency staff to determine whether the Agency had procedures for periodically reviewing the appropriateness of FACTS access privileges.
- Evaluated the effectiveness of selected access controls related to access privileges for FACTS and supporting IT resources. Specifically, we:
    - Observed a demonstration of the access capabilities to identify any vulnerabilities of the assigned FACTS user roles as of April 12, 2016.
    - Evaluated the appropriateness of the access privileges granted for 71 of the 162 users with active FACTS access privileges as of April 12, 2016.
    - Evaluated whether, as of May 17, 2016, 4 domain accounts in the Administrators group on the FACTS production database server and 5 domain account in the Administrators group on the FACTS production application server were appropriately restricted.
    - To determine the effectiveness of Agency controls over deactivating user access privileges, examined the 20 FACTS user accounts for users who separated from Agency employment during the period July 1, 2015, through May 5, 2016, and were listed on the FACTS users access list as of March 30, 2016, (active and inactive user accounts), as well as the 23 FACTS user accounts that Agency management removed from the March 30, 2016, users access list provided to us.
    - Examined the 1 FACTS user account for a user who had transferred from the Office of MPI to another Agency position.
- Evaluated user authentication controls for FACTS and the related IT resources.
- Evaluated the effectiveness of logging and monitoring controls related to FACTS IT resources.

- Evaluated the effectiveness of FACTS configuration management controls related to the authorization, testing, approval, and implementation of configuration changes into the production environment. Specifically, we evaluated the 11 configuration changes that were implemented into the production environment during the period July 1, 2015, through April 6, 2016, to determine whether the selected FACTS changes were appropriately authorized, tested, approved, and appropriately implemented into the production environment.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. 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.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

RICK SCOTT
GOVERNOR

JUSTIN M. SENIOR
INTERIM SECRETARY

January 5, 2017

Ms. Sherrill F. Norman, CPA
Auditor General
Claude Denson Pepper Building, Suite G74
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Thank you for the opportunity to respond to the preliminary and tentative findings and recommendations from your information technology operational audit of the Agency for Health Care Administration Fraud and Abuse Case Tracking System. In accordance with your request, we have emailed you the preliminary and tentative audit findings document with our response incorporated therein.

If you have any questions regarding our response, please contact Mary Beth Sheffield at 412-3978.

Sincerely,

Justin M. Senior
Interim Secretary

JMS/szg
Enclosure

2727 Mahan Drive • Mail Stop #1
Tallahassee, FL 32308
AHCA.MyFlorida.com

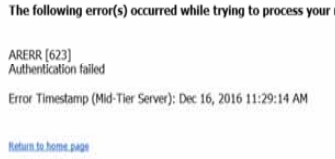
Facebook.com/AHCAFlorida
Youtube.com/AHCAFlorida
Twitter.com/AHCA_FL
SlideShare.net/AHCAFlorida

Florida Agency for Health Care Administration
Auditor General FY 2015-16 IT Operational Audit - FACTS
Response to Preliminary and Tentative Audit Findings and Recommendations

Finding#1	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Information Security Program Plan The Agency's Information Technology Security Plan needs improvement to provide for comprehensive and current Agencywide security controls to protect the Agency's IT resources.	We recommend that the Agency improve security controls that protect the Agency's IT resources by ensuring that the Agency's *Information Technology Security Plan* is kept current and includes an information security risk management process. Additionally, we recommend that the *Information Technology Security Plan* describe the controls in place or planned to meet the security requirements for the Agencywide information security program.	The AHCA Division of IT will update the Information Technology Security Plan (ITSP).	March 1, 2017	Karen Calhoun (850) 412-4849

Florida Agency for Health Care Administration
Auditor General FY 2015-16 IT Operational Audit - FACTS
Response to Preliminary and Tentative Audit Findings and Recommendations

Finding#2	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Security Administration Procedures The Agency had not developed written security administration procedures for authorizing and assigning user access accounts to FACTS.	We recommend that Agency management develop documented and approved security administration procedures for authorizing and assigning user access accounts to FACTS to ensure that access privileges granted are appropriately controlled according to management's expectations.	The Agency's Bureau of Medicaid Program Integrity (MPI) currently has written procedures in place but will develop written FACTS access management policies for authorizing and assigning user access accounts to FACTS.	July 1, 2017	Shannon Bagenholm (850) 412-4645 Ken Yon (850) 412-4637

Finding#3	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Access Authorization Documentation Complete and accurate FACTS access authorization documentation was not maintained thereby limiting management's assurance that FACTS user access privileges were authorized and appropriately assigned.	We recommend that Agency management use access authorization forms to document authorized user access privileges granted to FACTS and the network.	Access to the FACTS system is controlled by general network access. Network access is controlled by network authorization forms. Additionally, roles must be granted within the FACTS application itself. Users who have no roles within the system are met with the following error:  The following error(s) occurred while trying to process your request: ARERR [623] Authentication failed Error Timestamp (Mid-Tier Server): Dec 16, 2016 11:29:14 AM Return to home page AHCA will explore further access restriction options. See response to Finding #2. MPI will incorporate policies on maintaining user authorization and access to FACTS access management policies.	July 1, 2017 July 1, 2017	Karen Calhoun (850) 412-4849 Shannon Bagenholm (850) 412-4645 Ken Yon (850) 412-4637

Finding#4	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Access Control Alignment User access roles for FACTS were not adequately correlated to users' assigned job duties.	We recommend that the Agency develop FACTS user roles that reflect the required level of FACTS access privileges based on users' assigned job duties.	See response to Finding #2. MPI will incorporate adequate correlation of user access roles to users' assigned job duties in the FACTS access management policies.	July 1, 2017	Shannon Bagenholm (850) 412-4645 Ken Yon (850) 412-4637

Finding#5	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Appropriateness of Access Privileges The access privileges for some FACTS users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for their assigned job duties.	We recommend that Agency management limit user access privileges to FACTS to promote an appropriate separation of duties and to restrict users to only those user access privileges and functions necessary for the users' assigned job duties.	See response to Finding #2. MPI will define the appropriateness of user access privileges and roles in the FACTS access management policies.	July 1, 2017	Shannon Bagenholm (850) 412-4645 Ken Yon (850) 412-4637

Florida Agency for Health Care Administration
Auditor General FY 2015-16 IT Operational Audit - FACTS
Response to Preliminary and Tentative Audit Findings and Recommendations

Finding#6	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Periodic Review of User Access Privileges The Agency had not established procedures for the periodic review of FACTS user access privileges and did not perform such periodic reviews.	We recommend that Agency management establish and implement procedures for the periodic review of FACTS user access privileges to ensure that FACTS user access privileges are authorized and remain appropriate.	The updated ITSP will address periodic reviews. See response to Finding #2. MPI is actively performing periodic reviews of FACTS user access privileges. MPI will incorporate the periodic review of FACTS user access privileges in the FACTS access management policies.	March 1, 2017 July 1, 2017	Karen Calhoun (850) 412-4849 Shannon Bagenholm (850) 412-4645 Ken Yon (850) 412-4637

Finding#7	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Timely Deactivation of Access Privileges The Agency did not timely deactivate the access privileges of FACTS user accounts for users who separated from Agency employment or transferred into positions that did not require access to FACTS.	We recommend that Agency management ensure that FACTS user account access privileges of former users are timely deactivated to prevent former users or others from misusing the access privileges.	See response to Finding #2. MPI will address the timely deactivation of user access privileges in the FACTS access management policies.	July 1, 2017	Shannon Bagenholm (850) 412-4645 Ken Yon (850) 412-4637

Florida Agency for Health Care Administration
Auditor General FY 2015-16 IT Operational Audit - FACTS
Response to Preliminary and Tentative Audit Findings and Recommendations

Finding#8	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Configuration Management Controls Agency configuration management controls for FACTS need improvement to ensure that controls are in place to provide reasonable assurance that all configuration changes moved into the production environment follow an established configuration management process and are properly authorized, tested, and approved.	We recommend that Agency management ensure that controls are in place to provide reasonable assurance that all configuration changes that are moved into the production environment follow an established configuration management process and are properly authorized, tested, and approved.	The Division of IT will revise its Change Control Process policy and procedures to address Software-as-a-Service (SaaS) solution needs. MPI will refer to the response provided by IT.	July 1, 2017	Karen Calhoun (850) 412-4849 Shannon Bagenholm (850) 412-4645 Ken Yon (850) 412-4637

Florida Agency for Health Care Administration
Auditor General FY 2015-16 IT Operational Audit - FACTS
Response to Preliminary and Tentative Audit Findings and Recommendations

Finding#9	Recommendation	Agency Response	Anticipated Completion Date	Agency Contact
Security Controls – User Authentication, Logging, and Access Controls Certain security controls related to user authentication, logging, and access controls for FACTS and related IT resources need improvement to ensure the confidentiality, integrity, and availability of FACTS data and related IT resources.	We recommend that Agency management improve certain security controls related to user authentication, logging, and access controls to ensure the confidentiality, integrity, and availability of FACTS data and related IT resources.	The Agency will improve certain security controls as identified in the recommendation. MPI will refer to the response provided by IT.	July 1, 2017	Karen Calhoun (850) 412-4849 Shannon Bagenholm (850) 412-4645 Ken Yon (850) 412-4637