REPORT NO. 2015-023
OCTOBER 2014

DEPARTMENT OF CHILDREN AND FAMILIES

GRANTS AND OTHER REVENUE ALLOCATION AND TRACKING SYSTEM (GRANTS)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF CHILDREN AND FAMILIES

The Department of Children and Families is established by Section 20.19, Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. During the period of our audit, the following individuals served as Department Secretary:

Michael Carroll, Interim	From May 5, 2014
Esther Jacobo, Interim	From July 19, 2013, through May 2, 2014
David Wilkins	Through July 18, 2013

The audit team leader was William Tuck, 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 can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF CHILDREN AND FAMILIES

Grants and Other Revenue Allocation and Tracking System (GRANTS)

SUMMARY

The Department of Children and Families' (Department) Grants and Other Revenue Allocation and Tracking System (GRANTS) captures and sorts data from the State's accounting system, the Florida Accounting Information Resource Subsystem (FLAIR), to allocate expenditures to funding sources, calculate Federal reimbursements, and perform other financial activities. The Department's Office of Revenue Management, organizationally under the Chief Financial Officer who reports organizationally to the Assistant Secretary for Administration, utilizes GRANTS to collect and report data for all revenue sources used by the Department and to provide detailed analysis of grant activity, cost allocation, and cash management information. GRANTS supplies data used to compile Departmentwide reports required by the Federal Government, including the annual Schedule of Expenditures of Federal Awards.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to GRANTS. We also determined the status of corrective actions regarding audit findings included in our report No. 2007-200 that were applicable to the scope of this audit. Corrective actions were not taken for two of four applicable prior audit findings included in our prior report. In addition, another two of the four applicable prior audit findings were only partially corrected. One prior audit finding included in our report No. 2007-200 was not in the scope of this audit.

Our audit disclosed areas in which improvements in GRANTS IT controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: Certain GRANTS policies and procedures had not been established and other documentation needed improvement.

Finding No. 2: The Department did not timely deactivate the GRANTS-related access privileges of three former IT employees and two former IT contractors subsequent to the dates of termination of their employment or contracts.

Finding No. 3: Certain security controls related to user authentication, monitoring, and logging for GRANTS needed improvement.

Finding No. 4: Contrary to Section 119.071(5)(a)2.a., Florida Statutes, the Department collected and used certain social security numbers (SSNs) in GRANTS without specific authorization in law or without having established the imperative need to use the SSNs for the performance of its duties and responsibilities as prescribed by law.

Finding No. 5: The Department had not established data categorization policies and procedures and had not categorized its data in accordance with Federal Information Processing Standards Publication (FIPS PUB) 199, contrary to Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-2.001(3)(l), Florida Administrative Code.

BACKGROUND

GRANTS provides Department management with current financial information regarding cash and revenue. GRANTS was designed to capture Florida Accounting Information Resource Subsystem (FLAIR) accounting data, process the expenditures and revenues, assign them to the appropriate grant, and generate the appropriate reports for monitoring and development of Federal reports. GRANTS calculates indirect costs; allocates expenditures between

[1] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, in effect as of November 15, 2010; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.

Federal and State percentages, maintenance of effort, and matching; and prepares data processing billings and Federal draw requests from the FLAIR master file balances.

The primary flow of data within GRANTS starts with the FLAIR master and detail title and subsidiary information files processed through tables maintained in GRANTS. The table information is loaded into GRANTS from FLAIR and maintained by the users through on-line screens within GRANTS. Two other sources of transactional data are data processing billings from the Data Processing Cost Allocation System and manual adjustments through the Automated Manual Adjustment Processor application. The State Chief Financial Officer (CFO) State Accounts Master Balance file, which contains official Department cash activities based on State CFO records, is also appended to GRANTS.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Policies, Procedures, and Other Documentation

Effective management includes the establishment of policies and procedures that describe management's expectations for controlling Department operations. Written policies and procedures and other documentation, such as training materials and manuals, help ensure that management directives are clearly communicated, understood, accepted, and followed by staff.

As similarly noted in our report No. 2007-200, our review disclosed that certain GRANTS policies and procedures had not been established and other documentation needed improvement. Specifically:

- The Department had not established policies and procedures for software and firmware updates related to GRANTS to ensure that current, supported versions of the software and firmware were being used.
- There were several error and exception reports available for review to identify errors and exceptions, including invalid earnings reports, processing error reports, data relationship reports, and reconciliation reports. However, there were no procedures established requiring a timely review of the error and exception reports. According to Department management, the error and exception reports were not being reviewed or followed up on by Department staff.
- The Department had not established user training procedures and related documentation for GRANTS.
- The *GRANTS User Manual* was not up to date. For example, it did not reflect current GRANTS processing procedures for billing or GRANTS reporting capabilities.

Without written policies, procedures, and updated documentation, the risk is increased that tasks related to the above areas will not be carried out consistently and in a manner pursuant to management's expectations.

Recommendation: The Department should establish GRANTS policies and procedures for software and firmware updates and error and exception reports. Additionally, the Department should establish GRANTS user training procedures and related documentation and should ensure that the *GRANTS User Manual* is up to date and reflects current processing procedures and reporting capabilities for GRANTS.

Finding No. 2: Timely Deactivation of Access Privileges

Effective IT access controls include provisions for the timely deactivation of former employees' and contractors' access privileges to ensure that the access privileges are not misused by former employees, contractors, or others. Our audit disclosed that the Department did not timely deactivate the GRANTS-related access privileges of some former IT employees and IT contractors. Specifically, we noted the following:

- Access privileges that allowed inquiry access to the GRANTS application for one former IT employee were still active 1,005 days after her employment termination date. The Department had not retained documentation of the last logon date and was, therefore, unable to determine whether the access privileges of this employee were used after her employment termination date.

- Although Department management indicated that the domain user accounts of two former IT employees and two former IT contractors were disabled, the disabled domain user accounts were not removed from active access control groups with update access to either the application server or the database or both between 710 and 1,562 days after their employment termination and contract termination dates. Department management indicated that the access privileges of the former IT employees and IT contractors had not been used subsequent to their dates of employment terminations and contract terminations. However, if the disabled domain user accounts were to be reactivated, the users assigned to the reactivated domain user accounts would inherit the update access privileges to the application server or the database. As a result, the inherited access privileges may not be appropriate for the job duties of the users assigned to the reactivated domain user accounts.

Without the timely deactivation of former employees' and contractors' GRANTS-related access privileges and timely removal from active access control groups, the risk is increased that the access privileges may be misused by the former employees, contractors, or others to inappropriately disclose or make changes to GRANTS data and related IT resources.

Recommendation: The Department should ensure that the GRANTS-related access privileges of former employees and contractors are timely deactivated and removed from active access control groups.

Finding No. 3: Security Controls – User Authentication, Monitoring, and Logging

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit disclosed certain security controls related to user authentication, monitoring, and logging for GRANTS that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising GRANTS data and related IT resources. However, we have notified appropriate Department management of the specific issues. Similar issues were communicated to Department management in connection with our report No. 2007-200. Without adequate security controls related to user authentication, monitoring, and logging, the risk is increased that the confidentiality, integrity, and availability of GRANTS data and related IT resources may be compromised.

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

Finding No. 4: Use of Social Security Numbers (SSNs)

Section 119.071(4)(a), Florida Statutes, provides that all employee SSNs held by an agency are confidential and exempt from public inspection. Pursuant to Section 119.071(5)(a)2.a., Florida Statutes, an agency may not collect an individual's SSN unless the agency has stated in writing the purpose for its collection and unless the agency is specifically authorized by law to do so or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law.

As previously communicated in our report No. 2007-200, the Department collected and used certain SSNs in GRANTS. No specific authorization existed in law for the Department to collect the SSNs of GRANTS users and the Department had not established the imperative need to use the SSNs rather than another number. The use of the SSNs is contrary to State law and increases the risk of improper disclosure of SSNs.

Recommendation: In the absence of establishing an imperative need for the use of SSNs, the Department should comply with State law by establishing another number to be used in GRANTS rather than SSNs.

Finding No. 5: Data Categorization

AEIT Rule 71A-2.001(3)(l) and 71A-1.020(1), Florida Administrative Code, provides that agencies shall categorize all information and information systems in accordance with Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to estimate the magnitude of harm that would result from unauthorized access, unauthorized modification or destruction, or loss of availability of a resource. FIPS PUB 199 establishes security categories for both information and information systems.

Our review disclosed that the Department's IT risk management activities needed improvement with regard to categorizing IT resources. The Department had not established data categorization policies and procedures and had not categorized its data based on an assessment of the potential impact of a loss of confidentiality, integrity, or availability, contrary to FIPS PUB 199. Under these conditions, the risk is increased that unmitigated vulnerabilities may result that could impact the operations of the Department and the confidentiality, integrity, or availability of Department data and IT resources.

Recommendation: The Department should establish data categorization policies and procedures and categorize its data.

PRIOR AUDIT FOLLOW-UP

The Department had not taken corrective actions for two of the four prior audit findings included in our report No. 2007-200 that were applicable to the scope of this audit as described in the findings above. In addition, another two of the four applicable prior audit findings were only partially corrected. One prior audit finding included in our report No. 2007-200 was not in the scope of this audit.

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 April 2014 through June 2014 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls 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. An additional objective was to determine whether the Department had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2007-200 that were within the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to GRANTS during the period July 2013 through June 2014 and selected actions through August 25, 2014. The audit included selected application IT controls (including selected input, processing, and output controls) relevant to GRANTS and selected application-level general IT controls over security management, logical access to programs and data, and systems modification.

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 and IT controls and instances of noncompliance with applicable governing laws, rules, or contracts. 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 our 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 our 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 our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our 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 our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the key sources of data (internal and external) and related process flows that ensure the completeness, accuracy, validity, and confidentiality of data input into GRANTS.
- Obtained an understanding of the key transaction processing processes that ensure the completeness, accuracy, validity, and confidentiality of data processed in GRANTS.
- Obtained an understanding of the key types of data output and related processes that ensure the completeness, accuracy, validity, and confidentiality of outputs from GRANTS.
- Obtained an understanding of the changes to GRANTS, policies and procedures, or organizational structure.
- Evaluated the effectiveness of GRANTS transaction data input as of May 9, 2014, to determine if transaction data input was complete, accurate, valid, and confidential. Specifically, we obtained copies of reports and production examples to evaluate the effectiveness of data input.

- Evaluated the effectiveness of GRANTS transaction data processing as of May 21, 27, and 30, 2014, to determine if transaction data processing was complete, accurate, valid, and confidential. Specifically, we obtained copies of reports and production examples to evaluate the effectiveness of data processing.
- Observed and evaluated the effectiveness of GRANTS transaction data output as of May 30, 2014, to determine if transaction data output was complete, accurate, valid, and confidential. Specifically, we obtained copies of reports and production examples to evaluate the effectiveness of data output.
- Evaluated the effectiveness of application security management, including whether policies and procedures have been established, to control and periodically assess the application security.
- Observed and evaluated GRANTS access controls including user identification and authentication mechanisms.
- Observed and evaluated the effectiveness of GRANTS online edits. Specifically we evaluated 40 online edits of GRANTS as of May 9, 2014.
- Observed and evaluated the effectiveness of GRANTS user authorization and appropriateness of access controls. Specifically, we evaluated the access privileges of 22 user accounts with access privileges to the GRANTS application as of March 31, 2014, for supporting authorization forms and appropriateness of access to GRANTS. We also evaluated the appropriateness of access privileges of certain access control groups and domain user accounts on the GRANTS application server as of June 9, 2014, and the GRANTS database as of June 6, 2014.
- The Department did not make any systems modifications to GRANTS during our audit period; therefore, we did not evaluate GRANTS program change controls.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing 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 those matters requiring corrective action.

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 October 17, 2014, the Interim Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Interim Secretary

October 17, 2014

Mr. David Martin
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Martin:

Thank you for the opportunity to respond to your September 19 list of preliminary and tentative audit findings and recommendations on the information technology operational audit of the Department of Children and Families Grants and Other Revenue Allocation and Tracking System (GRANTS).

Enclosed is the Department of Children and Families' response. Should you have any questions, please contact Malone Smith, Director of Information Technology Planning and Administration, at (850) 320-9393.

We appreciate the work of your staff and look forward to working with them on future engagements.

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

Sincerely,

Mike Carroll
Interim Secretary

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS
DEPARTMENT OF CHILDREN AND FAMILIES
GRANTS AND OTHER REVENUE ALLOCATION AND TRACKING SYSTEM (GRANTS)
INFORMATION TECHNOLOGY OPERATIONAL AUDIT

Finding No. 1: Certain GRANTS policies and procedures had not been established and other documentation needed improvement.

Recommendation: The Department should establish GRANTS policies and procedures for software and firmware updates and error and exception reports. Additionally, the Department should establish GRANTS user training procedures and related documentation and should ensure that the *GRANTS User Manual* is up to date and reflects current processing procedures and reporting capabilities for GRANTS.

Response: The Executive Direction and Support (EDS) Information Technology (IT) unit, which is responsible for the support of GRANTS, is currently engaged in a project to upgrade the application to supported servers for both the application (Windows 2008) and database (SQL Server 2012). Additionally, EDS is upgrading and synchronizing the development and runtime environments. This project is scheduled for completion by January 31, 2015.

Additionally, EDS has created a Capacity Plan, which will create a schedule of routine upgrades of all applications in order to keep them supported hardware and software.

Procedures are being established for the GRANTS Unit Staff to monitor and review error and exception reports and follow up with appropriate Revenue Management Staff to resolve any errors.

In the past, due to the lack of turnover and number of users of the GRANTS system, formal training has never been developed. The GRANTS supervisors, with the assistance of the GRANTS system staff, have trained new users as needed. Once the user manual is updated, it will provide step-by-step instructions on the use of the system and training will be developed for new users.

The GRANTS User Manual is under revision; however, due to the planned major GRANTS rewrite, it has been put on hold until after the rewrite is completed.

GRANTS reporting capabilities are discussed in Chapter 2 of the GRANTS User Manual.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 2: The Department did not timely deactivate the GRANTS-related access privileges of three former IT employees and two former IT contractors subsequent to the dates of termination of their employment or contracts.

Recommendation: The Department should ensure that the GRANTS-related access privileges of former employees and contractors are timely deactivated and removed from active access control groups.

Response: As part of the software and firmware upgrade project, the EDS-IT unit will be creating Active Directory (AD) groups, which will be used to provide the appropriate and limited access to the GRANTS servers and databases by developers. EDS has created an initial version of the Standard Operating Procedures (SOP) manual for the unit, which is currently in force and has been distributed to the supervisors. The SOP contains the instructions for granting and removing access of staff to all databases, including GRANTS. Regarding employee separation, the supervisors will enter a change management ticket assigned to the Department's Security unit to have the individuals removed from all EDS AD groups. This removal will be accomplished prior to the last work day of the separating employee.

Finding No. 3: Certain security controls related to user authentication, monitoring, and logging for GRANTS needed improvement.

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

Response: After the EDS-IT unit completes the GRANTS upgrade project, the team will commence with a project to enhance the security controls of GRANTS to be in compliance with rule 71A of the Florida Administrative Code. This work has been added to the EDS governance release schedule and is scheduled to be completed by June 30, 2015.

Finding No. 4: Contrary to Section 119.071(5)(a)2.a., Florida Statutes, the Department collected and used certain social security numbers (SSNs) in GRANTS without specific authorization in law or without having established the imperative need to use the SSNs for the performance of its duties and responsibilities as prescribed by law.

Recommendation: In the absence of establishing an imperative need for the use of SSNs, the Department should comply with State law by establishing another number to be used in GRANTS rather than SSNs.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Response: The GRANTS Unit Staff have modified the procedures for the creation of user-IDs. The SSN is no longer required for an individual to be granted access to GRANTS and will no longer be collected.

Finding No. 5: The Department had not established data categorization policies and procedures and had not categorized its data in accordance with Federal Information Processing Standards Publication (FIPS PUB) 199, contrary to Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-2.001(3)(l), Florida Administrative Code.

Recommendation: The Department should establish data categorization policies and procedures and categorize its data.

Response: The Department is in the process of contracting with a vendor to assist us in the area of information technology security policies and procedures. One of the tasks specified is for the vendor to assist DCF in performing FIPS 199 systems categorization and/or confirm any existing categorizations are aligned with FIPS 199. We anticipate the systems categorization will be complete in March 2015.

[1] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.