



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



DEPARTMENT OF CHILDREN AND FAMILY SERVICES GRANTS AND OTHER REVENUE ALLOCATION AND TRACKING SYSTEM Information Technology Audit

SUMMARY

The Department of Children and Family Services' (Department) Grants and other Revenue Allocation and Tracking (GRANT) System captures and sorts data from the State's accounting system, Florida's Accounting Information Resource, (FLAIR), to allocate expenditures to funding sources, calculate federal reimbursements, and perform other financial activities. The Office of Revenue Management, organizationally within Financial Management under the Secretary of Administrative Services for the Department, utilizes the GRANT System 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. Ultimately, the GRANT System supplies data used to compile Departmentwide reports required by the Federal Government, including the annual Schedule of Expenditures of Federal Awards (SEFA).

Our audit focused on evaluating the effectiveness of selected internal controls related to the GRANT System and its information technology (IT) environment for the period October 2006 through March 2007. The results of our audit are summarized below:

Finding No. 1: The Department needed a more comprehensive security program to ensure that exposures and vulnerabilities of IT resources had been sufficiently assessed by management and addressed through enforced user and system security controls.

Finding No. 2: We noted that Department staff could not provide a comprehensive and accurate listing of all terminated employees. In addition, we noted instances where Department staff did not remove access privileges of terminated employees in a timely manner.

Finding No. 3: GRANT System documentation, policies, procedures, and training needed improvement.

Finding No. 4: Improvements were needed in the GRANT System's change management process to promote a proper segregation of duties and monitoring of change management activities.

Finding No. 5: The GRANT System did not produce transaction logs that were readily available for researching unauthorized or erroneous transaction activity.

BACKGROUND

Grant accountants in the Office of Revenue Management are the primary users of the GRANT System. The GRANT System has been in production since July 1994. The GRANT System has maintained a fairly stable environment with minimal changes having taken place since its implementation. At the time of our audit, maintenance of the GRANT application was the responsibility of one programmer/analyst within the Office of Information Systems.

Finding No. 1: Security Program

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The security program establishes a framework and continuing cycle of activity for assessing risk, developing and implementing effective control procedures, and monitoring the effectiveness of these procedures.

The Department had implemented many of the IT security elements necessary for a successful entitywide security program through various policies and procedures. However, our audit disclosed deficiencies in certain aspects of IT security, including a lack of appropriate policies, that indicated a need for a more comprehensive IT security program. Specifically:

- During our audit, the Default Administrative username was still being used on the Northwood wireless controller. Default usernames assigned by vendors to purchased software and hardware are commonly known throughout the IT community. In response to our audit inquiries, Department staff indicated they had since corrected this; however, no policy existed that explained the security risk of maintaining the system default settings on the wireless controller and the necessity of having to change them.
- The Northwood wireless controller was not updated with the latest version of firmware. Firmware and software are computer programs, but firmware programs, unlike software programs, become a permanent part of the computing device, in this case, the wireless controller. Cisco had released three new firmware versions for the 4400 series controller. In response to our audit inquiries, Department staff indicated that they had since addressed and resolved underlying technical issues and that the firmware would be upgraded. However, no

policy existed that provides a Departmentwide requirement for updating system firmware. While the above-noted issue related to firmware, we also found that no Departmentwide policy existed for updating system software.

- During our audit, we identified additional security control deficiencies in network, mainframe, and GRANT System application security. Specific details of these deficiencies, some of which involved a lack of policy, are not disclosed in this report to avoid the possibility of compromising the Department's security controls. However, the appropriate Department personnel have been notified of the deficiencies.

Without a comprehensive security program to follow, the Department may fail to consistently apply proper security controls and jeopardize the integrity, confidentiality, and availability of the Department's systems data.

Recommendation: The Department should establish and implement a comprehensive security program comprised of all appropriate IT-related policies and procedures, including those addressing the issues noted above.

Finding No. 2: Terminated Employees

Effective IT management includes implementing policies and procedures for authorizing access to information resources and documenting such authorizations. It is equally important to notify the security function immediately when an employee is terminated or, for some other reason, is no longer authorized access to information resources. Terminated employees, who continue to have access to critical or sensitive resources, pose a major threat, especially those individuals who may have terminated employment under acrimonious circumstances.

Access to the GRANT System was controlled through software, called Safe & Secure, on the Unisys mainframe and through the GRANT System itself. Through this environment, Department staff had to delete access in Safe & Secure and in the GRANT System to ensure that terminated employee access was completely removed.

Department staff could not, upon our request, provide a comprehensive and accurate listing of all terminated employees. There was no automated mechanism in place for the Department to obtain a comprehensive and accurate listing from People First, the State's human resource management system, of employees who terminated employment. By analyzing the access privileges in the GRANT System and Safe & Secure, along with hard copy documentation of employee GRANT System access deletions, we were able to compile a list of potentially terminated employees.

Our audit disclosed instances where Department staff had not properly removed access from both systems. During the audit period, out of a total of 54 GRANT System users examined, there were 9 user codes of terminated Department employees that remained in Safe & Secure. In addition, one of the 9 user codes remained in the GRANT System with an access profile. In some instances, the exact duration that the access privileges remained active beyond termination could not be determined because of the aforementioned lack of a comprehensive and accurate listing of terminated employees and their termination date. The Department was able to provide termination dates for 6 employees associated with 7 of the 9 user codes that remained in Safe and Secure for periods ranging from 5 to 1096 days. As of May 1, 2007, the Department had not provided termination dates for the remaining 2 employees. Subsequent to the completion of our audit field work, the Department deactivated the user codes on the mainframe and deleted the one profile in the GRANT System.

Similar issues with the reliability and accuracy of People First automated reports were noted in our audit report No. 2007-087. Upon inquiry of Department of Management Services staff, they indicated that they were aware of issues with the People First automated termination report and were working on a resolution as of the end of our current audit field work.

Furthermore, Department staff had not maintained adequate documentation of terminated employees for purposes of removing system access. According to Department policy, GRANT System staff should maintain a GRANT System User Access Request Form for all terminated users and documentation of notification to Data Security to delete the user from Safe & Secure. Our review disclosed that Department staff had not maintained the GRANT System User Access Request Forms that would document an employee's termination, subsequent removal of GRANT System access, and removal from Safe and Secure.

During other testing, we noted that Department staff had not properly deleted access for Department users in BL/SOURCE, a utility that allows modification and implementation of production software. Access to GRANT System files in BL/SOURCE was found active for four individuals who either no longer worked for the Department or did not require access in their current job duties. In response to our audit inquiries, Department staff acknowledged the status of the individuals and deleted their BL/SOURCE access. During our testing, we found four additional Department users who had various IT capabilities in the GRANT System but whose access was suspended due to an expired password. These users no longer needed the access to perform their job duties. Although the users' access was suspended, there was a risk of the users reactivating the accounts and gaining unauthorized access to production source code.

Notwithstanding the reporting issues with People First, the Department remains responsible for monitoring terminations and timely adjusting access privileges. The lack of a complete and accurate listing of employee terminations may have contributed to the above-noted inconsistencies in the removal of access capabilities for terminated employees. Without timely deletion of access of employees who terminate employment with the Department, the risk is increased that access privileges could be misused by the former employees or others.

Recommendation: Until the issue with the People First reporting functionality is resolved, the Department should enhance its alternative procedures to ensure that accurate and complete records of all employee terminations are maintained. Additionally, the Department should ensure that user access reviews are performed frequently and that proper access removal is completed, accompanied by appropriate documentation.

Finding No. 3:
GRANT System Documentation, Policies, Procedures, and Training

The integrity and effective operation of an IT system is enhanced when system users are afforded clear guidance through comprehensive documentation, policies, procedures, and training. System users rely on such guidance to effectively use the system. Our audit detected instances where GRANT System documentation, policies, procedures, and training needed improvement. Specifically:

There was no documentation or training to guide grant accountant supervisors or the GRANT System security coordinator when approving access profile levels. The grant accountant supervisors assumed that the GRANT System security coordinator had the responsibility of approving and assigning proper access levels. However, the security coordinator did not have adequate

documentation or training to determine appropriate access levels based on the user's job responsibilities. Additionally, due to a lack of system documentation and training, the security coordinator was not aware and, therefore, did not ensure that user access to sensitive employee information, such as social security numbers, was restricted and was monitored on a regular basis. Our audit disclosed instances where access was granted that unnecessarily allowed certain GRANT System users to select certain menu items that displayed social security numbers. Without proper documentation and training on security controls, users may be granted inappropriate access. This, in turn, could compromise the integrity of the GRANT System data and allow users access to sensitive employee information.

- The Department had not established policies, procedures, and training for monitoring and resolving detected GRANT System errors and exceptions. The GRANT System produces multiple processing error reports. These reports list items that cannot be processed further at specific points in the GRANT System due to incorrect or missing information. According to Department staff, there were no policies or procedures addressing the review of the error and exception reports, the reports were not being reviewed, and staff did not follow up on or keep track of reported errors. Without documented policies and procedures for error handling, there is limited assurance that errors and exceptions will be appropriately followed up on and resolved, jeopardizing the accuracy and completeness of GRANT System information.
- The Department had not established adequate policies, procedures, and training for GRANT System users. The GRANT System User Manual was last updated in 1997 and in many cases was no longer accurate. While a new user manual was being developed, no timeline existed to complete the manual, which had been in development for two years. In addition,

there was no overall training program for using the GRANT System. Employees relied on predecessor files, supervisor training, and on the job training. Without adequate documentation and training, staff may not be able to perform their jobs in an efficient and effective manner. For example, our audit disclosed instances of processing errors that might have been avoided had comprehensive user documentation and training been provided to staff. During our audit period, incorrect grant data changes were allowed to be processed, without being reviewed by the GRANT System supervisor, resulting in an invalid upload of general accounting transactions into FLAIR for the first quarter of 2007. Department staff subsequently discovered these erroneous charges and backed out the erroneous data, but did not process the FLAIR corrected input data tape until over one month later. Department staff attributed this to human error, but could not quantify the effect of the error.

Recommendation: The Department should establish comprehensive documentation, policies, procedures and training to promote the security and integrity of GRANT System data. This should include, policies and procedures to ensure that user access to the GRANT System is appropriate, properly approved, and reviewed on a regular basis. The Department should also develop a security training program to ensure GRANT System security and user staff understand their roles and responsibilities in the security process. In addition, the Department should develop and document policies and procedures to ensure that GRANT System errors and exceptions are being reviewed and corrected in a timely manner. The Department should also develop a timeline to complete the GRANT System user manual, including intervals for scheduling future updates to the manual to ensure it is kept current, and develop training to instruct users on system use.

Finding No. 4: Change Management

Proper controls over the modification of application software help ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help ensure that all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. Additionally, a proper segregation of software change management duties typically includes a separation between the performance of program changes, user acceptance testing, and the movement of programs into the production environment.

During our audit, we noted that the Department had not provided for an appropriate segregation of duties related to maintaining the GRANT System. As previously discussed, GRANT System maintenance support was primarily managed by one programmer/analyst, an independent contractor working in OIS. This individual controlled practically all changes to data files and source code, and performed all the testing of his changes, without independent monitoring or review of his actions. The absence of a proper segregation of change management duties, together with the lack of monitoring and review of the GRANT System change control activities, increase the risk that unauthorized or erroneous modifications could occur and not be timely detected.

Recommendation: The Department should examine the feasibility of establishing, for the GRANT System, a separation of the functions of application programming, implementation of programs into the production environment, and data modification. If such a segregation of duties is not practicable, the Department should, at a minimum, implement a monitoring and review process over GRANT System change control activities, to ensure that unauthorized or erroneous modifications, should they occur, are timely detected.

Finding No. 5:
Transaction Logs

A complete transaction log is a key output control to ensure complete and accurate results of data processing. The transaction log enables the tracking of a transaction from its source to inclusion in the organization's records, including any additional changes made to the original transaction.

During our audit, we noted that the GRANT System generated logging reports of who last accessed a specific screen within the system; however, it did not produce logging reports of the data changed. Although backup files existed that could be manipulated to produce history for a particular instance, transaction history was not readily available from the GRANT System; only the last access was reported. Without complete transaction logs within the GRANT System, the Department's ability to identify unauthorized or erroneous transaction activity was limited.

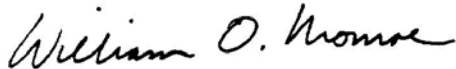
Recommendation: The Department should ensure that future application systems include sufficient logging and reporting capabilities that provide a complete record of changes to data, including who made the change and how the data changed.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to evaluate the effectiveness of selected Department IT controls. Our scope focused on selected general and application IT controls relevant to the GRANT System and the surrounding IT environment during the period October 2006 through March 2007. In conducting our audit, we interviewed appropriate Department personnel, observed Department processes and procedures, and performed various other audit procedures to test selected IT controls.

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 information technology audit.



William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated June 13, 2007, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. This audit was conducted by William Tuck, CISA, and supervised by Tina Greene, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.state.fl.us/audgen>); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

APPENDIX A
MANAGEMENT RESPONSE



State of Florida
Department of Children and Families

Charlie Crist
Governor

Robert A. Butterworth
Secretary

June 13, 2007

Mr. William O. Monroe, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Thank you for your May 17 letter accompanying the preliminary findings and recommendations of your report to be prepared on the Information Technology Audit of the Department of Children and Family Services, GRANT System.

The Department generally concurs with the findings of your report. Enclosed is the Department's response to the specific recommendations you provided. If you or your staff have additional questions, please feel free to call Mr. Kim Brock, Chief Information Officer at (850) 921-5565.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Robert A. Butterworth'. The signature is written in a cursive style with a large initial 'R'.

Robert A. Butterworth
Secretary

Enclosure

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

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS
Information Technology Audit of the
Department of Children and Family Services GRANT System
for the Period October 2006 through March 2007

Finding No. 1
Security Program

Recommendation: The Department should establish and implement a comprehensive security program comprised of all appropriate IT related policies and procedures, including those addressing the issues noted above.

Response: The Department concurs. The Department had already established a security program on the Department's intranet site and the program is comprised of all appropriate policies and procedures. We also engage in continuous process improvement for security practices. However, the Department agrees that additional specific policies need to be added to address the default user name and firmware update issues for wireless controllers that were part of the audit findings. These policies will be drafted in the next 90 days. The remaining confidential control issues are also being addressed.

Finding No. 2
Terminated Employees

Recommendation: Until the issue with the People First reporting functionality is resolved, the Department should enhance its alternative procedures to ensure that accurate and complete records of all employee terminations are maintained. Additionally, the Department should ensure that user access reviews are performed frequently and that proper access removal is completed, accompanied by appropriate documentation.

Response: An alternative solution to providing a listing of separations of employees would be to provide a listing or access to a listing of all current employees from the PeopleFirst system, both OPS and salaried, on a periodic basis. This list could be used by information systems or the GRANTS security officer to compare to the listing of those employees who have access to the GRANTS system. Any employee who has access to the GRANTS system but is not on the current employee listing would be an employee who is no longer with the department and should have their access level to the GRANTS system adjusted accordingly. The Department is researching ways to identify employees whose job duties no longer require access to the GRANTS system.

After the auditors brought the issue to our attention, user access request forms were completed for all terminated employees to delete user access to the

GRANTS system, where supervisors had failed to notify the GRANTS security coordinator. These forms were signed by the staff director of the Office of Revenue Management. Data Security was then notified to remove terminated employees from Safe and Secure. The GRANTS security coordinator will perform routine user access reviews to ensure that terminated employees are removed in a timely manner. However, even though these employees still had profiles remaining in the system, they would not have been able to access the system without network security.

The GRANTS security coordinator has requested an activity report quarterly from Data Security to monitor user code activity in the GRANTS system to determine if any user code(s) should be deactivated.

Finding No. 3

GRANT System Documentation, Policies, Procedures, and Training

Recommendation: The Department should establish comprehensive documentation, policies, procedures and training to promote the security and integrity of GRANT System data. This should include policies and procedures to ensure that user access to the GRANT System is appropriate, properly approved, and reviewed on a regular basis. The Department should also develop a security training program to ensure GRANT System security and user staff understand their roles and responsibilities in the security process. In addition, the Department should develop and document policies and procedures to ensure that GRANT System errors and exceptions are being reviewed and corrected in a timely manner. The Department should also develop a timeline to complete the GRANT System user manual, including intervals for scheduling future updates to the manual to ensure it is kept current, and develop training to instruct users on system use.

Response: DEPCON quarterly reports (CM700L1 and CM702L1) are now being monitored by the GRANTS security coordinator and GRANTS supervisors to determine that user access levels/profiles are appropriate.

GRANTS User Manual is currently under revision and should be completed by September 28, 2007.

During the audit, the security coordinator was apprised of five users whose profiles included access to sensitive employee information. Upon discovery, these profiles were updated to remove inappropriate access.

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.

Finding No. 4
Change Management

Recommendation: The Department should examine the feasibility of establishing, for the GRANT System, a separation of the functions of application programming, implementation of programs into the production environment, and data modification. If such a segregation of duties is not practicable, the Department should, at a minimum, implement a monitoring and review process over GRANT System change control activities, to ensure that unauthorized or erroneous modifications, should they occur, are timely detected.

Response: The Department concurs. The Department will look into a separation of IT functions by reviewing the options available with our new versioning software tool, BLSource. With the full implementation of this product, we will be able to monitor changes and approvals. This tool, along with our current Change Control Management procedure that separates our production and implementation procedures, will ensure a separation of IT functions.

Finding No. 5
Transaction Logs

Recommendation: The Department should ensure that future application systems include sufficient logging and reporting capabilities that provide a complete record of changes to data, including who made the change and how the data changed.

Response: The Department concurs. The Department will ensure that future application systems include sufficient logging and reporting capabilities.

THIS PAGE LEFT BLANK INTENTIONALLY