STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-186
April 2016

DEPARTMENT OF CHILDREN AND FAMILIES

Florida Safe Families Network (FSFN)

Sherrill F. Norman, CPA
Auditor General

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, Mike Carroll served as Department Secretary.

The team leader was Karen Thomas 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

DEPARTMENT OF CHILDREN AND FAMILIES

Florida Safe Families Network (FSFN)

SUMMARY

This operational audit of the Department of Children and Families (Department) focused on evaluating selected information technology (IT) controls applicable to the Florida Safe Families Network (FSFN) and included a follow-up on the findings included in our report Nos. 2014-143 and 2015-156 that were applicable to the scope of this audit. Our audit disclosed the following:

Finding 1: The Department lacked appropriate monitoring controls to ensure the timely input of child welfare case-related information into FSFN, thus increasing the risk that FSFN may not contain the most complete, accurate, and up-to-date data on which to make appropriate decisions regarding the cases. A similar finding was noted in our report No. 2015-156.

Finding 2: The Department had not established controls to ensure that all configuration changes related to FSFN IT maintenance and operations that had been moved into the production environment followed the Department's configuration management process, thus limiting management's assurance that all such configuration changes that had been moved into the production environment were appropriately authorized, tested, and approved.

Finding 3: As similarly noted in our report No. 2014-143, access authorization documentation for some users with access to FSFN was missing, incomplete, or inaccurate. As a result, management's assurance that access privileges were authorized and appropriately assigned is reduced.

Finding 4: Some FSFN security user groups allowed the users the ability to perform functions that were contrary to an appropriate separation of duties, thus increasing the risk that unauthorized modification, loss, or disclosure of FSFN data and related IT resources may occur. Similar findings were noted in prior audits of the Department, most recently in our report No. 2015-156.

Finding 5: The Department had not established procedures for the periodic review of FSFN user access privileges and did not perform such periodic reviews. Under these circumstances, management's assurance that FSFN user access privileges were authorized and appropriate is limited. A similar finding was noted in our report No. 2014-143.

Finding 6: Certain security controls related to user authentication and monitoring for FSFN and related IT resources continued to need improvement to ensure the confidentiality, integrity, and availability of FSFN data and related IT resources. A similar finding related to user authentication was communicated to Department management in connection with our report No. 2014-143.

BACKGROUND

The Department of Children and Families (Department) is charged with establishing a children and families client and management information system that provides information concerning children served

by the children and families programs.[1] The Florida Safe Families Network (FSFN) is Florida's Statewide Automated Child Welfare Information System and serves as the official system of record for documenting child protective investigations and child welfare casework Statewide, from the initial reporting of abuse and neglect to foster care and adoptions case management and permanency planning. FSFN is also the State's official record of all homes and facilities licensed by the State or approved for adoption placement. According to the Department, FSFN is a fully automated system that provides immediate electronic access to any and all information known about a case to support rapid and effective responses to the needs of children and families. State law[2] provides that, to the extent allowed by law and within specific appropriations, the Department shall deliver services by contract through private providers (service providers). FSFN supports Department, community-based care (CBC), and Sheriffs' offices child protection and child welfare-related processes and practices.

FINDINGS AND RECOMMENDATIONS

Finding 1: Monitoring Controls

Business process controls are the automated and manual controls applied to business transaction flows including the timely input of data during application processing. Automated controls are system based and may be used to control things such as the correctness or accuracy of data (e.g., edits and validations). Manual controls are typically used to ensure the reasonableness of transactions and include monitoring controls to timely identify and correct any errors or data exceptions.

Our audit follow-up procedures to determine the status of a finding noted in our report No. 2015-156 regarding the timely input of child welfare case-related information into FSFN included inquiries of Department personnel. In response to our inquiries, Department personnel indicated that the Department still lacked the appropriate monitoring controls necessary to ensure the timely input of child welfare case-related information into FSFN by the CBCs within 2 business days as stipulated in the standard contract between the Department and the CBCs. If the child welfare case-related information is not timely input, the risk is increased that FSFN may not contain the most complete, accurate, and up-to-date data on which to make appropriate decisions regarding the cases.

Recommendation: We recommend that Department management establish appropriate monitoring controls to ensure that FSFN includes the up-to-date information necessary for effective service delivery and case management.

Finding 2: Configuration Management Controls

Effective configuration management controls are intended to ensure that all configuration changes follow a configuration management process that ensures that configuration changes are appropriately authorized, tested, and approved for movement into the production environment. Additionally, the effectiveness of configuration management controls is enhanced by controls that ensure the configuration

[1] Section 409.146, Florida Statutes.

[2] Section 20.19(1)(c), Florida Statutes.

management process is followed when configuration changes are moved into the production environment.

Our audit procedures disclosed that the Department had a configuration management process in place to ensure that configuration changes were appropriately authorized, tested, and approved. However, the Department had not established controls to ensure that all the configuration changes related to FSFN IT maintenance and operations followed the Department's configuration management process when moved into the production environment.

Absent controls to ensure that all configuration changes follow the Department's configuration management process, management has limited assurance that the FSFN IT maintenance and operations-related configuration changes moved into the production environment had been appropriately authorized, tested, and approved.

Recommendation: We recommend that Department management establish controls to ensure that all configuration changes related to FSFN IT maintenance and operations follow the Department's configuration management process.

Finding 3: Access Authorization Documentation

Agency for Enterprise Information Technology (AEIT) rules[3] provide that agency information owners shall be responsible for authorizing access to information. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges authorized by management. Additionally, appropriately maintained access authorization documentation facilitates the complete and accurate assignment of user access privileges.

To determine whether the access privileges granted to FSFN were authorized and appropriately assigned, we requested access authorization documentation for 39 users with update access privileges to FSFN accounts as of September 23, 2015. Our audit procedures disclosed that the Department's access authorization documentation for some users with access to FSFN was missing, incomplete, or inaccurate. Specifically, we noted that:

- The Department could not provide access authorization documentation to evidence that the access privileges assigned for 6 of the 39 users included in our audit test were authorized and appropriate. Department management indicated that the access authorization documentation had been destroyed or misplaced.
- Access authorization documentation was provided by the Department for the remaining 33 users; however, the documentation for 2 users did not contain supervisor approvals. In addition, the documented level of access authorized for 19 users did not match the level of access granted for the users in FSFN.

Without complete and accurate access authorization documentation, management's assurance that access privileges are authorized and appropriately assigned is limited. A similar finding was noted in our report No. 2014-143.

[3] AEIT Rule 71A-1.007(1), Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; administrative authority; and administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, of the AEIT to the AST.

Recommendation: We recommend that Department management maintain complete and accurate access authorization documentation to support management's assurance that FSFN user access privileges are authorized and appropriately assigned.

Finding 4: Appropriateness of User 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 appropriate and necessary for the user's assigned job duties. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

FSFN security user groups organized users into groups based on their job duties and controlled user access privileges to FSFN. Our audit procedures disclosed that, as of July 30, 2015, some FSFN security user groups enabled users to perform functions that were contrary to an appropriate separation of duties. Specifically, we noted that there were security user groups that enabled users to both create payments to service providers and update service provider addresses. In response to our audit inquiry, Department management indicated that some FSFN security user groups were initially established that provided users the ability to perform incompatible functions and those groups were not subsequently appropriately adjusted to prevent the incompatible functions. Also, the Department permitted users to be assigned to multiple FSFN security user groups which allowed the users to perform incompatible functions through the combination of their assigned security user groups.

The existence of inappropriate and unnecessary user access privileges increases the risk that unauthorized modification, loss, or disclosure of FSFN data and related IT resources may occur. Similar findings were noted in prior audits of the Department, most recently in our report No. 2015-156. Department management indicated that, subsequent to our audit inquiry, some of the security user groups referred to above had been modified in December 2015 to promote a more appropriate separation of duties.

Recommendation: We recommend that Department management improve its access controls by continuing its efforts to limit FSFN security user group access privileges, thereby promoting a more appropriate separation of duties.

Finding 5: Periodic Reviews of User Access Privileges

AEIT rules[4] provide that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

Our audit procedures disclosed that the Department did not perform periodic reviews of FSFN user access privileges. In response to our audit inquiry, Department management indicated that the Department had not established procedures for the periodic review of FSFN user access privileges.

[4] AEIT Rule 71A-1.007(2), Florida Administrative Code.

Without periodic reviews of FSFN user access privileges, management's assurance that user access privileges were authorized and appropriate is limited. A similar finding was noted in our report No. 2014-143.

Recommendation: We recommend that Department management establish procedures for the periodic review of FSFN user access privileges and perform periodic reviews to verify that FSFN user access privileges are authorized and appropriate.

Finding 6: Security Controls – User Authentication and Monitoring

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 and monitoring for FSFN and related IT resources continued to need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising FSFN data and related IT resources. However, we have notified appropriate Department management of the specific issues.

Without appropriate security controls related to user authentication and monitoring for FSFN and related IT resources, the risk is increased that the confidentiality, integrity, and availability of FSFN data and related IT resources may be compromised. A similar finding related to user authentication was communicated to Department management in connection with our report No. 2014-143.

Recommendation: We recommend that Department management improve certain security controls related to user authentication and monitoring for FSFN and related IT resources to ensure the confidentiality, integrity, and availability of FSFN data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the applicable findings included in our report Nos. 2014-143 and 2015-156.

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 August 2015 through September 2015 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 FSFN during the period July 2015 through September 2015 and selected actions through February 10, 2016. The audit included selected business process application controls over transaction data input, processing, and output and selected application-level general controls applicable to FSFN that related to the deficiencies disclosed

in our report No. 2014-143 and selected issues noted in our report No. 2015-156 that were applicable to the scope of our audit. The audit also included selected application-level general controls related to security management, access to programs and data, and configuration management and determined whether the Department had a plan to ensure that FSFN was Statewide Automated Child Welfare Information System (SACWIS) compliant. 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 determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2014-143 and selected issues noted in our report No. 2015-156 that were applicable to the scope of our audit.
- 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 Department personnel.
- Obtained an understanding of FSFN's background, including FSFN's purpose and goals for promoting financial, operational, and compliance requirements.

- Obtained an understanding of FSFN data and business process flows, including key sources of data input and interfaces, key application transactions and processes, and key types of data output related to the application.
- Evaluated the effectiveness of selected FSFN business process application controls related to data input, processing, output, and interfaces.
- Obtained an understanding of the FSFN configuration management processes.
- Evaluated the effectiveness of selected FSFN configuration management controls. Specifically, we reviewed seven FSFN change requests that were completed between July 1, 2015, and September 17, 2015, to determine whether selected FSFN changes were appropriately authorized, documented, tested by an independent party, approved for production, and implemented.
- Obtained an understanding of the plan that had been implemented to ensure that FSFN is Statewide Automated Child Welfare Information System compliant.
- Obtained an understanding of selected security management controls, including security awareness training.
- Obtained an understanding of Department procedures for its account management processes for authorizing, creating, modifying, and revoking FSFN access.
- Determined whether the Department had procedures for periodically reviewing FSFN access appropriateness.
- Evaluated the effectiveness of selected FSFN access authorization controls. Specifically, we reviewed selected access authorization controls for 39 users with update access privileges to FSFN accounts as of September 23, 2015.
- Evaluated the effectiveness of selected FSFN access controls related to access privileges for access appropriateness. Specifically, we reviewed:
    - The FSFN access privileges granted for 23 users as of September 23, 2015, to determine the appropriateness of the access granted.
    - The access privileges granted for 5 FSFN security user groups as of July 30, 2015, to determine whether the access granted promoted an appropriate separation of duties.
    - The FSFN access histories of 3 former Department employees who separated on October 3, 2014; March 6, 2015; and August 8, 2015; respectively, to determine whether FSFN maintained a history of the access privileges that were granted to former employees, as required by the *General Records Schedule GS1-SL for State and Local Government Agencies*.
    - The FSFN security user groups as of July 30, 2015, to determine whether the assignment of a security user group or multiple security user groups promoted an appropriate separation of duties.
- Evaluated the effectiveness of selected FSFN user identification and authentication controls, FSFN database monitoring controls, and other security 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, 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

State of Florida
Department of Children and Families

Rick Scott
Governor

Mike Carroll
Secretary

March 21, 2016

Sherrill Norman
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Ms. Norman:

Thank you for your February 29 letter and the accompanying preliminary and tentative audit findings and recommendations on your information technology operational audit of the *Department of Children and Families, Florida Safe Families Network (FSFN)*. The department generally concurs with the findings of your report. Our responses to the findings and recommendations are attached.

If you or your staff have any questions, please contact, as applicable, Brad Wageman, Director of IT for Family and Community Services, at (850) 320-9159, or Joe Vastola, Chief Information Officer, at (850) 320-9170.

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

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

Sincerely,

Mike Carroll
Secretary

Attachment

1317 Winewood Boulevard, Tallahassee, Florida 32399-0700

Mission: Work in Partnership with Local Communities to 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

FLORIDA DEPARTMENT OF CHILDREN AND FAMILIES

FLORIDA SAFE FAMILIES NETWORK (FSFN) SYSTEM

Finding No. 1: The Department lacked appropriate monitoring controls to ensure the timely input of child welfare case-related information into FSFN, thus increasing the risk that FSFN may not contain the most complete, accurate, and up-to-date data on which to make appropriate decisions regarding the cases. A similar finding was noted in our report No. 2015-156.

Recommendation: We recommend that Department management establish appropriate monitoring controls to ensure that FSFN includes the up-to-date information necessary for effective service delivery and case management.

Office of Child Welfare Response: The Department of Children and Families, Office of Child Welfare's current 'Attachment I' to the Community Based Care (CBC) Lead Agency contract with each of the CBCs currently states, "The Lead Agency shall ensure that FSFN is updated within two (2) working days for standard case work of any changes known to the Lead Agency or its Case Management Organizations to ensure FSFN contains the most accurate and complete data regarding child welfare casework." The Department currently has a Contract Oversight Unit (COU) within its Contracted Client Services office that conducts an annual monitoring visit with all of the CBC lead agencies.

In addition, the Department is currently working a strategic initiative called 'FSFN System Adoption.' To support this initiative, the Office of Child Welfare has developed specific utilization standards for all subjects in our statewide system of care and is currently working with each CBC lead agency to review the utilization standards and to implement improvements.

Finding No. 2: The Department had not established controls to ensure that all configuration changes related to FSFN IT maintenance and operations that had been moved into the production environment followed the Department's configuration management process, thus limiting management's assurance that all such configuration changes that had been moved into the production environment were appropriately authorized, tested, and approved.

Recommendation: We recommend that Department management establish controls to ensure that all configuration changes related to FSFN IT maintenance and operations follow the Department's configuration management process.

Office of Information Technology Services Response: Currently, the Department verifies that the change requests included in the quarterly releases were tested and approved and are tracked through the associated ClearQuest tickets and the deployment process. The Department will add a process step for maintenance and operations code changes to validate no unauthorized changes have been added to the code build.

Finding No. 3: As similarly noted in our report No. 2014-143, access authorization documentation for some users with access to FSFN was missing, incomplete, or inaccurate. As a result, management's assurance that access privileges were authorized and appropriately assigned is reduced.

Recommendation: We recommend that Department management maintain complete and accurate access authorization documentation to support management's assurance that FSFN user access privileges are authorized and appropriately assigned.

Office of Information Technology Services Response: The Department is updating the IT Operational Security Plan by the end of FY 2015/2016 and plans to implement any new procedures contained in the Plan during FY 2016/2017. An anticipated outcome of the project will be providing all security officers with updated standard procedures so that complete and accurate access authorization documentation is maintained.

Finding No. 4: Some FSFN security user groups allowed the users the ability to perform functions that were contrary to an appropriate separation of duties, thus increasing the risk that unauthorized modification, loss, or disclosure of FSFN data and related IT resources may occur. Similar findings were noted in prior audits of the Department, most recently in our report No. 2015-156.

Recommendation: We recommend that Department management improve its access controls by continuing its efforts to limit FSFN security user group access privileges, thereby promoting a more appropriate separation of duties.

Office of Information Technology Services Response: After the audit period, the Offices of Child Welfare and Information Technology Services coordinated meetings to determine any changes required to ensure that there are appropriate separation of duties. It was determined that one change was needed for the Statewide Program

Office Worker Security User Group. This change was made to FSFN on December 7, 2015.

Finding No. 5: The Department had not established procedures for the periodic review of FSFN user access privileges and did not perform such periodic reviews. Under these circumstances, management's assurance that FSFN user access privileges were authorized and appropriate is limited. A similar finding was noted in our report No. 2014-143.

Recommendation: We recommend that Department management establish procedures for the periodic review of FSFN user access privileges and perform periodic reviews to verify that FSFN user access privileges are authorized and appropriate.

Office of Information Technology Services Response: The Department will review the statewide security policy as part of the IT Operational Security Plan to include a comprehensive periodic review and documentation of FSFN access privileges that includes verification of access by appropriate supervisory personnel independent of the users for whom the access verification pertains.

Finding No. 6: Certain security controls related to user authentication and monitoring for FSFN and related IT resources continued to need improvement to ensure the confidentiality, integrity, and availability of FSFN data and related IT resources. A similar finding related to user authentication was communicated to Department management in connection with our report No. 2014-143.

Recommendation: We recommend that Department management improve certain security controls related to user authentication and monitoring for FSFN and related IT resources to ensure the confidentiality, integrity, and availability of FSFN data and related IT resources.

Office of Information Technology Services Response: The Department has identified a solution to improve the security controls related to user authentication for FSFN and related IT resources. The Agency for State Technology (AST) will provide access logging and monitoring as part of their core service to the Department. Implementation of the changes that ensure user authentication and monitoring are targeted to be completed by the end of FY 2016/2017.