STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2016-004
July 2015

DEPARTMENT OF CHILDREN AND FAMILIES

Prior Audit Follow-Up

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. Michael Carroll served as Secretary during the period of our audit.

The team leader was Susan Phelan, CPA, and the audit was supervised by Lisa Norman, CPA.

Please address inquiries regarding this report to Lisa Norman, CPA, Audit Manager, by e-mail at lisanorman@aud.state.fl.us or by telephone at (850) 412-2831.

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

Prior Audit Follow-Up

SUMMARY

This operational audit of the Department of Children and Families (Department) focused on evaluating actions taken by the Department to correct deficiencies disclosed in our report No. 2014-188 related to the Domestic Violence Program, the Telework Program, and selected administrative activities. Our audit disclosed the following:

Domestic Violence Program

Finding 1: As similarly noted in our report No. 2014-188, the Department's monitoring efforts related to the Florida Coalition Against Domestic Violence were not always sufficient or properly documented.

Telework Program

Finding 2: As similarly noted in our report No. 2014-188, teleworker performance evaluations did not always include required notations to evidence the continuing appropriateness of the telework arrangements. Additionally, teleworking arrangements were not always accurately identified in the State's human resource information system, People First.

Computer Assignment and Data Security

Finding 3: The Department did not always document the assignment and return of laptop computers for Department employees. A similar finding was noted in our report No. 2014-188.

Finding 4: The Department did not document that former employees' laptop computers were properly sanitized to remove sensitive data before the laptops were surplused or reassigned.

Selected Administrative Activities

Finding 5: The Department had still not established policies and procedures for the collection and use of social security numbers or evaluated its collection and use of social security numbers to ensure compliance with State law.

Finding 6: Department controls over employee access to the Florida Online Accounting Information Resource Subsystem (FLAIR) and the Department's network continue to need improvement. Additionally, employee separation checklists used to account for the return of all State owned property, files, records, and work product for employees separating from Department employment were not always timely or properly completed.

BACKGROUND

State[1] law provides that the mission of the Department of Children and Families (Department) is to 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. The Department plans,

[1] Section 20.19(1)(a), Florida Statutes.

administers, and delivers most of its services to target groups through offices in 6 regions and 20 circuits. The regional offices are responsible for support services, contract management, and local program office functions. The circuits are responsible for field operations, such as protective investigations for children and adults and public assistance eligibility determinations. The Department's Central Office of Administrative Services provides administrative guidance and support to the regions in the areas of fiscal, budget, contract management, human resources, and general services and is responsible for ensuring Statewide compliance and adherence to State laws and Federal regulations. Within the Central Office of Administrative Services, the Office of Human Resources supports the effective and efficient delivery of human resource services.

FINDINGS AND RECOMMENDATIONS

DOMESTIC VIOLENCE PROGRAM

The Department's Domestic Violence Program operates as the central clearinghouse for State and Federal funding initiatives for the prevention and intervention of domestic violence. There are 42 certified domestic violence centers located throughout the State which provide domestic violence prevention and intervention services, such as emergency shelter, counseling, case management, information and referrals, and training for law enforcement and other professionals. The Department is responsible for overseeing the Domestic Violence Program, including certifying the domestic violence centers and administering State and Federal funding for the Domestic Violence Program. The Department is also responsible for providing quality assurance, technical assistance, and training for the State's 42 certified domestic violence centers, and for contracting with the Florida Coalition Against Domestic Violence (Coalition) for the coordination, delivery, management, and evaluation of domestic violence services. The Coalition is responsible for the implementation, administration, and evaluation of all services provided by the certified domestic violence centers. Other Coalition activities include legal initiatives, economic justice initiatives, operation of a Statewide toll-free hotline, assistance for law enforcement and State attorney specialized domestic violence units, court improvement programs, education and training programs, and fatality reviews. The Coalition accomplishes these responsibilities through subcontracts with traditional direct service providers, the criminal justice system, and professional associations.

For the 2014-15 fiscal year, the Department budgeted $36,957,341 for the Domestic Violence Program, including $18,577,348 from Federal sources[2] and $18,379,993 from State sources. State funding sources included fees assessed on marriage licenses[3] and dissolutions of marriage,[4] fines related to violations of injunctions for protection against domestic violence,[5] and general revenue. As of February 2015, the Department had allocated $36,473,017 of the 2014-15 fiscal year budgeted amount

[2] Violence Against Women Formula Grants (Catalog of Federal Domestic Assistance [CFDA] No. 16.588); Grants to Encourage Arrest Policies and Enforcement of Protection Orders Program (CFDA No. 16.590); Temporary Assistance for Needy Families (CFDA No. 93.558); and Family Violence Prevention and Services/Domestic Violence Shelter and Supportive Services (CFDA No. 93.671.

[3] Section 741.01, Florida Statutes.

[4] Section 28.101, Florida Statutes.

[5] Section 741.30, Florida Statutes.

to the Coalition and, of this amount, the Coalition had allocated $22,074,487 to the certified domestic violence centers.

Finding 1: Department Monitoring of the Coalition

State law[6] requires the Department to establish a contract monitoring unit and a monitoring process that includes, but is not limited to, requirements for developing and maintaining a set of procedures describing the contract monitoring process and for preparing a contract monitoring plan that includes sampling procedures and a description of the programmatic, fiscal, and administrative components that will be monitored on-site. The Department established a Contract Oversight Unit and policies and procedures[7] for administrative and programmatic contract oversight to help ensure compliance with State law. The contract oversight policies and procedures included instructions for preparing monitoring plans, conducting monitoring, and reporting the monitoring results. Department policies and procedures also required that monitoring team leaders, when preparing for an on-site monitoring visit, establish a monitoring scope, referred to as a charter, and develop a monitoring plan that included the charter and a sampling plan. Prior to the start of the on-site review, the Contract Oversight Unit manager was to review the proposed monitoring plan with the monitoring team leader and approve the plan. After approval, the monitoring team leader was to review, evaluate, and approve the monitoring tools to be utilized by team members to execute the monitoring plan.

For the 2013-14 fiscal year, the Department provided contract funding to the Coalition totaling $33,306,183, and the Coalition provided State and Federal funds totaling $22,074,487 to the State's 42 certified domestic violence centers. Pursuant to the terms of its contract with the Department, the Coalition was to allocate funds to the certified domestic violence centers based on a Department-established formula.

The Department's monitoring of the Coalition contract during the period July 1, 2014, through March 31, 2015, consisted of an on-site review conducted in March 2015 for which the Department issued a report in April 2015 with no findings noted. Our follow-up procedures performed to evaluate the Department's monitoring efforts disclosed that improvements were still needed. Specifically, as similarly noted in finding No. 1 of our report 2014-188, we found that:

- The Department's approved monitoring plan and monitoring tools did not include criteria to evaluate the Coalition's allocation of funds to, or monitoring of, the certified domestic violence centers. Additionally, we noted that the monitoring team did not document for the March 2015 on-site review the specific procedures performed or documentation reviewed regarding the Coalition's allocation of funds to, or monitoring of, the certified domestic violence centers. In response to our audit inquiry, Department management indicated that check marks made by the monitor on Department documentation indicated that the monitor had recalculated the allocation amount and matched it to the subcontract amount and that support was not retained for the review of the Coalition's subcontract monitoring efforts because no items of noncompliance were noted. Notwithstanding this response, the monitoring documentation did not clearly demonstrate the procedures performed.

[6] Section 402.7305(4), Florida Statutes.

[7] Department Operating Procedure 75-8, *Procurement and Contract Management, Policies and Procedures of Contract Oversight*.

- For 7 of the 12 monitoring tools completed by the Department monitoring team, no evidence was available to demonstrate that an independent supervisory review of the work had been performed. In addition, we noted 2 monitoring tools were completed and reviewed by the same individual. In response to our audit inquiry, Department management indicated that the monitoring staff did not adhere to Department policies and procedures when reviewing the identified tools.

Including all relevant requirements in the monitoring plan and contract monitoring tools would provide Department management with greater assurance, and enable the Department to better demonstrate, that the Coalition is properly administering Department funds. In addition, maintaining appropriate support for all monitoring procedures performed and evidence of an independent supervisory review of monitoring efforts would better demonstrate the sufficiency of the monitoring performed and the appropriateness of the conclusions made.

Recommendation: We recommend that Department management ensure that the monitoring plan and monitoring tools used to monitor the Coalition are updated to incorporate:

- **Criteria to evaluate the Coalition's allocation of funds to the certified domestic violence centers in accordance with the Department's funding formula.**
- **A review of the Coalition's monitoring of the certified domestic violence centers.**

In addition, to demonstrate the sufficiency of the monitoring work performed and the appropriateness of the conclusions made, we recommend that Department management ensure that independent supervisory reviews are conducted and documented.

TELEWORK PROGRAM

State law[8] establishes the State Employee Telework Program and defines telework as a work arrangement that allows a State employee to conduct all or some of his or her work away from the official worksite during all or a portion of the State employee's established work hours on a regular basis.[9] State law provides that State agencies may establish telework as an integral part of the normal business operations of the agency and establishes various requirements for those State agencies operating a Telework Program, including teleworker productivity monitoring and physical and electronic information security controls. Each State agency with a Telework Program is also required to designate those positions deemed appropriate for telework and to identify, in the State's human resource information system, People First, all currently participating employees and their respective positions.

The Department operated a Telework Program and the Department's Central Office of Human Resources established policies and procedures[10] governing the Telework Program. For the period July 1, 2014, through February 5, 2015, the Department had designated in People First 1,726 of its 11,900 employees as participating in the Telework Program. The Department's teleworkers included abuse registry counselors, public assistance application processors, and interviewing clerks.

[8] Section 110.171, Florida Statutes.

[9] According to Section 110.171(1)(c), Florida Statutes, telework does not include work performed away from the official worksite and outside of established work hours on an occasional basis or the performance of duties and responsibilities that, by their nature, are performed routinely in the field away from the official worksite.

[10] Department Operating Procedure 60-40, *Personnel, Alternative Work Locations*.

Finding 2: Telework Performance Evaluations and Teleworker Designations

State law[11] requires State agencies to establish performance standards and a system for monitoring the productivity of teleworkers that ensures that teleworkers maintain satisfactory performance levels and that the duties and responsibilities of the position remain suitable for a telework arrangement. State law[12] also authorizes State agencies to require written agreements between teleworkers and the agency that provide for the termination of an employee's participation in the Telework Program if the employee's continued participation is not in the best interest of the agency.

The Department's Central Office of Human Resources established Telework Program policies and procedures[13] that required a written agreement between the Department and each teleworker be established at least annually and also included provisions for evaluating teleworker performance and for annually assessing whether the telework arrangement was working satisfactorily and should be continued.

Department policies and procedures also required each teleworker to maintain an overall rating of "satisfactory" or higher on their annual performance evaluation in order to remain in the Telework Program. Department policies and procedures[14] required that employee performance evaluations be performed on an annual basis during the 60 day period beginning on August 1 of each year. In addition, for the evaluation period ended June 30, 2014, the Department issued a memorandum[15] instructing supervisors to ensure that all Department staff who teleworked had an approved telework agreement on file. The Department also instructed supervisors to ensure that each teleworker's performance evaluation contained a notation from the employee's supervisor stating that the telework agreement had been reviewed and that a determination had been made that either the telework arrangement was working satisfactorily and should be continued for another year or that the telework arrangement was not working as intended and was being discontinued.

As part of our audit, we reviewed Department documentation, including telework agreements and applicable performance evaluations, related to 40 employees who were identified in People First as participating in the Department's Telework Program during the period July 1, 2014, through February 5, 2015. We found that:

- For 6 of the 33 applicable 2014 performance evaluations, the employee's supervisor had not included the required notation stating whether the telework arrangement should be continued for another year. In response to our audit inquiry, Central Office of Human Resources management indicated that supervisors had not always followed Department guidance relating to performance evaluations for teleworkers. Similar instances were noted in our report No. 2014-188, finding No. 2.

[11] Section 110.171(4), Florida Statutes.

[12] Section 110.171(5), Florida Statutes.

[13] Department Operating Procedure 60-40, *Personnel, Alternative Work Locations*.

[14] Department Operating Procedure 60-35, *Personnel, Performance Evaluation Program for Career Employees, and Selected Exempt Service Employees covered by a Current Collective Bargaining Agreement*.

[15] Department Memorandum, dated July 7, 2014: *Performance Evaluations and Telework Information for the Performance Management Period Ending June 30, 2014*.

- The Department had incorrectly coded 4 of the 40 employees as teleworkers in People First. One of the 4 employees had never participated in the Telework Program and the other 3 employees had terminated from the Telework Program prior to July 1, 2014. As of February 5, 2015, the Department's People First records had incorrectly shown these 3 employees as active teleworkers for periods of approximately 10 months to over 3 years. According to Department management, these employees had been coded incorrectly due to errors made by Department staff and, subsequent to our audit inquiry, the Department updated People First for the employee who had never participated in the Telework Program and for 2 of the 3 employees who had terminated from the Telework Program.

Statements in the teleworkers' annual performance evaluations indicating that the telework arrangement is working satisfactorily enable the Department to demonstrate of record that the teleworking arrangement continues to be appropriate and in the best interest of the Department. Timely updating and accurately recording telework arrangements in People First allows the Department to correctly track and report on individuals participating in the Telework Program.

Recommendation: We again recommend that management in the Department's Central Office of Human Resources communicate to appropriate supervisory staff the requirements outlined in Department policies and procedures to help ensure that decisions to continue teleworking arrangements are properly documented in employee annual performance evaluations. We further recommend that Central Office of Human Resources management take appropriate measures to ensure that the designation of telework arrangements is accurately entered into People First and timely updated when employees no longer telework.

COMPUTER ASSIGNMENT AND DATA SECURITY

The Department established security controls to protect and ensure the appropriate use and maintenance of computer equipment used by Department employees. In accordance with Department policies and procedures,[16] supervisors were to require employees who were assigned State-owned laptop computers to complete and sign a State Owned Tangible Personal Property Assignment (CF 1941) form to document custody of the laptop. Additionally, the CF 1941 form included a space for the property consultant or designee to sign evidencing receipt of the laptop computer when it was turned in by the employee. Department policies and procedures[17] also required the use of an employee separation checklist to identify and account for all State property, files, records, and work product. Department Headquarters and each Region and Mental Health Facility were to utilize the Department's standard Employee Separation Checklist.[18] The Employee Separation Checklist included a space for the supervisor to record the date the employee's assigned laptop computer was returned. In addition, Department policies and procedures[19] required that prior to disposal, surplus, reassignment, or off-site repair, laptop computers be sanitized to remove sensitive data.

[16] Department Operating Procedure 80-2, *Property Management*.

[17] Department Operating Procedure 60-70, *Employee Separations and Reference Checks*.

[18] Department Form 789.

[19] Department Operating Procedure 50-2, *Systems Management, Security of Data and Information Technology Resources*, Chapter 2-4.

As discussed in findings 3 and 4, the Department did not always ensure that the assignment, return, and sanitization of sensitive data from laptop computers was appropriately documented. Similar deficiencies were noted in our report No. 2014-188, finding No. 3.

Finding 3: Computer Assignment

As part of our audit, we reviewed documentation to evidence the assignment of laptop computers to 38 Department employees hired during the period July 1, 2014, through February 5, 2015. Our review of available Department documentation disclosed that:

- For 6 employees, the CF 1941 forms were signed and dated from 63 to 127 business days after hire and subsequent to our audit inquiry. For an additional employee, while a form was provided, the employee had not signed and dated the form to evidence receipt of the laptop computer.
- Although requested, the Department was unable to provide properly completed CF 1941 forms for 7 employees.

In addition, we requested CF 1941 forms evidencing the return of laptop computers by 19 employees who had separated from Department employment during the period July 1, 2014, through January 31, 2015. Although we confirmed that the laptops were either in the Department's custody as of June 19, 2015, or had been properly disposed of, our audit inquiries and review of Department documentation disclosed that:

- For 4 former employees, the Department was unable to provide the required CF 1941 form demonstrating the return of the employee's assigned laptop computer.
- For 6 former employees, the Department provided CF 1941 forms. However, the forms for 5 former employees did not include the information necessary to demonstrate the date the laptop computers were returned to the Department and the form for the other former employee did not include the property consultant or designee's signature.
- For 9 of the 10 former employees for which a CF 1941 form was either not provided or was not complete, the Department provided Employee Separation Checklists as documentation for the return of the laptop computers. However, the Employee Separation Checklists provided did not include a space to record the property number of the laptop computer returned. Additionally, 5 of the 10 Employee Separation Checklists provided did not include laptop computer return information and 1 of the 5 Checklists was not signed by the former employee.

Absent documentation of the custody of computer equipment obtained and maintained in accordance with Department policies and procedures, Department management has reduced assurances regarding the adequate safeguarding of Department information technology resources.

Recommendation: We again recommend that Department management emphasize to staff the requirements for documenting the assignment and return of computer equipment.

Finding 4: Data Security

In performing their assigned duties, Department employees routinely access sensitive data, such as social security numbers and child abuse records, relating to Department clients. Consequently, the Department established policies and procedures outlining required processes to ensure the security of

sensitive data.[20] The policies and procedures required that, prior to disposal, surplus, reassignment, or off-site repair, Department computer equipment be sanitized to remove sensitive data. The policies and procedures also required that only authorized personnel perform the sanitization and specified that the date and method used to sanitize the equipment be documented. However, the policies and procedures did not establish a time frame within which the sanitization should occur or require that equipment awaiting sanitization be securely stored.

As part of our audit, we requested documentation to evidence the sanitization of sensitive data for 19 laptop computers assigned to 19 teleworkers who, during the period July 1, 2014, through January 31, 2015, separated from Department employment. In response to our audit request, Department management indicated that the Department had employed a standard process for data sanitization since the beginning of the 2014-15 fiscal year; however, the process was not formally documented and the Department was unable to provide documentation evidencing the sanitization of sensitive data for any of the 19 laptop computers.

Documentation evidencing the sanitization of sensitive data from computer equipment prior to disposal, surplus, reassignment, or off-site repair, provides Department management with assurance that the Department's sensitive data has been protected from inappropriate or unauthorized access. Timely sanitizing sensitive data from computer equipment when the equipment is returned by an employee reduces the risk that the data will be inadvertently exposed.

Recommendation: We recommend that Department management update policies and procedures to establish a time frame for the sanitization of sensitive data from computer equipment returned by Department staff and for the secure storage of equipment awaiting sanitization. In addition, we recommend that Department management follow established procedures regarding the maintenance of appropriate documentation regarding the sanitization of computer equipment.

SELECTED ADMINISTRATIVE ACTIVITIES

As part of our audit we also evaluated selected Department administrative activities and controls, including those related to the Department's processes for the collection and use of social security numbers and the administration of Florida Accounting Information Resource Subsystem (FLAIR) access privileges.

Finding 5: Collection of Social Security Numbers

The Legislature has acknowledged in State law[21] that a person's social security number (SSN) was never intended to be used for business purposes. However, over time the SSN has been used extensively for identity verification and other legitimate consensual purposes.

Recognizing that an SSN can be used to perpetrate fraud against an individual and acquire sensitive personal, financial, medical, and familial information, the Legislature specified[22] that State agencies may

[20] Department Operating Procedure 50-2, *Systems Management, Security of Data and Information Technology Resources*.

[21] Section 119.071(5), Florida Statutes.

[22] Section 119.071(5)(a)2.a., Florida Statutes.

not collect an individual's SSN unless the agency is authorized by law to do so or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law. Additionally, State agencies are required to provide each individual whose SSN is collected written notification regarding the purpose for collecting the number. The SSNs collected may not be used by the agency for any purpose other than the purposes provided in the written notification. State law further provides that SSNs held by an agency are confidential and exempt from public inspection and requires each agency to review its SSN collection activities to ensure the agency's compliance with the requirements of State law and to immediately discontinue SSN collection upon discovery of noncompliance.

In our report No. 2014-188, finding No. 5, we noted that the Department had not established written policies and procedures for the collection and use of SSNs or evaluated its collection and use of SSNs to ensure compliance with State law. Subsequent to our audit inquiries, in April 2013, Department management conducted a Departmentwide survey which identified certain information technology (IT) applications and 203 Department forms that potentially collected SSNs.

As part of our audit follow-up procedures, we inquired of Department management and were informed that, as of April 13, 2015, the Department still had not established written policies and procedures relating to the collection and use of SSNs, nor could the Department demonstrate compliance with applicable State law. In addition:

- Although we requested, the Department could not provide documentation demonstrating the Department's review of the IT applications or forms identified in the April 2013 survey. In response to our audit inquiry, Department management indicated that changes in personnel and a reassignment of responsibilities contributed to the lack of Department action on the April 2013 survey.
- Subsequent to our audit inquiry, Department management sent out a survey in March 2015 to assess compliance with applicable statutory requirements for 152 Department forms identified as collecting SSNs. The Department did not provide documentation to evidence the Department's determination that the 51 forms identified in April 2013 but excluded from the March 2015 survey either met the requirements of State law or were no longer in use. Department management indicated that they were not aware of which forms were included on the April 2013 survey and that they were working with the 152 forms more recently identified by staff.
- In April 2015, the Department provided us a list of 18 IT applications, including the Florida Online Recipient Integrated Data Access IT application and the Child Death Review IT application, which did not provide individuals with written notification regarding the purpose for collecting their SSNs. Although the Department had determined that the collection of SSNs by these IT applications was not in compliance with State law, the Department did not immediately discontinue the collection of SSNs as statutorily required. Department management indicated that, due to staff workload on other priorities and a lack of funding to upgrade old systems, the Department had not been able to make the changes needed to achieve full compliance for the identified IT applications.

Effective controls, including written policies and procedures regarding the Department's collection and use of individuals' SSNs, and periodic assessments of SSN collection activities, would better ensure and demonstrate Department compliance with statutory requirements and reduce the risk that the SSNs may be unnecessarily collected or utilized for unauthorized purposes.

Recommendation: We again recommend that Department management establish written policies and procedures regarding the collection and use of individuals' SSNs, document the

review of Department surveys of SSN collection activities, and take appropriate steps to demonstrate compliance with applicable statutory requirements.

Finding 6: FLAIR Access Controls

The Department utilizes FLAIR to authorize payment of Department obligations and to record and report financial transactions. Controls over employee access to FLAIR are necessary to help prevent and detect any improper or unauthorized use of FLAIR access. Accordingly, FLAIR access should be: (1) limited to properly authorized employees, (2) appropriate for the employee's assigned duties and responsibilities, (3) promptly deactivated when employees separate from the Department or are reassigned to positions no longer requiring FLAIR access, and (4) periodically reviewed for continued appropriateness.

Department procedures[23] required supervisors to notify the appropriate Security Officer to deactivate security access to assigned computer and data systems, including access to the Department's network, within 24 hours of an employee's separation. The procedures also required staff at Department Headquarters and at each Region and Mental Health Facility to utilize the Department's standard Employee Separation Checklist. The Employee Separation Checklist included a checkbox for notifying the FLAIR Security Officer to deactivate the employee's FLAIR access and a checkbox for notifying the Network Manager to deactivate the employee's network access. Upon completion, the forms were to be sent to Human Resources staff who were then to forward the forms to the appropriate parties.

As similarly noted in our report No. 2014-188, finding No. 6, our follow-up audit procedures found that while Department procedures addressed the deactivation of IT access for separating employees, the Department had not established policies and procedures requiring the conduct of periodic reviews of employee FLAIR access to identify and resolve any instances where excess or incompatible privileges had been granted or access was no longer needed. Additionally, our tests of Department FLAIR and network access controls and review of Department access privileges again disclosed that Department controls over employee access to FLAIR and the Department's network needed improvement. Specifically, we found that:

- Employees performing financial management functions had been granted update capabilities to incompatible functions in FLAIR. We reviewed the appropriateness of assigned update capabilities for 14 user accounts (assigned to 14 employees) during the period July 1, 2014, through January 31, 2015. We found for 7 user accounts (assigned to 7 employees) that:
  - Two user accounts had update capabilities to both the disbursement and cash receipts functions;
  - Two user accounts had update capabilities to both the fixed assets accounting and fixed assets custodial functions; and
  - Three user accounts had update capabilities to the disbursement and cash receipts functions and to the fixed assets accounting and fixed assets custodial functions.

  Subsequent to our audit inquiry, the incompatible access privileges were removed for the 7 user accounts. Incompatible access privileges heighten the risk that errors or fraud may occur and not be timely detected. In response to our audit inquiry, Department management indicated that

[23] Department Operating Procedure 60-70, *Personnel, Employee Separations and Reference Checks*.

incompatible access situations may occur because of oversights; however, the Department is in the process of reviewing all staff access to resolve any incompatible access privileges.

- Network access privileges and access to FLAIR were not always timely deactivated upon a user's separation from Department employment. We examined FLAIR access records for 41 user accounts with FLAIR update capabilities assigned to 23 employees who separated from Department employment during the period July 1, 2014, through February 13, 2015. Our examination disclosed that FLAIR access privileges for 15 FLAIR user accounts (assigned to 12 employees) remained active from 2 to 91 business days (an average of 23 business days) after the employees' separation dates. Network access privileges for 6 of the 12 former employees had remained active for 3 to 39 business days (an average of 11 business days) after the employees' separation dates. Additionally, our review of the usage of the 15 FLAIR user accounts assigned to the former employees identified three FLAIR transactions, totaling $396, that were entered using a deceased employee's FLAIR user account that had not been timely deactivated. The deceased employee's FLAIR user account and network account remained active for 91 and 6 business days, respectively, after the employee's date of death. In response to our audit inquiry, Department management indicated that the deceased employee's FLAIR user account was used because no other staff had the access needed to approve the three transactions.
- Supervisors did not always follow Department policies and procedures when completing Employee Separation Checklists and, therefore, Employee Separation Checklists were not always timely or properly completed. Our review of the Employee Separation Checklists for the 12 employees for whom the Department had not timely deactivated FLAIR access privileges disclosed that:
  - Four Employee Separation Checklists were completed from 2 to 106 business days (an average of 32 business days) after the employees' separation dates.
  - The supervisor did not mark the box indicating that FLAIR access privileges should be deactivated for six Employee Separation Checklists.

The effective separation of incompatible accounting duties, prompt deactivation of access privileges upon a user's separation from employment, and periodic and timely review of employee access privileges lessen the risk of unauthorized disclosure, modification, or destruction of Department data.

Recommendation: We again recommend that Department management establish policies and procedures requiring periodic reviews of FLAIR access privileges to aid in the identification and resolution of any instances where excess or incompatible privileges have been granted or access privileges are no longer needed. We also recommend that Department management ensure that all employee separation checklists are timely and appropriately completed, and that FLAIR and network access privileges are timely deactivated upon a user's separation from Department employment.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2014-188.

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 operational audit from January 2015 through May 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 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.

This operational audit focused on evaluating actions taken by the Department to correct deficiencies disclosed in our report No. 2014-188 related to the Domestic Violence Program, the Telework Program, and selected administrative activities. The overall objectives of the audit were:

- To evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, administrative rules, contracts, grant agreements, and guidelines.
- To examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, the reliability of records and reports, and the safeguarding of assets, and identify weaknesses in those internal controls.
- To determine whether the management has corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2014-188.
- 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 those programs, activities, or functions 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 transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions 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 program, activity, or function; 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 transactions and records. Unless otherwise indicated in this report, these transactions and records 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 vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit we:

- Evaluated Department actions to correct the findings noted in our report No. 2014-188. Specifically, we:
  - Reviewed applicable laws, rules, regulations, and Department policies and procedures, and interviewed Department personnel to gain an understanding of the Domestic Violence Program's operations.
  - Obtained an understanding of internal controls and evaluated the effectiveness of key Domestic Violence Program processes, policies, and procedures.
  - Examined Department documentation for the on-site monitoring visit conducted in March 2015 and performed other procedures to assess the sufficiency of Department monitoring activities related to the Florida Coalition Against Domestic Violence (Coalition).
  - Examined documentation related to the Department's cost analysis of the Coalition contract for the 2014-15 fiscal year to determine whether the Department verified the allowability, reasonableness, and necessity of the Coalition's proposed budget.
  - Examined documentation related to the funding formula used by the Coalition to allocate funding to the certified domestic violence centers for the 2014-15 fiscal year to determine whether the formula was approved by the Department, and whether the formula considered factors such as, population, rural characteristics, geographical area, and incidence of domestic violence.
  - Obtained an understanding of the Department's policies and procedures related to Telework Program operations to evaluate whether the Department had established policies and procedures that were adequate and designed to reasonably ensure compliance with significant governing laws and rules.
  - From the population of 1,726 employees designated as teleworkers in People First from July 1, 2014, through February 5, 2015, examined documentation for 40 employees to determine whether the Department had appropriately documented the execution of telework agreements and monitoring of employee performance.
  - From the population of 1,546 employees hired by the Department during the period July 1, 2014, through February 5, 2015, examined documentation for 38 employees who were assigned a laptop computer to determine whether property assignment forms appropriately documented the assignment and custody of computer equipment.
  - Examined Department records related to 19 of the 138 telework employees who separated from Department employment during the period July 1, 2014, through January 31, 2015, to determine whether documentation was available to evidence that the laptop computers assigned to the former employees had been returned and sanitized to remove sensitive data in accordance with Department policies and procedures.
  - From the population of 1,546 employees hired by the Department during the period July 1, 2014, through February 5, 2015, examined documentation for 40 employees to determine whether the Department had documented the conduct of employee background screenings.

- Interviewed Department management and evaluated Department compliance with applicable statutory requirements for collecting and utilizing individuals' social security numbers.
- Compared dates of employment separations with the dates user access privileges were deactivated to evaluate the timeliness of the deactivation of FLAIR access privileges for the 41 FLAIR user accounts related to 23 Department employees who separated from Department employment during the period July 1, 2014, through February 13, 2015. Additionally, reviewed the separation checklists for the 12 employees for whom the Department did not timely remove FLAIR access privileges to determine whether the checklists had been timely and properly completed.
- Examined FLAIR access control records for 14 FLAIR user accounts, from the 533 FLAIR user accounts for Department employees with FLAIR update privileges during the period July 1, 2014, through January 31, 2015, to determine whether the access privileges were appropriate given the employees' job duties.

- Reviewed applicable laws, rules, and other State guidelines to obtain an understanding of the legal framework governing Department operations.
- Examined documentation supporting travel-related costs totaling $8,264 incurred by the Secretary and the General Counsel during the period December 8, 2014, through March 11, 2015, to determine whether such documentation evidenced that the travel costs were properly approved and met the requirements of State law.
- Observed, documented, and evaluated the effectiveness of selected Department processes and procedures for the Department's budgetary, cash management, revenues, and cash receipts processes.
- 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 at pages 15 through 21.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each State agency on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our 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

July 23, 2015

Ms. Sherrill Norman
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1 450

Dear Ms. Norman:

Thank you for your June 22 letter and the accompanying preliminary and tentative audit findings and recommendations on the audit of *Department of Children and Families, Prior Audit Follow-Up*. 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, Mr. Christopher Meadows, Director of Contract Services at (850) 717-4602, Mr. Matt Howard, Director of General Services at (850) 717-4017, Ms. Kimberly McMurray, Chief Financial Officer, at (850) 4733, Mr. Scott Stewart, Chief Information Officer at (850) 320-9132, or Ms. Stephanie Reaves, Director of Human Resources at (850) 488-1700.

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 FINDINGS

DEPARTMENT OF CHILDREN AND FAMILIES

PRIOR AUDIT FOLLOW-UP

OPERATIONAL AUDIT

DOMESTIC VIOLENCE PROGRAM

Finding No. 1: **As similarly noted in our report No. 2014-188, the Department's monitoring efforts related to the Florida Coalition Against Domestic Violence were not always sufficient or properly documented.**

Recommendation: We recommend that Department management ensure that the monitoring plan and monitoring tools used to monitor the Coalition are updated to incorporate:

- Criteria to evaluate the Coalition's allocation of funds to the certified domestic violence centers in accordance with the Department's funding formula.
- A review of the Coalition's monitoring of the certified domestic violence centers.

In addition, to demonstrate the sufficiency of the monitoring work performed and the appropriateness of the conclusions made, we recommend that Department management ensure that independent supervisory reviews are conducted and documented.

Response: The Department agrees that actual payments made from the Florida Coalition Against Domestic Violence (FCADV) to the centers were not evaluated against the validated formulas and that the subcontract monitoring documentation could have been more specific about what was evaluated. The Department appreciates the guidance and feedback from the Auditor General and will consider these recommendations when planning the scope and executing the next monitoring of the FCADV. The Department will continue to improve implementation of quality assurance reviews by monitoring team leaders.

TELEWORK PROGRAM

Finding No. 2: **As similarly noted in our report No. 2014-188, teleworker performance evaluations did not always include required notations to evidence the continuing appropriateness of the telework arrangements. Additionally, teleworking arrangements were not always accurately identified in the State's human resource information system, People First.**

Recommendation: We again recommend that management in the Department's Central Office of Human Resources communicate to appropriate supervisory staff the requirements outlined in Department policies and procedures to help ensure that decisions to continue teleworking

arrangements are properly documented in employee annual performance evaluations. We further recommend that Central Office of Human Resources management take appropriate measures to ensure that the designation of telework arrangements is accurately entered into People First and timely updated when employees no longer telework.

Response: We agree with the recommendation to continue to communicate to appropriate supervisory staff to ensure that decisions to continue the telework arrangement are properly documented in the employees' annual performance evaluations based on our current process for extension of telework agreements. We reiterated and emphasized this requirement in a Department communication regarding completion of the annual performance evaluations for the period ending June 30, 2015, which was disseminated on June 12, 2015.

We also agree with the recommendation to "take appropriate measures to ensure that the designation of telework arrangements is accurately entered into People First and timely updated when employees no longer telework." Please see the following CFOP provisions that address these requirements.

CFOP 60-40, Chapter 9, (Alternate Work Locations) provides in pertinent part as follows in §9-9:

> a. An employee may request approval to telework by completing the Telework Agreement (form CF 1916, available in DCF Forms) and submitting to his/her supervisor.
>
> e.(1) The approved Telework Agreement or the Notice of Termination of Telework Agreement shall be sent to the Human Resources Service Center and the Service Center representative will update the information in People First….
>
> e.(2) The supervisor shall check to ensure that the People First telework screen is updated for employees approved to telework.

CFOP 60-40, Chapter 9, provides in pertinent part as follows in §9-7:

> k. The requirements for terminating optional or required telework are described in this paragraph:
>
> k.(3) …The Notice of Termination of Telework Agreement (form CF 752, available in DCF Forms) will be used to provide the required written notice of termination of the telework arrangement.
>
> k.(5) A copy of the written notice of termination of optional telework or required telework also shall be provided to the Human Resources Shared Services Center to remove the telework designation from the People First System.

Additionally, CFOP 60-40, Chapter 9, §9-10 provides as follows:

> A report of all employees participating in required telework and optional telework will be generated at six-month intervals by Headquarters Human Resources and distributed to management for updating and verification of those employees participating in required and optional telework.

Management in the Department's Central Office Human Resources will continue to emphasize these requirements related to People First in subsequent telework communications sent to DCF Leadership.

Note that the Department does not currently have any positions in which telework is required (all current telework arrangements are optional telework). If and when we do have required telework, any such requirement must be included in the Position Description in accordance with CFOP 60-40, Chapter 9, §9-7a. In such cases, the position attribute People First screen would include telework designation.

COMPUTER ASSIGNMENT AND DATA SECURITY

Finding No. 3: **The Department did not always document the assignment and return of laptop computers for Department employees. A similar finding was noted in our report No. 2014-188.**

Recommendation: We again recommend that Department management emphasize to staff the requirements for documenting the assignment and return of computer equipment.

Response: The Department concurs with the follow up finding. The Office of General Services will continue to work with Region General Services and Information Technology staff to reiterate the importance of proper documentation evidencing issuance and receipt of Department-owned equipment. Additionally, the Office of General Services will take the lead in streamlining processes related to this effort, to include an update of DCF Operating Procedure 80-2, Property Management.

Finding No. 4: **The Department did not document that former employees' laptop computers were properly sanitized to remove sensitive data before the laptops were surplused or reassigned.**

Recommendation: We recommend that Department management update policies and procedures to establish a time frame for the sanitization of sensitive data from computer equipment returned by Department staff and for the secure storage of equipment awaiting sanitization. In addition, we recommend that Department management follow established procedures regarding the maintenance of appropriate documentation regarding the sanitization of computer equipment.

Response: All Department laptop computers have endpoint encryption installed to protect data stored on the laptops.

The Department is in the midst of a project to update its information security operating procedures. An outcome of the project will be a DCF Media Protection operating procedure that describes acceptable sanitization methods, includes a time frame for sanitizing hard drives from computer equipment returned by Department staff, updates requirements regarding documentation of media sanitization, and requires that all media awaiting sanitization is securely stored and accessible only to limited information technology services personnel.

SELECTED ADMINISTRATIVE ACTIVITIES

Finding No. 5: The Department had still not established policies and procedures for the collection and use of social security numbers (SSNs) or evaluated its collection and use of social security numbers to ensure compliance with State law.

Recommendation: We again recommend that Department management establish written policies and procedures regarding the collection and use of individuals' SSNs, document the review of Department

surveys of SSN collection activities, and take appropriate steps to demonstrate compliance with applicable statutory requirements.

Office of Information Technology Services Response: Much of the Department's SSN collection is through the use of forms, paper or electronic, developed by the business areas to capture information they identify as necessary for program operations. The DCF Office of General Services is leading a statewide project in conjunction with the Department's program areas to review all DCF forms that collect SSNs and ensure that statutory authority exists for collection of the SSNs and that the form includes a written statement of the reason for the SSN collection.

Information technology is a business enabler and use of SSNs within an information system occurs in those instances where the SSN was defined as a required data element by the business (and collected through a form). Details regarding the list of 18 applications (systems) referenced as collecting SSNs in the 2014-188 prior audit follow up are provided below:

1. Florida On-Line Recipient Integrated Data Access System (FLORIDA) – The written statement for use of employee SSNs as unique identifiers in this system is provided on the Security Agreement Form, CF0114. At present, the Department is not able to discontinue use of SSNs as unique identifiers in this system due to the scope and cost of the changes required to eliminate SSNs in the FLORIDA system. Replacement of these functions was included in a legislative budget request (LBR) for Fiscal Year 2015-16 to replace all legacy components of the FLORIDA system. The LBR was not funded.
2. Adult Protective Services Information System – A written statement in both English and Spanish is in progress. Anticipated publication date is August 2015.
3. Information Delivery System Query Facility (IDSQF) – This is an information data warehouse used for reporting purposes. It collects and displays information received from or submitted to the Department of Financial Services (DFS) Florida Accounting Information Resource (FLAIR) system. There is no direct SSN collection into this system by the Department.
4. Background Screening System – SSNs stored in this system are received from the Florida Department of Law Enforcement (FDLE) as part of the criminal history results related to statutorily-required background screening. There is no direct SSN collection into this system by the Department.
5. Caretaker Screening Information System – SSNs stored in this system are received from FDLE as part of the criminal history results related to statutorily-required background screening. There is no direct SSN collection into this system by the Department.
6. Caretaker Screening Portal– SSNs stored in this system are received from FDLE as part of the criminal history results related to statutorily required background screening. There is no direct SSN collection into this system by the Department.
7. Child Care Licensing Application – The program's application forms provide a written statement of the purpose for SSN collection as a footnote.
8. Child Death Review – Collects and displays internal information about child fatalities from other systems, such as the Florida Safe Families Network (FSFN). There is no direct SSN collection into this system by the Department.
9. Florida Safe Families Network (FSFN) – The Office of Child Welfare stopped requiring collection of user SSNs for FSFN system access effective June 2015.
10. Food Stamps Data Sharing System – Client SSNs in this system are a data feed from the FLORIDA system. There is no direct SSN collection into this system by the Department.

11. Integrated Benefit Recovery System – Client SSNs in this system are a data feed from the FLORIDA system. There is no direct SSN collection into this system by the Department.
12. Dashboard – Collects and displays information collected by other systems. There is no direct SSN collection into this system by the Department.
13. Alcohol, Drugs, and Mental Health Data Warehouse – This is the official data repository for substance abuse and mental health (SAMH) data from the SAMH providers. Clients are advised by the providers during enrollment that their information, including SSNs will be used for treatment, payment, and operations, and will be shared with the Department. There is no direct SSN collection into this system by the Department
14. Substance Abuse Mental Health – Clients are advised by the providers during enrollment that their information, including SSNs will be used for treatment, payment, and operations, and will be shared with the Department. There is no direct SSN collection into this system by the Department.
15. Applicant Tracking Information System – This system and its data belong to the Agency for Persons with Disabilities (APD). The Department has been hosting the servers in our SunCoast data center. There is no direct collection of any data into this system by the Department. The application and database are in the process of being transferred to APD as of June 2015.
16. Funds Accountability System – This is a Community-Based Care (CBC) system. The Department hosts the servers in our SunCoast data center.
17. Home Care for the Disabled Vouchering System – This is an accounting vouchering system that tracks subsidy payments made to family members providing in-home care to disabled adults. SSNs stored in this system are used as the Employer Identification Numbers (EIN) required by DFS for payments. The Home Care for Disabled Adults Application Form collects the SSNs stored in this system.
18. IT Security/Risk Mitigation Service – A written statement of the purpose for SSN collection is provided at the time it is collected.

Office of General Services Response: The Offices of General Services and Information Technology Services will coordinate with the Assistant Secretary for Administration and Office of General Counsel to formalize operating procedures governing collection and use of Social Security Numbers. A draft operating procedure has been developed and will be further refined and reviewed to ensure compliance with statutory requirements.

Additionally, the Office of General Services will continue its work with the Program Areas to update forms that require collection of Social Security Numbers so that they meet statutory requirements. This effort will include the deletion of several forms no longer needed as indicated by the survey conducted in April 2015.

SELECTED ADMINISTRATIVE ACTIVITIES

Finding No. 6: Department controls over employee access to the Florida Online Accounting Information Resource Subsystem (FLAIR) and the Department's network needed improvement. Additionally, employee separation checklists used to account for the return of all State-owned property, files, records, and work product for employees separating from Department employment were not always timely or properly completed.

Recommendation: We again recommend that Department management establish policies and procedures requiring periodic reviews of FLAIR access privileges to aid in the identification and resolution of any instances where excess or incompatible privileges have been granted or access privileges are no longer needed. We also recommend that Department management ensure that all employee separation checklists are timely and appropriately completed, and that FLAIR and network access privileges are timely deactivated upon a user's separation from Department employment.

Response: The Office of Financial Management will establish policies and procedures requiring periodic reviews of FLAIR access privileges to aid in the identification and resolution of any instances where excess or incompatible privileges have been granted or access privileges are no longer needed and requiring timely deactivation of FLAIR access upon a user's separation from Department employment by September 30, 2015.