REPORT NO. 2014-188
APRIL 2014

DEPARTMENT OF CHILDREN AND FAMILIES

DOMESTIC VIOLENCE PROGRAM, TELEWORK PROGRAM, AND SELECTED ADMINISTRATIVE ACTIVITIES

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF CHILDREN AND FAMILIES

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

Esther Jacobo, Interim	From July 19, 2013
David Wilkins	Through July 18, 2013

The audit team leader was Frank Becton, CPA, and the audit was supervised by Karen Van Amburg, 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 can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF CHILDREN AND FAMILIES

Domestic Violence Program, Telework Program, and Selected Administrative Activities

SUMMARY

This operational audit of the Department of Children and Families (Department) focused on Department activities and functions related to the Domestic Violence Program and the Telework Program and selected administrative activities. Our audit disclosed the following:

DOMESTIC VIOLENCE PROGRAM

Finding No. 1: Department monitoring of the Florida Coalition Against Domestic Violence (Coalition) was not always properly documented or sufficient to ensure that the Coalition complied with contractual terms and applicable State laws and Federal regulations.

TELEWORK PROGRAM

Finding No. 2: The Department could not provide written telework agreements for some employees participating in the Department's Telework Program. Additionally, teleworkers' performance evaluations did not always include required notations to evidence the continuing appropriateness of the telework arrangements.

Finding No. 3: The Department did not always document the assignment and return of laptop computers for teleworking employees. Additionally, Department policies and procedures were not sufficient to ensure that terminated or transferred Telework Program employees' laptop and desktop computers were timely sanitized to remove sensitive data or that documentation of the sanitization was maintained.

Finding No. 4: The Department did not always properly document the timely review of teleworker background screening results and, in some instances, the dates that fingerprints were submitted for background screenings were inaccurately recorded in People First.

SELECTED ADMINISTRATIVE ACTIVITIES

Finding No. 5: The Department had 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 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 and did not always include all the required elements.

BACKGROUND

State law[1] 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, 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

[1] Section 20.19, Florida Statutes.

regions in the areas of fiscal, budget, contract management, and general services and is responsible for ensuring Statewide compliance and adherence to State laws and Federal regulations.

FINDINGS AND RECOMMENDATIONS

Domestic Violence Program

Pursuant to State law[2] the Department is to provide services relating to domestic violence. 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; certifies and provides quality assurance, technical assistance, and training for the 42 certified domestic violence centers located throughout the State; and contracts with the Florida Coalition Against Domestic Violence (Coalition) for the coordination, delivery, management, and evaluation of domestic violence services. The certified domestic violence centers 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 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 enters into subcontracts with traditional direct service providers, the criminal justice system, and professional associations to support its activities and accomplish its responsibilities.

For the 2012-13 fiscal year, the Department budgeted $31,008,216 for the Domestic Violence Program, including $18,805,367 from Federal sources[3] and $12,202,849 from State sources. State funding sources included fees assessed on marriage licenses[4] and dissolutions of marriage,[5] fines related to violations of injunctions for protection against domestic violence,[6] and general revenue. Of the amount budgeted for the 2012-13 fiscal year, the Department allocated $30,275,620 (97.6 percent) to the Coalition, of which the Coalition allocated $20,074,485 (66.3 percent) to the certified domestic violence centers. The Coalition utilized the remaining $10,201,135 for other direct services and administration.

Finding No. 1: Department Monitoring of the Coalition

State law[7] requires the Department to establish a contract monitoring unit and a monitoring process that includes, but is not limited to:

- 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.
- Conducting analyses of the performance and compliance of an external service provider by means of desk reviews if the external service provider will not be monitored on-site during the fiscal year.
- Providing a written report presenting the results of the monitoring within 30 days after the completion of the on-site monitoring or desk review.

[2] Section 20.19(3)(a)4., Florida Statutes.
[3] 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/Battered Women's Shelters (CFDA No. 93.671).
[4] Section 741.01, Florida Statutes.
[5] Section 28.101, Florida Statutes.
[6] Section 741.30, Florida Statutes.
[7] Section 402.7305(4), Florida Statutes.

The Department established policies and procedures for administrative and programmatic contract oversight[8] to help ensure compliance with State law. The contract oversight policies and procedures included instructions on 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. The Contract Oversight Unit manager was to review the proposed monitoring plan with the monitoring team leader and approve the plan prior to the start of the on-site review. After plan 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.

The Department's contracts with the Coalition were for $29.2 million for the 2011-12 fiscal year and $30.3 million for the 2012-13 fiscal year. The Department's monitoring of the Coalition contracts consisted of a desk review for the 2011-12 fiscal year and an on-site review for the 2012-13 fiscal year. Our evaluation of the Department's monitoring efforts disclosed that the Department did not maintain sufficient documentation supporting the conclusions made regarding Coalition compliance with the contract terms and applicable State and Federal requirements. Specifically:

- The Department could not provide documentation supporting the conclusions of the desk review performed for the 2011-12 fiscal year. Our audit tests disclosed that the desk review was evidenced by a single form indicating there were no concerns with the performance or compliance of the Coalition; however, no documentation identifying the documents reviewed or the specific evaluation criteria utilized to assess the Coalition's performance was available. We also noted that Department policies and procedures did not require monitors to maintain documentation supporting desk review conclusions.
- The Department did not always document the performance of planned on-site monitoring procedures or that monitoring efforts were complete and included all elements required by State law. Specifically:
    - For the 2012-13 fiscal year contract, the Department prepared a monitoring plan, performed on-site monitoring, and issued a report to the Coalition with no findings identified. The monitoring plan developed by the Department included seven specific areas to be examined during the on-site monitoring. Our review of Department documentation for the on-site monitoring disclosed that the monitor did not document examination efforts for three of the seven areas listed on the monitoring plan: the monthly report of Domestic Violence Program activity, the database for information on the status of domestic violence advocate-victim privilege, and Coalition subcontracting requirements and subcontractor monitoring. In response to our audit inquiry, Department management confirmed that there was no evidence that monitoring was performed for those three areas. In addition, we noted that three of the five monitoring tools completed by the Department monitor contained no evidence of supervisory review as Department procedures did not require supervisory review of the monitor's work.
    - The monitoring plan did not include an evaluation of the Coalition's allocation of funding to the certified domestic violence centers. State law[9] specifies that all funds collected and appropriated to the Domestic Violence Program for certified domestic violence centers are to be distributed annually according to a formula approved by the Department. State law further provides that, in developing the formula, the factors of population, rural characteristics, geographical area, and the incidence of domestic violence are to be considered. Department management indicated in response to our audit inquiry that the Department had not reviewed the amounts allocated by the Coalition to the certified domestic violence centers since at least March 2012. Our audit procedures also disclosed that the formula used by the Coalition to allocate funds to the certified domestic violence centers had last been updated in July 2004. Subsequent to our audit inquiry in April 2013, the Coalition prepared and the Department approved a new allocation formula in May 2013 that incorporated information from the 2010 United States Census.
    - Although Department policies and procedures provided for administrative and programmatic monitoring of contract providers, the policies and procedures did not sufficiently address how the statutorily

[8] Department Operating Procedure 75-8, *Procurement and Contract Management, Policies and Procedures of Contract Oversight.*
[9] Section 39.905(7)(a), Florida Statutes.

required[10] monitoring of contract providers' fiscal activities was to be performed. As a result, the Department's monitoring plan that established the scope of the on-site monitoring of the Coalition did not include the monitoring of Coalition fiscal activities. Examples of fiscal areas that were not reviewed included, but were not limited to, indirect costs and Coalition personnel compensation packages.

Absent policies and procedures that provide detailed instructions for monitoring contract provider fiscal activities, require documentation to support monitoring conclusions, and provide for supervisory review to ensure monitoring is conducted as planned, the Department has reduced assurance that the monitoring performed will be sufficient to identify deficiencies in the Coalition's compliance with contractual requirements and State law and Federal regulations. Additionally, the exclusion of the Coalition's allocation of funds to the State's certified domestic violence centers from the Department's monitoring process prevents the Department from verifying that funds are allocated by the Coalition to the centers in accordance with the Department-approved allocation formula.

Recommendation: We recommend that Department management strengthen contract monitoring policies and procedures to ensure that: monitoring of contract provider fiscal activities is performed, supervisory reviews of the monitor's work are conducted and documented, and the conclusions made during desk reviews are adequately supported. Additionally, we recommend that Department management ensure that when monitoring the Coalition, the allocation of funds to the domestic violence centers be addressed.

Telework Program

State law[11] 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.[12] 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[13] governing the Telework Program. At March 5, 2013, the Department had designated in People First 1,353 of its 11,279 employees as teleworkers. The Department's telework employees included abuse registry counselors, public assistance application processors, and interviewing clerks.

Finding No. 2: Teleworker Agreements and Performance Evaluations

State law[14] requires that State agencies 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

[10] Section 402.7305(4)(b), Florida Statutes.
[11] Section 110.171, Florida Statutes. Prior to July 1, 2012, State law included similar provisions for the State Employee Telecommuting Program.
[12] 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.
[13] Department Operating Procedure 60-40, *Personnel, Alternative Work Locations*.
[14] Section 110.171(4), Florida Statutes.

responsibilities of the position remain suitable for a telework arrangement. State law[15] also authorizes State agencies to require written agreements between teleworkers and the agency that provide for the termination of an employee's participation in a Telework Program if the employee's continued participation is not in the best interest of the agency.

Department Telework Program policies and procedures[16] contained requirements for establishing annual written agreements between the Department and each teleworker, evaluating teleworker performance, and annually assessing whether the telework arrangement was working satisfactorily and should be continued.

Department policies and procedures also required that each teleworker maintain an overall rating of "satisfactory" or higher on their annual performance evaluation in order to remain in the Telework Program. The employee performance evaluations were to be performed on an annual basis during the 60-day period beginning on August 1 of each year.[17] In addition, during the 2011-12 fiscal year performance evaluation period, the Department implemented a process requiring that the annual performance evaluation document for each teleworker contain 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.[18]

As part of our audit, we reviewed Department documentation, including telework agreements and performance evaluations, related to 40 employees who participated in the Department's Telework Program during the period July 2011 through February 2013. We found that:

- For 7 teleworkers, the Department could not provide a written telework agreement effective for the 2011-12 annual evaluation period.
- For 11 of the 34 applicable 2011-12 fiscal year performance evaluations (6 of the 40 employees did not become teleworkers until the 2012-13 fiscal year), the employee's supervisor had not included the required notation stating whether or not the telework arrangement should be continued for another year. In response to our audit inquiry, Department Central Office Human Resources staff indicated that supervisors had not always followed Department guidance relating to performance evaluations for teleworkers.

Written telework agreements and 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.

Recommendation: We recommend that Department Central Office Human Resources staff continue to communicate to appropriate supervisory staff the requirements outlined in Department policies and procedures to help ensure that telework agreements are executed and that decisions to continue teleworking arrangements are properly documented in the employees' annual performance evaluations.

Finding No. 3: Teleworker Computer Assignment and Data Security

The Department established security controls to protect, and ensure the appropriate use and maintenance of, State-owned computer equipment used by teleworkers. In accordance with Department policies and procedures,[19] supervisors were to require employees who were assigned State-owned laptop computers to complete and sign a

[15] Section 110.171(5), Florida Statutes.
[16] Department Operating Procedure 60-40, *Personnel, Alternative Work Locations.*
[17] Department Operating Procedure 60-35, *Personnel, Performance Evaluation Program for Career Employees, and Selected Exempt Service Employees Covered by a Current Collective Bargaining Agreement.*
[18] Department Memorandum, dated July 10, 2012: *Annual Performance Evaluations 2012 and Telework Agreements.*
[19] Department Operating Procedure 80-2, *Property Management.*

State-Owned Tangible Personal Property Assignment (CF 1941) form to document custody of the laptop. Supervisors were to submit the completed and signed form to the appropriate property consultant within 10 days of assignment of the laptop computer. 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.

The Department also established policies and procedures outlining required processes to ensure the security of sensitive data.[20] Department employees routinely access sensitive data, such as social security numbers and child abuse records, relating to Department clients when performing their assigned duties. 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 of the sanitization and the method of sanitation used be documented.

As part of our audit, we requested for examination CF 1941 forms evidencing the assignment of laptop computers to 40 employees who were teleworking as of March 5, 2013. Additionally, we requested CF 1941 forms evidencing the return of laptop computers for 12 teleworkers who had separated from Department employment during the period July 2011 through February 2013 and 10 employees who were required to turn in their laptops when they transferred from a teleworking position to another position within the Department during that period. Although requested, the Department was unable to provide CF 1941 forms demonstrating the assignment of laptop computers to 11 of the active teleworkers, or the return of laptop computers by 14 former teleworkers (7 terminated teleworkers and 7 transferred teleworkers).

We also requested documentation to evidence the sanitization of sensitive data for 34 laptop and 9 desktop computers assigned to 30 former teleworkers who, during the period July 2011 through February 2013, either separated from Department employment (14 former teleworkers) or transferred from a teleworking position to another position (16 former teleworkers). Our audit inquiries and review of available Department documentation disclosed that:

- According to Department staff, 1 desktop and 3 laptop computers were in secure storage at the time of our audit field work; however, none of the 4 computers had been sanitized to remove sensitive data. Department records indicated that, as of May 23, 2013, the 4 computers had been in secure storage from 84 to 358 days.
- For 2 other desktop and 11 other laptop computers, the Department was unable to provide documentation evidencing the sanitization of sensitive data.
- For one former teleworker, the Department did not maintain records documenting the type of computer equipment assigned or evidencing that the equipment had been turned in and sanitized.

Although Department policies and procedures required sanitization of sensitive data from computer equipment, the policies and procedures did not establish a time frame within which the sanitization should occur.

Storing computer equipment that has not been sanitized increases the risk of unauthorized access of sensitive data. In addition, absent proper documentation of the assignment, custody, and sanitization of computer equipment, Department management has reduced assurance that Department staff have complied with the policies and procedures designed to protect the Department's sensitive data and information technology resources.

Recommendation: We recommend that Department management update policies and procedures to include a required time frame for sanitizing the computer equipment returned by Department staff. In addition, we recommend that Department management continue to emphasize to staff the requirements for documenting the assignment, custody, and sanitization of computer equipment.

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

Finding No. 4: Teleworker Background Screenings

State law[21] requires that each State agency designate those positions that, because of the special trust, responsibility, or sensitive location, require a level 2 background screening[22] as a condition of employment and continued employment. The Department designated all of its positions as positions of special trust, responsibility, or sensitive location, and established employee background screening policies and procedures requiring that all selected applicants be screened prior to initial employment and that employees be re-screened at no more than 5-year intervals as a condition of continued employment.[23]

Department policies and procedures specified that background screening coordinators were to submit the fingerprints of prospective employees to the Department of Law Enforcement for processing and review all criminal history record information to determine if there were any disqualifying arrests pending disposition, convictions, or court pleas. For prospective employees with no criminal history, the background screening coordinator was to issue a clearance letter or other documentation evidencing that the candidate had successfully completed the background screening and the letter or documentation was to be placed in the employee's personnel file. Additionally, Department policies and procedures provided that the applicable Human Resources Manager was responsible for updating the People First Fingerprints Overview screen to reflect the date the fingerprints were submitted and the date the background screening was completed. In response to our audit inquiry, Department management indicated that they planned to use the dates in the Fingerprints Overview screen to identify when employees were due for re-screening.

As part of our audit, we examined personnel files and People First records for 40 teleworkers to determine whether the Department had timely requested and reviewed background screenings for each employee, whether documentation prepared by background screening coordinators was timely prepared and appropriately included in the employees' personnel files, and whether People First had been appropriately updated. Our examination disclosed that:

- For 3 of the 40 teleworkers, although the People First Fingerprints Overview screen indicated that background screenings had been completed, the employees' personnel files did not contain, and the Department was unable to provide, clearance letters or other documentation evidencing that the results of the background screenings had been reviewed by a background screening coordinator.
- For the 37 teleworkers for whom background screening documentation was available, we noted:
  - Clearance letters, or other documentation evidencing the review of background screening results, were not included in 32 of the employees' personnel files. Subsequent to our audit inquiry, the Department provided documentation evidencing that background screenings had been conducted and reviewed; however, the Department could not demonstrate that the background screenings for 17 of the 32 teleworkers had been timely reviewed.
  - The fingerprints submittal dates entered into the People First Fingerprints Overview screen did not agree with the dates on the clearance letters for 9 teleworkers.

In response to our audit inquiry, Department staff indicated that the background screening coordinators had not followed Department policies and procedures regarding the issuance and maintenance of clearance letters or other

[21] Section 110.1127(2)(a), Florida Statutes.
[22] As defined in Section 435.04, Florida Statutes, a level 2 background screening includes, but need not be limited to, fingerprinting for Statewide criminal history records checks through the Department of Law Enforcement, national criminal history records checks through the Federal Bureau of Investigation, and may include local criminal records checks through local law enforcement agencies.
[23] Department Operating Procedure 60-25, *Personnel, Employee Security Background Screening.*

documentation demonstrating that the results of the background screening had been reviewed. Additionally, Department staff indicated that, although the Human Resources managers had received verbal instructions, the Department's written policies and procedures did not specifically address how to enter the background screening dates into People First.

Absent documentation of the timely review of employee background screening results, the Department cannot demonstrate that employees have the appropriate backgrounds to be in positions of special trust, responsibility, or sensitive location. Additionally, absent accurate data in People First, the Department's ability to rely on People First to identify when employee background screenings need to be re-performed is limited.

Recommendation: We recommend that Department management ensure that background screening coordinators timely issue and place background screening clearance letters or other equivalent documentation in the applicable employee personnel files, in accordance with Department policies and procedures. We also recommend that Department management update policies and procedures to provide specific written instruction for entering in People First the dates fingerprints are submitted and background screenings are completed.

Selected Administrative Activities

Finding No. 5: Collection of Social Security Numbers

The Legislature has acknowledged in State law[24] 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[25] that State agencies may 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.

We noted that the Department had not adopted written policies and procedures relating to the collection and use of SSNs. Additionally, we found that the Department could not demonstrate the statutorily required review of its SSN collection activities. Department management conducted a Departmentwide survey in April 2013, subsequent to our audit inquiry, to identify all forms and information technology systems which collected SSNs. The survey results showed that 203 Department forms and 51 Department information technology systems potentially collected SSNs. However, Department management reported in response to our audit inquiry that, as of December 2013, the process of evaluating the survey results to determine the appropriate action for each of the potential SSN collection points had not been completed.

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

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

Recommendation: We recommend that Department management establish written policies and procedures regarding the collection and use of individuals' SSNs, timely finalize the review of the Departmentwide survey of SSN collection activities, and take appropriate steps to demonstrate compliance with applicable statutory requirements.

Finding No. 6: Information Technology Access Controls

The Department utilizes the Florida Accounting Information Resource Subsystem (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. Accordingly, FLAIR access should be: (1) limited to properly authorized employees, (2) appropriate for the employee's assigned duties and responsibilities, and (3) promptly revoked when employees separate from the Department or are reassigned to positions no longer requiring FLAIR access.

Department procedures[26] required that supervisors notify the appropriate Security Manager or Officer to delete security access to assigned computer and data systems, including those accessible via the Department's network, within 24 hours of an employee's separation. The procedures also required the use of an employee separation checklist to identify and account for all State property, files, records, and work product. Headquarters and each Region, Circuit, and Mental Health Facility were to either utilize the Department's standard employee separation checklist or develop and utilize an employee separation checklist that contained all of the elements from the standard checklist. The standard employee separation checklist included a checkbox for notifying the FLAIR Security Manager or Officer to delete the employee's FLAIR access and a checkbox for notifying the Network Manager to delete the employee's network access.

While Department procedures addressed the deletion of information technology access for separating employees, we noted that the Department had not established policies and procedures requiring the periodic review of employees' FLAIR access to identify and resolve any instances where excess or incompatible privileges had been granted or access was no longer needed. In addition, our tests of Department FLAIR and network access controls and review of Department employee access privileges disclosed that:

- Employees performing financial management functions had been granted update capabilities to incompatible functions in FLAIR. Our review of FLAIR access privileges for 22 Headquarters employees disclosed that 15 employees had update access to both the disbursement and cash receipts functions; 1 employee had update capabilities to both the vendor file function and the disbursement function; and 4 employees had update capabilities to both the fixed assets accounting and fixed assets custodial functions. These incompatible access privileges heighten the risk that errors or fraud may occur and not be timely detected.
- Access to FLAIR was not always timely revoked upon employment termination. We examined FLAIR access records for 66 employees with FLAIR update capabilities who separated from Department employment during the period July 2011 through February 2013. Our examination disclosed that FLAIR access privileges for 37 employees remained active from 2 to 400 days (an average of 49 days) after the employees' termination dates. Further, for 10 of the 37 terminated employees, we found that network access remained active for 10 to 52 days (an average of 33 days) after the employees' termination dates, and 5 of the 37 employees'

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

network access was still active as of November 5, 2013, although their employment had been terminated for 460 to 851 days. Our audit tests did not disclose any FLAIR transactions entered by the 37 employees subsequent to their termination dates.

- Employee separation checklists were not always timely or properly completed, and the checklists used did not always include all required elements. Our review of the separation checklists for 6 of the 37 employees for whom the Department had not timely removed FLAIR access privileges disclosed that:
  - Three employee separation checklists were completed 11, 19, and 114 days, respectively, after the employees' separation dates. For one of these three checklists, we also noted that the supervisor did not mark the box indicating that FLAIR access should be deleted.
  - Two separation checklists did not include all the elements of the Department's standard employee separation checklist, as a place to indicate that FLAIR access should be deleted was not included.

Without periodic and timely reviews of user access, the Department cannot be assured that FLAIR access privileges are appropriate and provided only to authorized employees. Additionally, absent effective procedures, including the timely and accurate completion of separation checklists that promote the prompt deactivation of employee access privileges upon employment termination, the Department is exposed to a greater risk of unauthorized disclosure, modification, or destruction of Department data and IT resources.

Recommendation: We 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 contain all the required information and are timely completed, and that FLAIR and network access privileges are timely deactivated upon employment termination.

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 2013 through October 2013, and selected actions through December 2013, 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 the activities and functions related to the Domestic Violence Program and the Telework Program, and selected Department 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 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:

Domestic Violence Program

- 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.
- For 10 of the 42 domestic violence centers certified by the Department during the 2011-12 fiscal year, evaluated application, certification, and assessment documentation to determine whether the Department had properly determined whether the domestic violence centers met certification eligibility requirements.
- Examined the two contracts between the Department and the Florida Coalition Against Domestic Violence (Coalition) in effect during the period July 2011 through February 2013 to determine whether the contract terms and conditions were sufficient to provide for compliance with applicable laws, rules, and regulations, and the appropriate delivery of Domestic Violence Program services.
- Examined documentation for six contract payments, totaling $13,870,965, made by the Department to the Coalition during the period July 2011 through February 2013 to determine whether the payments were accurate, correctly recorded, properly supported, and made after services were provided.
- Examined 16 of the 49 reports required to be submitted by the Coalition to the Department during the period July 2011 through February 2013 to determine whether the Department timely reviewed the reports for completeness and timeliness, and, if applicable, followed up on any deficiencies noted in the reports. The reports included areas such as subcontractor monitoring, service data, and quarterly expenditures.

- Evaluated the Department's processes for monitoring the Coalition, including the risk assessment process, the development and use of monitoring plans and monitoring tools, and the reporting of monitoring results, to determine whether the Department properly monitored the Coalition's compliance with contractual provisions and State laws and Federal regulations.
- Examined documentation related to the Department's cost price analysis for the 2012-13 fiscal year contract with the Coalition to evaluate whether the Department complied with guidance from the Department of Financial Services and whether the information utilized for the cost price analysis was sufficient to ensure that the costs associated with the contract were reasonable.
- Examined position descriptions, payroll records, and time sheets for the three Department employees with salaries totaling $411,524 charged to the Domestic Violence Program during the period July 2011 through February 2013 to verify that the employees worked on the Program.
- Surveyed the 42 certified domestic violence centers to ascertain the extent of the domestic violence centers' satisfaction with the Coalition and the Department.

Telework Program

- Reviewed applicable laws, rules, regulations, and Department policies and procedures, and interviewed Department personnel to gain an understanding of the Department's Telework Program operations.
- Performed inquiries, observations, inspections of documents and records to determine whether the Department had established and implemented controls necessary to administer the Telework Program.
- Examined records related to 40 Department teleworkers, judgmentally selected from the population of 1,353 employees designated as teleworkers in People First as of March 5, 2013, to determine whether the Department had documented the conduct of employee background screenings, provision of security awareness training, appropriate assignment of computer equipment and access privileges, execution of telework agreements, and monitoring of employee performance.
- Examined Department records related to 14 teleworkers who terminated employment with the Department during the period July 2011 through February 2013 to determine whether the computers assigned to the former employees had been sanitized to remove sensitive data in accordance with Department policies and procedures.
- Examined Department records for 16 employees who transferred from a teleworking position to another position during the period July 2011 through February 2013 to determine if the Department had appropriately updated People First to reflect that the employee was no longer teleworking and whether the computers assigned to the employees had been sanitized to remove sensitive data in accordance with Department policies and procedures.

Selected Administrative Activities

- Evaluated the timeliness of the deactivation of FLAIR access privileges for 66 Department employees who terminated employment during the period July 2011 through February 2013. Additionally, reviewed the separation checklists for 6 of the 37 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 36 Department employees with FLAIR access privileges to determine whether the access privileges were reasonable given the employees' job duties. In addition, from the population of approximately 446 Department employees with FLAIR update privileges, reviewed records for 22 employees assigned to the Department Headquarters office to determine whether any of the employees had incompatible or excessive FLAIR update privileges.
- Evaluated Department policies, procedures, and processes for collecting and utilizing individuals' social security numbers to determine the extent of Department compliance with the applicable requirements of State law.
- Observed, documented, and evaluated the effectiveness of selected processes and procedures for the assignment and use of motor vehicles with acquisition costs totaling approximately $5.7 million as of December 31, 2012. Examined records related to five expenditures, totaling $134,449, for the acquisition of

motor vehicles to determine whether the acquisitions complied with State law, were appropriately documented, and served an authorized purpose.

- Observed, documented, and evaluated the effectiveness of selected processes and procedures for ensuring the management of Department tangible personal property in compliance with applicable laws and rules. The acquisition costs of Department tangible personal property totaled approximately $56.2 million as of June 30, 2012.
- Observed, documented, and evaluated the effectiveness of selected processes and procedures for the Department's purchasing processes.
- Observed, documented, and evaluated the effectiveness of selected processes and procedures for the Department's acquisition, assignment, and use of wireless devices with related costs totaling approximately $3.1 million for the 2011-12 fiscal year.

Overall, we:

- 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.

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.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a response letter dated March 28, 2014, the Interim Secretary of the Department provided responses to our audit findings and recommendations. The Interim Secretary's response is included as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

State of Florida
Department of Children and Families

Rick Scott
Governor

Esther Jacobo
Interim Secretary

March 28, 2014

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

Dear Mr. Martin:

Thank you for your March 6 letter and the accompanying preliminary and tentative audit findings and recommendations on the audit of *Domestic Violence Program, Telework Program, and Selected Administrative Activities.* 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, Ms. Cyndee Odom, Director of Domestic Violence, at (850) 922-0185, Ms. Dennise Parker, Director of Human Resources, at (850) 488-1700, Ms. Kimberly McMurray, Interim Director of Financial Management, at (850) 717-4760, or Mr. Joe Vastola, Interim Chief Information Officer, at (850) 320-9265.

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,

Esther Jacobo
Interim Secretary

Attachment

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

RESPONSE TO PRELIMINARY AND TENTATIVE FINDINGS

DEPARTMENT OF CHILDREN AND FAMILIES
DOMESTIC VIOLENCE PROGRAM, TELEWORK PROGRAM,
AND SELECTED ADMINISTRATIVE ACTIVITIES

OPERATIONAL AUDIT

DOMESTIC VIOLENCE PROGRAM

Finding No. 1: Department monitoring of the Florida Coalition Against Domestic Violence (Coalition) was not always properly documented or sufficient to ensure that the Coalition complied with contractual terms and applicable State laws and Federal regulations.

Recommendation: We recommend that Department management strengthen contract monitoring policies and procedures to ensure that: monitoring of contract provider fiscal activities is performed, supervisory reviews of the monitor's work are conducted and documented, and the conclusions made during desk reviews are adequately supported. Additionally, we recommend that Department management ensure that when monitoring the Coalition, the allocation of funds to the domestic violence centers be addressed.

Response: The Office of Domestic Violence Program in collaboration with the Office of Contracted Client Services have reviewed the Auditor General's recommendation and will continue to work together to enhance contract monitoring activities.

Regarding the recommendation that Department management strengthen contract monitoring policies and procedures to ensure that monitoring of contract provider fiscal activities is performed:

- The Department has a Single Audit Unit that performs desk reviews of single audits of contract providers prepared by Independent CPA firms. This is done to verify compliance with OMB Circular A-133 and §215.97, Florida Statutes, (F.S.), as specified in the contract audit attachment. The Single Audit Unit has completed current desk reviews of the Coalition's recent audits.
- While §402.7305, F.S., does not require the Department to conduct fiscal monitoring of every provider as part of its contract monitoring, the Department will consider what activities may also be necessary for fiscal monitoring.
- The Department plans to identify appropriate measures and develop tools to monitor fiscal activities when this is appropriate, along with identifying the available resources (the Contract Oversight Unit among others) to perform fiscal monitoring of contract providers.

Regarding the recommendation that Department management strengthen contract monitoring policies and procedures to ensure that supervisory reviews of monitor's work are conducted and documented and the conclusions made during desk reviews are adequately supported:

- The Department is in the process of updating its monitoring procedures to better address requirements for quality assurance by team leaders, to ensure tools are reviewed and any findings are supported by appropriate documentation. Full implementation of this plan will be accomplished following a statewide meeting and training in July 2014.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

- The Department has redesigned the desk review process to include specific identification of the documents and information reviewed from the contract manager's file in drawing conclusions, such that an auditor could also obtain the same document from the contract file if desired. Individuals involved in the contract, including the contract manager, are surveyed as part of the process, and the returned survey(s) are retained as working papers.

Regarding the recommendation that Department management ensure that when monitoring the Coalition, the allocation of funds to domestic violence centers be addressed:

- The Department will include an evaluation of the Coalition's allocation of funding to the certified domestic violence centers based on the approved formula in the scope of the next monitoring of the Coalition or review through another mechanism, if more appropriate.

TELEWORK PROGRAM

Finding No. 2: The Department could not provide written telework agreements for some employees participating in the Department's Telework Program. Additionally, teleworkers' performance evaluations did not always include required notations to evidence the continuing appropriateness of the telework arrangements.

Recommendation: We recommend that Department Central Office Human Resources staff continue to communicate to appropriate supervisory staff the requirements outlined in Department policies and procedures to help ensure that telework agreements are executed and that decisions to continue teleworking arrangements are properly documented in the employees' annual performance evaluations.

Response: Based on our current process for extension of telework agreements, we concur with the recommendations to continue to communicate to appropriate supervisory staff -

- the requirements outlined in Department policies and procedures to help ensure that telework agreements are executed
- that decisions to continue the telework arrangements are properly documented in the employees' annual performance evaluations.

An executed Telework Agreement is required for all new optional teleworkers. We are approaching the annual review and extension of telework arrangements with the next annual employee performance evaluations to be completed within 60 days after the upcoming ending evaluation period of June 30, 2014. We will take the opportunity to reiterate and emphasize the requirements as well as the process for decisions to continue the telework arrangement.

In the event we change our process for extensions of telework agreements, we will communicate any such changes to affected staff to insure there is a clearly communicated process for extensions. We will reiterate and emphasize this requirement in a Department communication regarding completion of the upcoming annual performance evaluations for the period ending June 30, 2014.

Finding No. 3: The Department did not always document the assignment and return of laptop computers for teleworking employees. Additionally, Department policies and procedures were not sufficient to ensure that terminated or transferred Telework Program employees' laptop and desktop computers were timely sanitized to remove sensitive data or that documentation of the sanitization was maintained.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation: We recommend that Department management update policies and procedures to include a required time frame for sanitizing the computer equipment returned by Department staff. In addition, we recommend that Department management continue to emphasize to staff the requirements for documenting the assignment, custody, and sanitization of computer equipment.

Office of General Services Response: The Office of General Services, in conjunction with Human Resources and the Office of Information Technology Services, will review all applicable procedures and forms related to the assignment of equipment to telecommuters. These include:

- CFOP 80-2: Property Management;
- CFOP 50-2: Security of Data and Information Technology Resources;
- CFOP 60-40, Chapter 9: Alternative Work Locations;
- Form CF1941: State Owned Tangible Personal Property Assignment; and
- Form CF1916: Telecommuting Agreement.

Within 90 days, the Department will make updates to operating procedures, forms and operational practices to ensure that equipment is accounted for and documented in a timely manner.

Office of Information Technology Services Response: The Office of Information Technology Services will review any applicable procedures to closer match the recommendations in the National Institute of Standards and Technology (NIST) Special Publication 800-88, Guidelines for Media Sanitization as applicable to sanitation of computer hard drives in a timely manner.

Within 90 days, the Department will make updates to operating procedures, forms and operational practices to ensure sanitation when necessary will be completed within a timely manner.

Finding No. 4: The Department did not always properly document the timely review of teleworker background screening results and, in some instances, the dates that fingerprints were submitted for background screenings were inaccurately recorded in People First.

Recommendation: We recommend that Department management ensure that background screening coordinators timely issue and place background screening clearance letters or other equivalent documentation in the applicable employee personnel files, in accordance with Department policies and procedures. We also recommend that Department management update policies and procedures to provide specific written instructions for entering in People First the dates fingerprints are submitted and background screenings are completed.

Response: We concur with the recommendation. The Department has implemented a Human Resources Shared Services (HRSS) delivery model. One process change that has occurred with implementation of HRSS is the use of an Appointment Checklist, which includes a background screening clearance block. The HRSS Center will not process an employee appointment and put an employee on payroll unless the selected applicant has been background screened and cleared the screening. The Appointment Checklist includes the Date Submitted and the Date Completed. The completed Appointment Checklist is incorporated into the employee's personnel file, and becomes a part of the employee's official personnel record.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

The Background Screening section of the Appointment Checklist includes the following statement:

> If the employee being appointed has not been screened since 8/1/2010, they must be successfully re-screened before the appointment will be approved. (underline added for emphasis).

Note: The background screening law changed effective 8/1/2010 and now requires that all selected candidates pass the required background screening before beginning employment.

The Appointment Checklist constitutes the equivalent documentation of background screening clearance, and documents that the selected applicant has cleared the background screening process.

Note: This background screening process applies to all employees—not just teleworkers.

CFOP 60-25, Chapter 2, §2-5 n., Employee Security Background Screening, was last revised effective November 15, 2012, and includes the following specific information related to entering into People First:

> The servicing Human Resources employee relations representative is responsible for ensuring that the People First "Fingerprints Overview" screen is updated with current information for each employee who is rescreened. For new employees, the Human Resources Shared Services Center representative will ensure that the information is input into People First with current information.

We will ensure there are specific written instructions for Human Resources staff to accomplish this policy.

SELECTED ADMINISTRATIVE ACTIVITIES

Finding No. 5: The Department had 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.

Recommendation: We recommend that Department management establish written policies and procedures regarding the collection and use of individuals' SSNs, timely finalize the review of the Departmentwide survey of SSN collection activities, and take appropriate steps to demonstrate compliance with applicable statutory requirements.

Response: Collection and Use of SSNs is a statewide issue for the Department. Management will request the General Counsel to opine on the correct avenue to address the policies and procedures issue.

Upon review of the survey, there are 203 DCF forms and 19 DCF systems statewide that capture SSNs.

Of the 19 DCF systems that capture SSNs, five (FLORIDA, Information Delivery System Query Facility, Child Death Review, IT Security Risk Mitigation Service, and FSFN) did not meet statutory requirements. We are reviewing the current security policies requiring collection of

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

SSNs as part of the security request process to determine whether this requirement is imperative for the performance of the department's duties and responsibilities as prescribed by law. For the FLORIDA System, the Department met with the vendor who was unable to provide an acceptable solution. We will work with our O&M contractor (Deloitte) and IT staff to determine the feasibility of developing and implementing a solution in-house. DCF is following up with the Feds on an issue related to the modification of historic data which will affect the actual solution to be proposed. The time frame for the resolution has not yet been established.

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 and did not always include all the required elements.

Recommendation: We 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 the Department management ensure that all employee separation checklists contain all the required information and are timely completed, and that FLAIR and network access privileges are timely deactivated upon employment termination.

Response: The Department will establish policies and procedures requiring periodic reviews of FLAIR access privileges and will review procedures to ensure FLAIR access privileges are timely deactivated upon employment termination. Also, the Department will reinforce the current procedures to ensure the separation checklists contain all the required information and are timely completed.

For network access privileges, a daily report (HRTS-People First Daily Load Results & Terminated Employee File) is generated and sent to all DCF Security Officers (statewide). The Security Officers use this report to confirm access to the Department's network has been terminated. In addition, SOP S-12, Procedure for Review of Access Levels of Current Employees and Contractors states that supervisors must periodically review the access levels of current employees to ensure that current employees still require the granted access level necessary to perform their duties. The principle of least privilege must be followed. This review must be done at least once annually. The supervisor must report all access level discrepancies immediately to the Security Officer.