

**New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor**

**Department of Children and Families
New Jersey Statewide Protective Investigation
Reporting and Information Tool (NJ SPIRIT)**

May 15, 2013 to July 31, 2015

**Stephen M. Eells
State Auditor**



LEGISLATIVE SERVICES COMMISSION

ASSEMBLYMAN
VINCENT PRIETO
Chairman

SENATOR
THOMAS H. KEAN, JR.
Vice-Chairman

SENATE

CHRISTOPHER J. CONNORS
NIA H. GILL
ROBERT M. GORDON
JOSEPH M. KYRILLOS, JR.
JOSEPH PENNACCHIO
STEPHEN M. SWEENEY
LORETTA WEINBERG

GENERAL ASSEMBLY

JON M. BRAMNICK
ANTHONY M. BUCCO
JOHN J. BURZICHELLI
THOMAS P. GIBLIN
LOUIS D. GREENWALD
SCOTT T. RUMANA

OFFICE OF THE STATE AUDITOR
(609) 847-3470
FAX (609) 633-0834

STEPHEN M. EELLS
State Auditor

GREGORY PICA
Assistant State Auditor

JOHN J. TERMVNA
Assistant State Auditor

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES

OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

PERI A. HOROWITZ
Executive Director
(609) 847-3901

The Honorable Chris Christie
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Vincent Prieto
Speaker of the General Assembly

Ms. Peri A. Horowitz
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of Children and Families, New Jersey Statewide Protective Investigation Reporting and Information Tool (NJ SPIRIT) for the period of May 15, 2013 to July 31, 2015. If you would like a personal briefing, please call me at (609) 847-3470.

Stephen M. Eells
State Auditor
November 16, 2015

Table of Contents

Scope.....	1
Objectives	1
Methodology.....	1
Conclusions.....	2
Background.....	2
Findings and Recommendations	
System Documentation.....	3
User Access.....	4
NJ SPIRIT User Accounts	4
Disaster Recovery Plan.....	5
Auditee Response.....	6

Scope

We have completed an audit of the Department of Children and Families (DCF), New Jersey Statewide Protective Investigation, Reporting and Information Tool (NJ SPIRIT), for the period May 15, 2013 to July 31, 2015. Our audit evaluated selected information technology general and application controls related to the processing of case management data and financial transactions through this system.

Objectives

The objectives of our audit were to determine the adequacy of general and application controls for change management, system backup and recovery, contingency planning and disaster recovery, system security, and data integrity which included data origination, data input, data processing, and data output.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section I, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. 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. Additional guidance for conduct of the audit was provided by *Control Objectives for Information and related Technology* (CobIT) issued by the IT Governance Institute, the *Federal Information System Controls Audit Manual* (FISCAM) issued by the United States Government Accountability Office (GAO), and the International Organization for Standardization (ISO).

In preparation for our testing we studied circular letters promulgated by the Department of the Treasury and policies and guidelines of the agency. Provisions that we considered significant were documented, and compliance with those requirements was verified by interview, observation, and tests of controls. In addition, we obtained and reviewed system administration, security, and user manuals. Functions we considered significant were documented and implementation of those features was verified. We also interviewed agency personnel to obtain an understanding of the internal controls.

A nonstatistical sampling approach was used. Our tests of selected general and application controls were designed to provide conclusions about the adequacy of those controls in place for change management, system backup and recovery, contingency planning and disaster recovery, system security, and data integrity.

Conclusions

We found that the DCF Information Technology management and staff take administering and securing the application very seriously and have adequate controls and processes in place to provide for change management, system backup and recovery, contingency planning and disaster recovery, system security, and data integrity. We did note, however, some of these controls and processes can be improved.

Background

The NJ SPIRIT is a comprehensive, automated case management tool that integrates various aspects of case practice in a single statewide system, including intake, investigation, case planning, case recording, resource management, service delivery tracking, and financial management. The primary business purpose of the application is to be the electronic system of record for all DCF-Division of Child Protection and Permanency (DCP&P) cases. This includes all phases of the division's involvement with a family and includes the child abuse or neglect reporting hotline (State Central Registry), investigations, ongoing case management and services, resource family management, and permanency. Additional business purposes include financial management for payments to service and resource home providers and to gather information to support Social Security Act Title IV-E reimbursements for adoption assistance for children adopted from foster care.

NJ SPIRIT processes approximately \$25 million per month for client services and child board and subsidy payments. The caseload managed by DCP&P staff for any given time throughout the year includes 25,000 active cases in the system, involving 50,000 children, 7,400 of which are active placements.

System Documentation

User access documentation needs improvement.

NJ SPIRIT has Detailed System Design (DSD) documentation provided by the vendor for the application and its functionality. However, it provides insufficient definitions and descriptions of each user group, their respective security profiles, and the resources and actions within a security profile.

A user's access to NJ SPIRIT and their capabilities within the application are based on their functional title and associated user group. A security matrix was developed by the DCF staff during the initial system development life cycle and was used to assign a user to a user group. It has been updated to include additional user groups since the application became fully implemented in 2007.

As part of their change control process, the DCF, in July 2014, began incorporating the windows and tabs a user can access into the DSDs when a change is implemented. This process still does not fully define a particular user group or sufficiently describe what a user can view or what actions may be performed within a window or tab.

Industry best standards dictate an entity should implement effective authorization controls. This requires the ability to readily determine a user's access to data.

Additionally, with a potential reduction in staff due to retirements or other attrition, it is important to adequately document this process to allow for the proper transfer of knowledge. CobiT PO7.5 Dependence Upon Individuals states that an entity should minimize the exposure to critical dependency on key individuals through knowledge capture (documentation), knowledge sharing, succession planning, and staff backup. This documentation was not provided by the vendor when the project was completed.

Without adequately documenting the user groups and what they can view or what actions they can perform, the risk increases that a user can access a window or tab and view personally identifiable information and use it for improper purposes.

Recommendation

We recommend the DCF continue their efforts to document the user groups and windows and tabs affected by a change request. We also recommend the DCF ensure the documentation of the user groups, windows, and tabs is readily available when needed.

»»««

User Access

Some users have been granted unnecessary access to case information.

Access to NJ SPIRIT is controlled by a user ID, user groups, and security profiles. These items comprise the Worker Record. User groups are the top level of security classification for access to NJ SPIRIT. Assignment to a user group is based on job function. A user can be assigned to more than one user group. Within each user group are security profiles. Security profiles are used to define the types of access allowed within a user group. However, NJ SPIRIT users have access privileges to all security profiles associated with a user group, whether necessary or not. Our review found some users have the ability to view specific information for which they have no business use.

During the system development life cycle, the DCF used the Wisconsin model for assigning users to a user group and did not adequately document this process. DCF analysts interviewed users to determine their job responsibilities and assigned them to user groups based on their duties. However, some of these user groups allow access beyond what a user would need.

Recommendation

We recommend that the applicable security profiles be reviewed to prevent users from access to data for which there is no business use.

We have provided the detail for this finding under separate cover to DCF management.

»»<<»

NJ SPIRIT User Accounts

User accounts were not removed timely from NJ SPIRIT or Active Directory.

We tested user access for the period of May 15, 2013 to March 7, 2014 to determine the effectiveness of the process for removing user access for both Active Directory and NJ SPIRIT. Active Directory is a directory service that authenticates and authorizes all the users and computers in a Windows domain network. We judgmentally sampled 141 out of 273 separated users and found 27 NJ SPIRIT users and 15 Active Directory users were not removed within 30 days as outlined in DCF policy. Additionally, eight separated employees still had active NJ SPIRIT accounts, and 31 still had network access through Active Directory.

We tested a subsequent period of user access to NJ SPIRIT from March 8, 2014 to February 25, 2015 to determine if the same conditions existed. Of 50 sampled items, we determined 11 NJ SPIRIT users were not removed timely. It should be noted our first sample disclosed it took an average of 25 days to remove a user, while our second sample disclosed the average dropped to 11 days. Industry best standards state that inactive accounts and accounts for separated

individuals are to be disabled and removed timely.

Prior to our audit period, the DCF conducted annual security reviews to determine if a user's job status had changed and modified it accordingly. During the audit, the security reviews increased to semi-annually, then monthly, which reduced the time to remove a user's access.

By not removing inactive accounts and accounts for separated users timely, individuals may obtain unauthorized or inappropriate access to the application or data.

Recommendation

We recommend the DCF continue their efforts in their security reviews and remove or modify a user's access accordingly.



Disaster Recovery Plan

The DCF should continue their efforts to maintain a disaster recovery plan and exercise guide that reflects the current IT environment.

Our review of the disaster recovery plan in place at the beginning of our audit period found it was out-of-date and did not reflect the current IT environment with regard to hardware, software, personnel, and alternate recovery site.

Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an entity's ability to accomplish its mission. Industry best standards state the prioritized listing of critical information resources and operations should be periodically reviewed to determine whether it reflects current conditions. Such reviews should occur whenever there is a significant change in the entity's mission and operations or in the location or design of the systems that support these operations.

As of the end of the audit period, the DCF had updated their disaster recovery plan and exercise guide to reflect the current IT environment as it related to hardware, software, network components, alternate recovery site, and personnel.

Recommendation

We recommend the DCF continue their efforts to maintain a current disaster recovery plan and exercise guide.





State of New Jersey

DEPARTMENT OF CHILDREN AND FAMILIES

P.O. Box 729

TRENTON, NJ 08625-0729

CHRIS CHRISTIE
Governor

KIM GUADAGNO
Lt. Governor

ALLISON BLAKE, PH.D., L.S.W.
Commissioner

November 10, 2015

John J. Termyna, Assistant State Auditor
Office of Legislative Services
Office of the State Auditor
125 South Warren Street
P.O. Box 067
Trenton, NJ 08625-0067

Dear Mr. Termyna:

This is in response to your letter of October 22, 2015 concerning the Office of Legislative Services, Office of the State Auditor (OSA) draft audit report entitled "Department of Children and Families, New Jersey Statewide Protective Investigation Reporting and Information Tool (NJ SPIRIT)." Your letter provides an opportunity to comment on the draft audit report.

The objective of the audit was to determine the adequacy of general and application controls for change management, system backup and recovery, contingency planning and disaster recovery, system security, and data integrity which included data origination, data input, data processing, and data output.

The draft audit report concluded that the Department of Children and Families (DCF) Information Technology management and staff take administering and securing the application very seriously and have adequate controls and processes in place to provide for change management, system backup and recovery, contingency planning and disaster recovery, system security, and data integrity. However, it was noted, that some of the controls and processes could be improved upon.

The specific auditor's recommendations and DCF Information Technology responses are provided below:

System Documentation:

Recommendation:

We recommend the DCF continue their efforts to document the user groups and windows and tabs affected by a change request. We also recommend the DCF ensure the documentation of the user groups, windows, and tabs is readily available when needed.

Response:

DCF continues to document the user group, windows and tabs affected by a change request to enhance the user access documentation. In addition, through special reporting DCF can define what each of the user groups are and the functionality within each of the windows and tabs. The special reporting documentation describes what a user can view and what actions may be performed within a window and or tab. This is available for review upon request.

User Access:

Recommendation:

We recommend that the applicable security profiles be reviewed to prevent users from access to data for which there is no business use.

Response:

DCF has taken action to prevent user access to those employees identified as not having a justified business use. Protocol is in place to periodically review users' profiles in order to ensure appropriate access.

NJ SPIRIT User Accounts:

Recommendation:

We recommend DCF continue their efforts in their security reviews and remove or modify a user's access accordingly.

Response:

DCF has already taken action and will continue our efforts in security reviews and remove and or modify a user's access accordingly.

Disaster Recovery Plan:

Recommendation:

We recommend DCF continue their efforts to maintain a current disaster recovery plan and exercise guide.


Response:

DCF has already taken action and will continue our efforts to maintain a current disaster recovery plan and exercise guide.

John J. Termyna
November 10, 2015
Page 3

DCF would also like to recognize the professionalism and dedication demonstrated by your staff throughout this review. Thank you for this opportunity to respond.

Sincerely,



Allison Blake, Ph.D., L.S.W.
Commissioner