CITY OF PHILADELPHIA
PENNSYLVANIA

OFFICE OF THE CONTROLLER

Promoting honest, efficient, and fully accountable government

City of Philadelphia
Review of the General Information Technology Controls Over the Department of Human Services' Family and Child Tracking Systems
Fiscal 2011

City Controller
ALAN BUTKOVITZ

CITY OF PHILADELPHIA

OFFICE OF THE CONTROLLER
1230 Municipal Services Building
1401 John F. Kennedy Boulevard
Philadelphia, PA 19102-1679
(215) 686-6680 FAX (215) 686-3832

ALAN BUTKOVITZ
City Controller

GERALD V. MICCIULLA
Deputy City Controller

September 19, 2013

Anne Marie Ambrose, Commissioner
Department of Human Services
One Parkway Building, 1515 Arch Street
Philadelphia, PA 19102

We reviewed and evaluated the effectiveness of the Department of Human Services' general information technology controls over its Family and Child Tracking Systems for fiscal 2011. A synopsis of the results of our work is provided in the executive summary to the report.

We discussed our findings and recommendations with your staff at an exit conference and included your responses to our comments as part of the report. Our recommendations have been numbered to facilitate tracking and follow-up in subsequent years. We believe that, if implemented by management, these recommendations will improve the Department of Human Services' information system controls.

We would like to express our thanks to the management and staff of the Department of Human Services for the courtesy and cooperation displayed toward us during the conduct of our work.

Very truly yours,

ALAN BUTKOVITZ
City Controller

cc: Honorable Michael A. Nutter, Mayor
Honorable Darrell L. Clarke, President,
and Honorable Members of City Council
Members of the Mayor's Cabinet
Adel W. Ebeid, Chief Innovation Officer

REVIEW OF THE FAMILY AND CHILD TRACKING SYSTEMS GENERAL INFORMATION TECHNOLOGY CONTROLS

EXECUTIVE SUMMARY

Why the Controller's Office Conducted the General Controls Review

The Department of Human Services utilizes two Family and Child Tracking Systems in the administration of the city's Children and Youth Program, a major federal and state grant program. These two information technology database systems are commonly referred to as Legacy FACTS and FACTS2. We reviewed the general information technology controls over the Family and Child Tracking Systems security management, logical and physical access, configuration management, segregation of duties, and contingency planning to determine if these controls were suitably designed and operating effectively.

What the Controller's Office Found

The Controller's Office noted a number of internal controls deficiencies that the Department of Human Services needs to address. Highlights of the deficiencies include:

- **Information Technology Governance** – Formal policies and procedures for the areas included within the scope of this review were not available or were not adequately documented. A lack of formalized policies and procedures could result in the inconsistent application of controls, the inability to secure city data and maintain a stabilized information technology environment, and an increased risk that overall strategies and objectives will not be met.

- **Access** – Consultants had access to data with the ability to change data without independent review. Further, we noted that consultants were permitted full access to software and case file histories, and were not subject to personal security clearances or background checks. In addition, access authorizations for former employees and generic user names had not been disabled or removed. The integrity of the data is at risk in the absence of adequate access controls.

- **Security** – The Department of Human Services had not appointed a security officer and did not have a security policy. By not specifically appointing a qualified employee with security expertise, and by not developing a comprehensive security policy, systematic threats for unauthorized software modifications may exist and not be addressed, resulting in lost, damaged or compromised data.

- **Contingency Plans** – Management had not developed a comprehensive contingency plan for restoring critical applications and data. Without formalized policies and procedures in place, management runs the risk of users not following a standard process, and most importantly, the inability to access critical data for at risk children and restore all system resources after a disabling event occurs.

What the Controller's Office Recommends

The Controller's Office has developed a number of recommendations to address these findings. The recommendations can be found in the body of this report.

CONTENTS

BACKGROUND

Functions and Systems Overview

The Department of Human Services (DHS) was established by the Philadelphia Home Rule Charter to provide and promote safety and permanency for children and youth at risk of abuse, neglect, and delinquency. In accomplishing its goals, DHS utilizes two Family and Child Tracking Systems, commonly referred to as Legacy FACTS and FACTS2, in the administration of the city's Children and Youth Program, a major federal and state grant funded program.

Legacy FACTS was developed in 1990 as a mainframe database system used to manage case assignments and placements, generate reports and billings to grantor agencies, and maintain service care provider payment information. FACTS2, placed into development in 2009, is a more effective and efficient web-based client-server case management database system that has the ability to interface with provider and prevention services applications. The goal of FACTS2 is to provide a single electronic case management system that would be accessible by both internal DHS users and external service providers and allow both to perform and complete all case related work while providing management and monitoring staff with appropriate tools to ensure compliance with state and federal regulations and report complete and accurate data.

Since 2009, DHS has operated Legacy FACTS and FACTS2 as two parallel database systems. The department is currently in the process of integrating FACTS2 functionality with Legacy FACTS. The integration of the two systems was expected to be completed in 2011, but system modifications and other factors have pushed back the completion date to 2015.

Management

A commissioner, appointed by the city's managing director with the approval of the mayor, directs the activities of DHS. The department's information technology unit consists of two divisions: the network division and the systems division. The network division is responsible for the department's local area networks, and the system division is responsible for database management, system design and development, system programming and maintenance, quality assurance, and user training.

The city's Office of Innovation and Technology (formerly the Division of Technology) was established by Executive Order 12-11 to be responsible for all city information technology projects, including project management, in consultation and cooperation with applicable city departments. To meet its executive order responsibilities, the Office of Innovation and Technology assigned an Information Technology Director, a Project Manager, and a Systems Manager to oversee and direct the work of the DHS' system division staff and consultants on the design, development, operation, and maintenance of Legacy FACTS and FACTS2.

Internal Control

City agency heads have the responsibility for establishing and maintaining effective information system controls. Information system controls include both general controls and application controls. General controls, which were the focus of our examination, consist of security management, logical and physical access, configuration management, segregation of duties, and contingency planning.

GENERAL INFORMATION TECHNOLOGY CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEMS (FACTS)
FISCAL 2011

No	Observation/ Condition	Risk/Potential Effect	Recommendation	Department Response
	Information Technology Governance			
1.	Management did not provide us with formal comprehensive policies and procedures governing many of its critical control activities for accessing data; segregating incompatible duties; assessing and monitoring risk to ensure the effective management of security threats; and planning for contingencies to mitigate the impact of unplanned interruptions. Absence of such formal policies and procedures may indicate controls do not exist, or if they do, they may not be understood or adequately applied.	When policies and procedures have not been formally developed and adequately documented, there is an increased risk that critical control procedures may be inconsistently applied. Formal policies and procedures help prevent errors by ensuring uniformity in routine applications.	Management should develop and document formal comprehensive policies and procedures for controls over access to programs and data, changes to software, security threats, and contingency planning for unplanned interruptions [302211.01]. Management should also design and implement appropriate monitoring controls to ensure that policies and procedures, once established, are complied with on a consistent basis [302211.02].	Procedures are being documented to outline the tasks/owners and necessary service levels for DHS IT Operations, Data Management and User Access/Control. Single points of responsibility are being identified and appropriate oversight will be applied. Draft completion date by 12/31/2013.

GENERAL INFORMATION TECHNOLOGY CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEMS (FACTS)
FISCAL 2011

No	Observation/ Condition	Risk/Potential Effect	Recommendation	Department Response
	Segregation of Duties			
2.	Job descriptions for positions exempt from civil service did not always include clear and specific duties, responsibilities, and prohibited activities. In addition, these job descriptions lacked the technical knowledge, skills, abilities, experience, and education required for the successful performance of the position. Such information is useful in segregating incompatible duties as well as in the hiring, promoting, and performance evaluation process.	Undefined or inadequately defined job descriptions increase the risk that employees may not understand their responsibilities and fail to identify those activities that are prohibited. In addition, where decision making is not clearly linked to authority, responsible individuals may not be held accountable.	Management should review the actual duties of staff on a periodic basis to ensure that duties are consistent with existing job descriptions. Position descriptions for exempt employees should clearly describe the employees duties and reporting responsibilities, as well as the knowledge, skills, experience, and education required for the position [302211.03].	City of Philadelphia IT Job descriptions have been created by the Office of Innovation and Technology. Existing descriptions are out of date and not applicable to the demands of today's IT organization. DHS IT is establishing an IT Organization structure including role, responsibility, goal, and metrics definition at each level of the organization. Draft definition completed and implemented by 12/31/2013.
3.	Management had not properly segregated duties and responsibilities. We were informed that system programmers, consultants, and system administration personnel had the ability to access, add, modify and delete data. Programmers should not be responsible for moving programs into production, or have access to production libraries or data.	When duties are not adequately segregated, there is an increased risk that data could be erroneously added, modified, or deleted and not be detected by management.	Management should properly segregate duties and responsibilities for its programmers, consultants, and system administration personnel. Specifically, the ability to add, change, or remove data should be delegated to individuals who are not responsible for programming activities. In all cases, direct access to databases should be restricted to the database administrator and production control personnel. Lastly, only system users should be responsible for transaction origination and for initiating corrections or changes to existing data files [302211.04].	Currently, DHS IT has the ability to change production level data due to the DHS policy of limiting user functionality to change/delete various functions within FACTS2 and ECMS. IT plans on adding the necessary application functionality to allow users, where applicable, to change/delete data. This would eliminate the need for IT to complete many of these data change tasks.

GENERAL INFORMATION TECHNOLOGY CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEMS (FACTS)
FISCAL 2011

No	Observation/ Condition	Risk/Potential Effect	Recommendation	Department Response
	Segregation of Duties			
4.	File matches to populate and synchronize data between Legacy FACTS and FACTS2 were performed by a programming consultant. However, we could not identify any independent verification procedures to ensure that the exchanges or transfers of data between the two database systems were complete and accurate.	Without independent verification and reconciliation there is the risk that data could be dropped, inadvertently changed or corrupted without detection.	Require that the synchronization of data between Legacy FACTS and FACTS2 be independently verified. Control totals matching data transmitted to data received should be routinely employed to ensure data integrity [302211.05].	The QA function within DHS IT will review the sync process and the quality of the data being synchronized in both FACTS and FACTS2. At this time, users of both applications and the output of our reporting processes have not identified any significant data quality issues. The sync process will not be necessary in the future with the retirement of the legacy FACTS system.

GENERAL INFORMATION TECHNOLOGY CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEMS (FACTS)
FISCAL 2011

No	Observation/ Condition	Risk/Potential Effect	Recommendation	Department Response
	Access Controls			
5.	Access controls require that management periodically review access authorizations for continuing appropriateness. Unnecessary user identification numbers and identification numbers for separated employees and consultants should be disabled and removed in a timely manner. Our review found no evidence that this control procedure was operating effectively. Management provided us with a system generated list of users that were authorized access to Legacy FACTS and FACTS2. We found that the list contained former employees (one employee separated from the city as far back as 1997) as well at least 19 generic user names. Generic users are often created during system implementations, but should be deleted, for security purposes, once the system is live. Access controls also require that significant system events, such as access to and modification of sensitive or critical system resources, be logged and software be used to maintain an audit trail of these events for review by management. Although both Legacy FACTS and FACTS2 contain an audit trail security feature, an independent program consultant informed our staff that he had the ability to turn off the audit trail software so that program /data modifications would not be logged or tracked.	Unauthorized access to data increases the risk that data could be compromised without management detection, and also presents opportunities for the possible abuse of confidential information. The use of generic user accounts results in a lack of accountability within the system. Allowing generic users to remain active is highly risky because some generic users are given administrative privileges which allow them to access, alter, and view programs and confidential data. Further, the ability to turn off the software's audit trail feature allows unauthorized changes to programs and data to be concealed and not subject to review by management.	We recommend management establish and implement a procedure to ensure mandatory and timely notification to security personnel of the hiring, transfer, or termination of both information technology staff and independent contractors. Security personnel should disable and remove accounts for separated employees and consultants in a timely manner [302211.06]. We also recommend that management remove access authorizations for all generic user accounts. Users should be assigned a unique account to provide a mechanism to log, monitor, and hold individuals accountable for activities performed [302211.07]. Finally, the ability of some individuals to turn off the system's logging and audit trail feature should be immediately rescinded [302211.08].	Application Access control procedures are being documented for each DHS application. The updated DHS IT organization structure will support the Access Control procedures. Draft procedures scheduled for completion 12/31/2013. After completion, the QA/Operations IT team will review all users and access privileges for accuracy.

GENERAL INFORMATION TECHNOLOGY CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEMS (FACTS)
FISCAL 2011

No	Observation/ Condition	Risk/Potential Effect	Recommendation	Department Response
	Security Controls			
6.	Security procedures should include the requirement for screening outside contractors participating in the design, development, operation or maintenance of sensitive applications, as well as those having access to sensitive data. We found that management did not perform security background checks for employees of its contractors even though these consultants were involved in the development, operation, and maintenance of both Legacy FACTS and FACTS2, and had the ability to add, delete, and modify confidential data as discussed in comment number three. Furthermore, we believe that management should not rely on background checks performed by contractors for its own employees because of the potential conflict of interest.	Providing contractors with open access to highly confidential records on troubled children and youth prepared by social workers, health care professionals and the courts, may result in unauthorized disclosures or misuse by irresponsible individuals.	We recommend management perform independent background checks for its outside consultants commensurate with the level of risk involved for the type of service performed. Background investigations should be addressed as part of the contracting process and should be completed prior to the start of the work [302211.09].	DHS IT will initiate any required background checks for all Consultants/Contractors through HR and Procurement/Vendor Management.
7.	Management had not appointed a Security Officer to institute security management policies and procedures. The Mayor's Executive Order No. 2-97 requires that the Mayor's Office of Information Services (now the Office of Innovation and Technology) will coordinate with management of city departments to ensure the designation of an Information Technology Security Officer for each city agency.	The lack of a dedicated security function may mask vulnerabilities to the misuse and abuse of data including unauthorized access, intrusion threats, viruses, emergency shutdowns, loss of data and data theft.	We recommend management formally establish a Security Officer position in accordance with the Mayor's Executive Order. We believe that the Security Officer position once established will improve controls and reduce the risk of security threats [302211.10].	Currently, DHS IT does not have the necessary skills/experience available to have a Security Officer. DHS will explore the possibility of obtaining a staff member with the requisite skills to serve in this position. In the meantime, DHS IT will leverage the expertise of the OIT Security Office to identify and address any IT Security risks.

GENERAL INFORMATION TECHNOLOGY CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEMS (FACTS)
FISCAL 2011

No	Observation/ Condition	Risk/Potential Effect	Recommendation	Department Response
	Configuration Management			
8.	Management's Systems Development Life Cycle (SDLC) plan to guide its ongoing development of a single unified database for all children and youth case file histories was not complete. A SDLC methodology consists of policies and procedures that govern software development and modifications as a software product goes through each phase of its life cycle (initiation, design/development, implementation, and operations/maintenance). Our review found that management's SDLC lacked many of the procedures that should be followed for each phase of a system's life cycle, as well as information system controls that should have been integrated into the SDLC to ensure protection of the database's information. We also noted that DHS did not utilize a checklist to ensure that procedures/tasks required for each of the SDLC phases were addressed. A checklist would identify the tasks to be performed, the individual(s) responsible for completing each task, when the task was started and completed, the tools and techniques used, and the results obtained.	Projects lacking a formal SDLC may result in wasted resources when system development efforts are not adequately planned and fail to consider all core requirements, and the implementation procedures lack direction or defined timelines.	We recommend that management develop a comprehensive SDLC plan and provide the necessary support and cooperation to ensure that the plan is effectively implemented [302211.11]. We also recommend that management consider utilizing a checklist to document that tasks required for each of the SDLC phases were addressed [302211.12].	DHS IT currently follows an SDLC and over time will more consistently follow the SDLC of OIT. DHS IT has a documented SharePoint PMO site that has each application development project and phase documented. Some of the SDLC check point gates are not documented due to the aggressive development and implementation cycles driving our projects. This is a practical reality given the demands on IT and the resources available to meet the needs of the Agency.

GENERAL INFORMATION TECHNOLOGY CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEMS (FACTS)
FISCAL 2011

No	Observation/ Condition	Risk/Potential Effect	Recommendation	Department Response
9.	**Configuration Management** We observed that computer equipment assigned to user groups within the Department of Human Services (DHS) was not optimally configured. Specifically, the equipment's operating systems and memory lacked the necessary capacity to permit efficient data entry and retrieval by user groups.	Ongoing programming changes to databases had resulted in less than optimal system configurations. Inefficiencies, such as excessive time lost by staff and management, occur when equipment operates slowly due to inadequate data processing capabilities.	We recommend coordinated planning by management to ensure that system configurations are routinely evaluated and continuously upgraded to ensure the effective use of the system and its capabilities [302211.13].	DHS IT has developed a 4 year plan to renew all end user desktops and/or laptops. By the end of 2013/early 2014, over 400 desktops/laptops will be upgraded to Windows 7and Microsoft Office 2010. Per the plan, the remaining base of users will be upgraded over the next 3 years including the upgrade of the user interfaces for our applications to a consistent web based experience for DHS users. This plan has been requested in the 2014/2015 Needs based Budget to the Commonwealth of Pa.

GENERAL INFORMATION TECHNOLOGY CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEMS (FACTS)
FISCAL 2011

No	Observation/ Condition	Risk/Potential Effect	Recommendation	Department Response
	Contingency Planning			
10.	We found that maintenance contracts were not adequately monitored. For example, a tape drive designated to backup data for case documentation was diagnosed as requiring servicing on April 13, 2011. Servicing was not available due to an expired maintenance agreement that had lapsed due to nonpayment. The problem was not resolved until a new maintenance agreement was executed on March 2, 2012, a delay of over a year.	The inability to service and maintain information systems may lead to the loss of critical information, and cause the city to incur potential liability to the detriment of the children and youth under DHS' care.	We recommend that all critical maintenance contracts and agreements be identified, monitored, and timely renewed. An effective program for maintenance will ensure that the impact of unexpected service interruptions that can occur from hardware equipment failures will be minimized [302211.14].	DHS IT completed a physical inventory for all Servers, Storage, Network and end user devices on June 30, 2013. We are currently reviewing existing maintenance and support contracts to ensure they are consistent with our inventory of IT assets and the needs of DHS. We expect to continue this review process Quarterly.
11.	Management had not developed a comprehensive contingency plan for restoring critical applications. An effective contingency plan should include arrangements for alternative processing facilities in case DHS facilities are significantly damaged or cannot be accessed, and provides for the periodic testing of the plan under conditions that simulate a disaster.	The lack of appropriate contingency planning makes DHS vulnerable to data loss, and in more extreme situations, may cause a temporary cessation of operations.	We recommend management develop and implement a comprehensive contingency plan that includes testing and recovery of critical systems, identifying alternative processing facilities, and providing detailed instructions of actions to be taken under varying types of contingencies [302211.15].	DHS IT is in the process of developing a BCP for the entire Agency. In addition, we are discussing our needs with the Office of Innovation and Technology to leverage any disaster recovery capabilities they may offer.

GENERAL INFORMATION CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEM (FACTS)

Family and Child Tracking System Overview

The Department of Human Services (DHS) contracted with outside consultants for the development of the initial Family and Child Tracking System (Legacy FACTS) in 1990. The design was a real time on-line text based system application linking a flat file database to DHS clients and users. The Legacy FACTS database resides on the Office of Innovation and Technology's IBM mainframe and is used for various financial applications including: reports and billing; payment data for the service care providers; and vendor, financial and placement information.

In 2009 DHS began a major upgrade development project to migrate its mainframe flat file data operations (Legacy FACTS) to a more effective and efficient Oracle client-server relational database system, known as FACTS2. Until DHS can fully integrated Legacy FACTS with FACTS2, the systems are operating as two parallel databases.

Both Legacy FACTS and FACTS2 are case management systems that are specifically designed to permit the social worker to manage caseload information from his/her desktop. Although the Legacy FACTS database resides on the mainframe, it is fully accessible via network servers by a single personal computer. FACTS2 database resides on servers and is equally accessible from desktop personal computers. The initial input is at the social worker level. Each social worker allowed to enter information is uniquely identified on the system by a user identification profile.

The FACTS2 system initiates a case when a potential threat to a child is reported and includes any applicable juvenile justice references. A report to DHS registering a complaint of child endangerment is directed to the Intake Unit of DHS for investigation and assigned a unique case number. If the Intake Unit recommends services, the case status changes to "open for service" and the case number is used as the reference number. If the Intake Unit does not recommend services, the case is closed and the case number is deleted from use and cannot be referenced further.

The FACTS2 system contains a template and a drop down menu that offers eight options: Work-On, Party Search, Case Management Form, Case Search, Work Product Search, Worker Search, Portal, and Photo Management. The user has more functionality within each area compared to Legacy FACTS whereby emails are sent to active worker and supervisors when notes are added to an active case, and photographs may be added to the case file. The main feature of FACTS2 was the development of the Electronic Case Management System (ECMS). The ECMS includes detailed case information (case status, status date, assignment date, to whom assigned, case parties, case activities, and party relationships) and has the ability to cross-reference cases by case number or case name (last name of the family).

The transition form Legacy FACTS to FACTS2 was to have been completed in 2011, but because of changing functionality (the addition of the ECMS and other upgrades) the completion date is now 2015 with a strong possibility that the targeted completion date may not be achievable.

GENERAL INFORMATION CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEM (FACTS)

Information Systems Management

An Information Technology Director and Deputy Director manage DHS' information technology unit. The unit consists of two divisions: the network division and the systems division.

The network division is headed by a network administrator. A local area network (LAN) administrator is responsible for each of the department's networks. Some LAN administrators are independent contractors and report directly to the Deputy IT Director. At the time of our review this division was responsible for the operation of 16 local area network blade servers and multiple remote printers located at various locations, as well as 2,308 personal computers (desktops and laptops) of different manufactures and configurations.

The systems division includes the areas of database management, system design and development, system programming and maintenance and quality assurance and user training. It is responsible for the design, development, operation, and maintenance of both Legacy FACTS and FACTS2.

General Information Technology Controls

Organization Environment Controls (Information Technology Governance)

Information technology governance consists of the leadership and organization structures and processes that ensure that the organization's information technology sustains and extends the organization's strategy and objectives.

System Access and Security Controls (Access to Programs and Data)

Segregation of Duties – These controls provide reasonable assurance that incompatible duties are effectively segregated. They include controls over personnel activities through formal operating procedures, supervision, and review. Key duties and responsibilities need to be divided or segregated among different people to reduce the risk of error or fraud.

Access Controls – These controls provide reasonable assurance that access to computer resources (data, equipment, and facilities) is reasonable and restricted to authorized individuals. Proper access controls includes effective protection of information system boundaries, identification and authentication mechanisms, authorization controls, protection of sensitive system resources, audit, and monitoring capability, including incident handling, and physical security controls.

Security Management – These controls provide reasonable assurance that security management is effective. Security management controls should include periodic assessments and validation of risk, security control policies and procedures, security awareness training and other security-related issues.

GENERAL INFORMATION CONTROLS REVIEW
FAMILY AND CHILD TRACKING SYSTEM (FACTS)

Application Development and System Software Controls (Change Management)

Configuration Management – These controls provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended. Effective configuration management includes documentation of policies, plans, and procedures. Controls should include proper authorization, testing, and approval, tracking of all configuration changes to protect against known vulnerabilities, and documentation and approval of emergency changes.

Disaster Planning and Contingency Controls (Computer Operations)

Contingency Planning – These controls provide reasonable assurance that contingency planning protects information resources and minimizes the risk of unplanned interruptions. It also provides for the recovery of critical operations should interruptions occur. Contingency planning requires an effective assessment of critical and sensitive computerized operations, identification of supporting resources, steps taken to prevent and minimize potential damage and interruption, comprehensive contingency plan, and periodic testing of the contingency plan.