DISTRICT OF COLUMBIA OFFICE OF THE INSPECTOR GENERAL

OIG Project No. 13-1-22MA

OIG

March 2017

CHILD AND FAMILY SERVICES AGENCY:

FACES INFORMATION SYSTEM DID NOT ENSURE CONTROL OBJECTIVES WERE CONSISTENTLY MET

Guiding Principles

*Workforce Engagement * Stakeholders Engagement * Process-oriented * Innovation*
** Accountability * Professionalism * Objectivity and Independence * Communication * Collaboration*
** Diversity * Measurement * Continuous Improvement*

Mission

Our mission is to independently audit, inspect, and investigate matters pertaining to the District of Columbia government in order to:

- prevent and detect corruption, mismanagement, waste, fraud, and abuse;

- promote economy, efficiency, effectiveness, and accountability;

- inform stakeholders about issues relating to District programs and operations; and

- recommend and track the implementation of corrective actions.

Vision

Our vision is to be a world class Office of the Inspector General that is customer-focused, and sets the standard for oversight excellence!

Core Values

Excellence * Integrity * Respect * Creativity * Ownership
* Transparency * Empowerment * Courage * Passion
* Leadership

WE ARE
WASHINGTON
DC

HIGHLIGHTS PAGE

OIG Project No. 13-1-22MA **March 2017**

CHILD AND FAMILY SERVICES AGENCY:

FACES Information System Did Not Ensure Control Objectives Were Consistently Met

OIG

Why OIG Did This Audit

The Office of the Inspector General (OIG) performed this audit to assess the adequacy and effectiveness of controls within the D.C. child welfare computerized management system known as FACES. The Child and Family Services Agency (CFSA) maintains child-welfare records in the FACES application and also uses it as its accounts payable subsidiary ledger for approving disbursements related to child welfare services. Annualized disbursements approved in FACES during the audit period (October 2011 to May 2013) totaled approximately $115.4 million.

The communication of and access to computer information among all pertinent parties involved with child welfare cases affects the children monitored, their families, and the social workers who provide them services and support. A lack of reliable and accurate information puts the safety and economic security of these children at risk and may expose CFSA to undetected fraudulent activities.

The audit objectives were to:
(1) determine whether the controls surrounding FACES provide for accuracy, authorization, maintenance, completeness, and storage of data; and
(2) evaluate the effectiveness of internal controls intended to safeguard against fraud, waste, and abuse.

What OIG Recommends

The OIG made 29 recommendations to CFSA that are necessary in addressing control deficiencies identified during our audit.

What the OIG Found

Although CFSA has implemented information system controls to ensure data confidentiality, integrity, and availability of its FACES information for managing the District's child welfare cases, our audit identified vulnerabilities with this computerized management system.

Specifically, we found that CFSA did not meet all business process control objectives to provide for data: 1) accuracy, 2) authorization, 3) maintenance, 4) completeness, and 5) storage.

We identified 27 specific deficiencies related to the five business process control objectives. We attributed the deficiencies generally to failure in the application's design and to a lack of management oversight to correct errors from data input and output. For instance, CFSA granted inappropriate access to multiple users to input data and did not have formal procedures to identify or prevent inaccurate data entry, such as duplicate payments.

Regarding a lack of management oversight, we noted that CFSA lacked an IT strategic plan, did not have procedures to implement security practices consistently, and failed to perform risk assessments.

As a result, CFSA may be at risk of having incomplete or inaccurate information about the children it serves and the payments it makes to providers for services, which may prevent the effective management of the District's child welfare program.

Furthermore, we determined that CFSA spent an additional $1.4 million to maintain FACES over the course of 3 years by using the services of a contractor rather than District employees, which resulted in wasteful spending related to inefficient resource management and inadequate planning. We attribute this to ineffective governance and improper evaluation of cost.

GOVERNMENT OF THE DISTRICT OF COLUMBIA
Office of the Inspector General

Inspector General

OIG

March 31, 2017

Brenda Donald
Acting Director
D.C. Child and Family Services Agency
200 I Street, S.E.
Washington, D.C. 20003

Dear Acting Director Donald:

Enclosed is the final audit report *Child and Family Services Agency: FACES Information System Did Not Ensure Control Objectives Were Consistently Met* (OIG Project No. 13-1-22MA). The audit was included in the OIG's *Fiscal Year 2013 Audit and Inspection Plan* dated August 31, 2012. As such, our audit objectives were to determine whether the controls surrounding FACES provide for accuracy, authorization, maintenance, completeness, and storage of data. We conducted this audit from April 2013 to December 2016 in accordance with generally accepted government auditing standards. Additionally, we assessed whether the internal controls were adequate to safeguard against fraud, waste, and abuse. We appreciate that the former Child and Family Services Agency (CFSA) Chief Information Officer was able to work with us between August 2014 and June 2016 to consolidate the original recommendations into the 29 contained in this report and to proactively address many of these recommendations.

CFSA concurred with 17 of our 29 recommendations and outlined actions that it believes meet the intent of our recommendations. CFSA's response and planned actions meet the intent of recommendations 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 20, 22, 23, 24, 25, 26, and 27; therefore, we consider these recommendations resolved and open pending completion of planned actions or evidence of stated actions.

For recommendations 1, 2, 15, 17, 18, 19, 21 and 28, CFSA did not concur, but proposed actions sufficient to meet the intent of the recommendations. We also consider these recommendations resolved and open pending evidence of stated actions. For recommendation 10, CFSA did not concur. However, given the action taken, we consider this recommendation resolved and closed.

For recommendations 9, 16, and 29, CFSA did not concur or provide a sufficient response for not addressing the recommendation; therefore, we consider these recommendations open and unresolved pending reconsideration from CFSA.

We request that CFSA reconsider its position on the following recommendations and respond to us within 30 days:

- CFSA indicated that allowing supervisors to initiate and approve their own transactions will remain part of the process. However, CFSA has not implemented any controls to mitigate the risk of fraudulent or erroneous transactions (Recommendation 9).
- CFSA stated its risk-based controls are OCTO's responsibility. However, CFSA did not provide a documented plan to support how the agency will mitigate its risks (Recommendation 16).
- CFSA indicated that the decision of the contracting officer is final, regardless of economy or viable alternatives. However, the contracting officer's determination that it was more economically feasible to outsource was not supported by the procurement documentation (Recommendation 29).

A complete list of the disposition of our 29 recommendations is included in Appendix D at the end of this report.

We appreciate the cooperation and courtesies extended to our staff during this audit. If you have any questions concerning this report, please contact me or , Assistant Inspector General for Audits, at (202) 727-2540.

Sincerely,

Daniel W. Lucas
Inspector General

DWL/rjb

Enclosure

cc: See Distribution List

DISTRIBUTION:

The Honorable Muriel Bowser, Mayor, District of Columbia, Attention: Betsy Cavendish (via email)
Mr. Rashad M. Young, City Administrator, District of Columbia (via email)
Mr. Barry Kreiswirth, General Counsel, City Administrator, District of Columbia (via email)
Ms. HyeSook Chung, Deputy Mayor for Health and Human Services, District of Columbia (via email)
The Honorable Phil Mendelson, Chairman, Council of the District of Columbia (via email)
The Honorable Brianne K. Nadeau, Chairperson, Committee on Human Services, Council of the District of Columbia (via email)
The Honorable Brandon T. Todd, Chairperson, Committee on Government Operations (via email)
Mr. John Falcicchio, Chief of Staff, Office of the Mayor (via email)
Mr. Kevin Harris, Director, Office of Communications, Executive Office of the Mayor (via email)
Mr. Matthew Brown, Director, Mayor’s Office of Budget and Finance (via email)
Ms. Nyasha Smith, Secretary to the Council (via email)
The Honorable Karl Racine, Attorney General for the District of Columbia (via email)
Mr. Jeffrey DeWitt, Chief Financial Officer, Office of the Chief Financial Officer (via email)
Mr. Timothy Barry, Executive Director, Office of Integrity and Oversight, Office of the Chief Financial Officer (via email)
The Honorable Kathy Patterson, D.C. Auditor, Office of the D.C. Auditor, Attention: Cathy Patten (via email)
Mr. Jed Ross, Director and Chief Risk Officer, Office of Risk Management (via email)
Mr. Gary Engel, Managing Director, FMA, GAO, (via email)

TABLE OF CONTENTS

Page

BACKGROUND

CFSA is the public child welfare agency in the District of Columbia. CFSA's mission is to improve the safety, permanence, and well-being of abused and neglected children in the District of Columbia, and to strengthen their families. CFSA's four primary functions are to: (1) take and investigate abuse and neglect reports; (2) assist families; (3) provide safe out-of-home care; and (4) reestablish permanent homes.[1] As of June 30, 2016, CFSA managed cases for 2,548 children: 1,020 placed in out-of-home care, and 1,528 provided in-home assistance.[2]

CFSA uses the FACES[3] application to manage child welfare cases and report activities to the District of Columbia Council, federal agencies, and the federal court monitor.[4] This application is a federally sponsored system designed to hold a state's official case records, which includes a case management history on all children and families served by the state's Title IV-B and Title IV-E entities.[5] In addition to tracking child welfare cases, FACES is the accounts payable subsidiary ledger for disbursements related to child welfare. Annual disbursements approved in FACES during the period from October 1, 2011, to May 31, 2013, totaled approximately $115.4 million. As of January 2014, there were approximately 1,100 CFSA and 300 private agency users of the FACES application.

The Child Information Systems Administration (hereinafter CFSA's IT Department) is the designated team within CFSA that supports information technology (IT) services for the entire organization, and maintains and modifies FACES. CFSA outsources many of the application development and support services to Deloitte Consulting LLC with additional infrastructure support performed under agreement with the Office of the Chief Technology Officer.

We conducted our audit work from April 2013 through December 2016 in accordance with generally accepted government auditing standards. The audit objectives were to: (1) determine whether the controls surrounding FACES provide for accuracy, authorization, maintenance, completeness, and storage of data; and (2) evaluate the effectiveness of internal controls intended to safeguard against fraud, waste, and abuse.

To determine whether the controls surrounding FACES provide for accuracy, authorization, maintenance, completeness, and storage of data, we interviewed responsible CFSA personnel to obtain a general understanding of the FACES processes used to: a) manage and monitor child welfare cases, and b) administer payments supporting the Agency's programs.

[1] We obtained the information in this paragraph from CFSA's website at http://cfsa.dc.gov/page/about-cfsa (last visited May 14, 2014).

[2] We obtained this information from the July 2016, Children and Youth CFSA Statistics, published on CFSA's website, *available at* http://cfsa.dc.gov/page/faqs-cfsa (last visited Oct. 31, 2016).

[3] In February 2006, FACES was replaced with FACES.NET, a web-based application that was in operation during the entire audit period and is referred to as "FACES" throughout this report.

[4] The *LaShawn A. v. Fenty* Amended Implementation Plan (2007) held the District accountable for performance benchmarks that covered the child welfare system and practice. FACES information was submitted monthly to a court-appointed monitor because of this case.

[5] We obtained this information from the U.S. Department of Health and Human Services, *available at* http://www.acf.hhs.gov/programs/cb/research-data-technology/state-tribal-info-systems (last visited Aug. 20, 2014).

We based our audit program on the Federal Information System Controls Audit Manual (FISCAM), which contains guidance for reviewing information system controls that are necessary to ensure data accuracy, authorization, maintenance, completeness, and storage.

To evaluate the effectiveness of safeguards against fraud, waste, and abuse, we assessed CFSA’s response to our internal control questionnaire, reviewed policies, and observed the performance of procedures. We analyzed the costs of retaining the services of IT contractors in comparison to using District employees and considered the potential for CFSA employees to commit fraud.

FINDINGS

FACES INFORMATION SYSTEM'S CONTROLS DID NOT PROVIDE REASONABLE ASSURANCE THAT DATA ACCURACY, AUTHORIZATION, MAINTENANCE, COMPLETENESS, AND STORAGE OBJECTIVES WERE CONSISTENTLY MET

CFSA's FACES information system controls did not provide reasonable assurance that data accuracy, authorization, maintenance, completeness, and storage control objectives were consistently met during data input, processing, and output. We identified 27 deficiencies that could compromise the confidentiality, integrity, and availability of child welfare data within the FACES information system. Specifically, the controls did not consistently ensure that: 1) information in FACES was accurate; 2) transactions were authorized appropriately; 3) maintenance practices addressed risks to data availability; 4) information processed was complete; and 5) stored data was protected against risks of unauthorized access.

Information Was Not Always Accurate

We identified instances where information in FACES was not correctly processed, entered into the application in the proper format, or corrected timely. Specifically, we observed inaccurate contract remaining balances and invoice dates entered without formatting controls. Additionally, there were no established timeframes to correct inaccurate data. These conditions did not conform to the control objective for accuracy that requires proper recording of data.

Table 2 provides further details of the deficiencies we found with the accuracy control objective.

Table 2. Deficiencies Affecting the Accuracy Control Objective

Condition	Criteria	Cause	Effect
(1) Inaccurate Contract Balances in FACES The record that tracks the remaining balance available under a contract was not accurate in the FACES application. Balances are currently tracked manually outside of FACES.	Organizations should control the processing of information based on enterprise risk, to ensure that information processing is accurate.[6]	Deloitte's application manager stated that the contract limit counter that tracks and tallies expenditures may have been disabled for an unknown business reason.	Maintaining and independently updating information in separate systems can result in a loss of data integrity and may result in payment errors.

[6] COBIT 5, DSS06.02, *Control the processing of information.*

Condition	Criteria	Cause	Effect
(2) No Data Entry Controls for Service Dates There were no input edits to ensure invoice service dates were entered in a valid date format or that the service date occurred in the past. We observed invalid date formats and inappropriate future dated transactions in the accounts payable subsidiary ledger of FACES. Implementing input edits will prevent some data entry errors we observed but it will not guarantee the data entered are accurate.	*See* Criteria for Condition 1.	In the opinion of a CFSA IT official, the edit was not specified in the design document.	Service date errors increase the likelihood that duplicate payment transactions will occur and reviews designed to identify duplicate payments may be less effective due to erroneous dates.

Condition	Criteria	Cause	Effect
(3) No Established Timeframes to Correct Inaccurate Data CFSA did not establish guidelines to correct errors identified on FACES' exception reports. We could find no documentation or directives on how such errors were to be monitored, recorded, and resolved. During the period tested, it took approximately 32 days, on average, to correct duplicate child records and more than 4 months to correct payment address errors once FACES identified and reported errors.	Organizations should manage business process exceptions and errors and facilitate their correction.[7]	Operations management has not developed review standards for exception reports.	Inaccurate information may affect case management and transaction processing. For example, the longer a duplicate child record remains uncorrected, the greater the possibility that case workers will not have access to a child's complete record, conflicting information will be collected, and additional employee hours will be required to merge and verify records.

Source: OIG Analysis

Inappropriate User Access Compromised the Appropriate Authorization of Transactions

CFSA did not implement certain business process controls to ensure proper approval of all transactions in accordance with management's authorization. We identified that CFSA did not implement formal procedures to: 1) accurately and consistently designate access rights and limitations according to business needs; and 2) apply appropriate segregation of duties (SOD) controls when approving transactions. These conditions did not conform to the control objective for authorization.[8]

CFSA Lacked Formal Procedures to Ensure User Permissions Matched Business Needs

CFSA's IT Department did not formally document information security procedures or obtain operations management approval of the position security map.[9] Additionally, we found that

[7] COBIT 5, DSS06.04, *Manage errors and exceptions*.

[8] FISCAM defines this as the "validity" business process control objective.

[9] The "position security map" indicates what functions within FACES each person is permitted access based on that person's role and business needs.

CFSA did not provide privileged[10] users individual user IDs, monitor privileged user accounts, or conduct periodic reviews to determine whether user permissions were properly set or remained appropriate over time.

Table 3 below provides further details of the deficiencies we found with the authorization control objective resulting from a lack of formal procedures.

Table 3. Procedural Deficiencies Affecting the Authorization Control Objective

Condition	Criteria	Cause	Effect
(4) No Formally Documented Information Security Procedures The security administration function did not formally document information security procedures. The procedures available are included with the general Employee Security Policy[11] and provide basic security objectives rather than detailed FACES procedures that would assist security users and their backup personnel in the consistent setup of users and application of policies.	Organizations should develop and disseminate procedures to facilitate the implementation of the access control policy and associated access controls.[12]	We attribute this condition to a lack of management oversight to ensure procedures affect the consistent execution of policies.	Security administration responsibilities may be improperly and inconsistently implemented allowing inappropriate user access to data and payment transactions.

[10] A "privileged" user is an individual with access to system control, monitoring, or administration functions (i.e., a system administrator in this instance).

[11] D.C. CHILD AND FAMILY SERVICES AGENCY, EMPLOYEE SECURITY POLICY, § VII (Rev. June 2, 2011).

[12] U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, app. F at F-7, AC-1 (NIST SPECIAL PUB. 800-53, Rev. 4), *available at* http://dx.doi.org/10.6028/NIST.SP.800-53r4 (last visited Nov. 4, 2016).

Condition	Criteria	Cause	Effect
(5) *Unix and Oracle Administrators Did Not Have Individual User IDs* Shared generic/privileged accounts were used to perform system administration functions without adequate monitoring controls over such activities.	Each user account will be assigned to one individual and will have a unique password.[13]	CFSA's IT Department did not: (1) create comprehensive procedures for privileged user accounts; and (2) perform periodic user access reviews.	CFSA will not be able to safeguard individual accountability in its systems administration functions. In addition, CFSA will not be able to timely identify and address questionable, fraudulent, or erroneous activities by employees using shared user IDs.

[13] D.C. CHILD AND FAMILY SERVICES AGENCY, USER PASSWORD POLICY, § VII(A)(1)(a)(i) (Rev. Apr. 26, 2011).

Condition	Criteria	Cause	Effect
(6) No Business Approval of Position Security Map (Security Profiles by Position) There was no evidence that CFSA business operations personnel reviewed and approved the position security map or reviewed the defined permissions for SOD conflicts. A review of all permissions indicated that 735 of the 1,379 users (53 percent) examined had more access than defined on the Position Security Map. Additionally, two inactive security codes (used to assign permissions) were assigned in 145 profiles and at least one position allowed incompatible functions.	Organizations should limit access rights to business requirements and adhere to the principle of least privilege.[14]	Review of the security map was not conducted annually or whenever systemic changes affecting user permissions occurred. Risk assessments are not performed when additional permissions (security codes) are requested by operational managers.	Failure to evaluate and obtain business approval of the position security map may lead to insufficient protection of sensitive information and allow incompatible functional capabilities by users within the application. Additionally, inactive security codes could be activated at a future time and consequently give certain users inappropriate permissions.
(7) No Monitoring of Privileged User Accounts We observed that CFSA's IT Department did not implement a mechanism for monitoring the activities of staff with high-level system access privileges.	Audit trails maintain a record of system activity. In conjunction with appropriate tools and procedures, audit trails can establish individual accountability.[15]	CFSA issued a policy titled, *Audit Trail Monitoring and Reporting,* but did not dedicate resources to implement this policy.	Failure to record, monitor, protect, and review suspicious activity reports regarding those with high-level system access privileges may result in undetected security violations and a loss of individual accountability.

[14] U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, app. F at F-18, AC-6 (NIST SPECIAL PUB. 800-53, Rev. 4), *available at* http://dx.doi.org/10.6028/NIST.SP.800-53r4 (last visited Nov. 4, 2016).

[15] U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, GENERALLY ACCEPTED PRINCIPLES AND PRACTICES FOR SECURING INFORMATION TECHNOLOGY SYSTEMS, § 3.13 (NIST SPECIAL

Condition	Criteria	Cause	Effect
(8) No Periodic User Access Reviews Performed CFSA did not perform periodic user access reviews to determine whether user permissions were properly set-up or remained appropriate over time. For example, CFSA's fiscal operations department incorrectly believed that four individuals could provide accounts payable approval for demand payments, but there were actually 18 individuals with this capability.	Periodically, it is necessary to review user account management on a system. Such reviews may examine the levels of access each individual has in conformity with the concept of least privilege.[16] District financial system reviews will be conducted twice-a-year.[17]	CFSA's IT management did not recognize the need for this periodic review process and stated that while such reviews are not performed on a schedule, the IT manager in charge of security will review access when there are organizational changes.	Failure to perform periodic reviews of user permissions may lead to insufficient protection of sensitive data, unauthorized user access as responsibilities change, and inappropriate approvals of financial transactions.

Source: OIG Analysis

CFSA Did Not Segregate Incompatible Functions or Prevent Supervisors from Approving Transactions They Initiated

We observed instances where CFSA did not segregate duties, which is necessary to ensure that the people entering data into FACES are not the same people who also verify and approve the data or transactions. Specifically, "[w]ork responsibilities should be segregated so that one individual does not control all critical stages of a process."[18] SOD is the practice of dividing incompatible functions in critical processes among different individuals to prevent one individual from having the ability to authorize, perform, and monitor a particular IT activity or FACES function. SOD includes the effective control of personnel activities through formal operating procedures, access rights, supervision, and review.

PUB. 800-14, Sept. 1996), *available at* http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf (last visited Nov. 8, 2016).

[16] U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, AN INTRODUCTION TO COMPUTER SECURITY: THE NIST HANDBOOK, § 10.2.2 (NIST SPECIAL PUB. 800-12, 1995), *available at* http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (last visited Nov. 8, 2016).

[17] D.C. OFFICE OF THE CHIEF FINANCIAL OFFICER, OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS, POLICIES AND PROCEDURES MANUAL, Vol. V, § 25309001.30(4)(D) (updated Sept. 30, 2014).

[18] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM) 301, GAO-09-232G (Feb. 2009).

Table 4 provides further details regarding the weaknesses we identified in the authorization of transactions related to SOD.

Table 4. SOD Deficiencies Affecting the Authorization Control Objective

Condition	Criteria	Cause	Effect
(9) Supervisors Initiated and Approved Their Own Transactions We noted that supervisors have the ability to perform the same tasks in FACES as their subordinates. Individuals with supervisory permissions may initiate and approve their own transactions, or edit and approve a transaction initiated by a subordinate, thereby circumventing proper review and approval. From our analysis of 10 different transaction approval types, we determined that 59 supervisory users initiated a transaction and subsequently approved the same transaction at least once during the audit period.	Transactions should be created by authorized individuals following established procedures, including adequate SOD regarding the origination and approval of these transactions.[19]	CFSA's IT management did not design or configure security profiles to prevent supervisors from performing a subordinate's task or require alternate workflows for transactions initiated by supervisors.	Allowing a supervisor to approve his/her own work or edit and approve a subordinate's work could result in fraudulent or erroneous transactions being entered without timely detection.

[19] COBIT 5, DSS06.02, *Control the processing of information*, Activity 1.

Condition	Criteria	Cause	Effect
(10) Inconsistent Functionality for Supervisors to Return Deficient Transactions for Correction We observed that some transactions requiring supervisory review, and found to be deficient (i.e., required correction before approval), did not follow current practice because they could not be electronically returned in FACES to the initiator for correction. Specifically, we observed this lack of functionality occurred on related approval screens of the Safety Assessment, Information and Referral, and Referral Acceptance approval processes.	"Validate input data and … send back for correction as close to the point of origination as possible."[20]	Although we were unable to determine why this condition existed, the Chief Information Officer (CIO) speculated that this feature was most likely not specified in the design document for certain enhancements.	Without the functionality to easily return and track certain transactions for correction, supervisors have created an inefficient manual process to effect data correction. Additionally, there is a risk that supervisors may make the required changes without the initiator's knowledge because supervisors currently have the capability of editing and approving transactions.

[20] COBIT 5, DSS06.02, *Control the processing of information*, Activity 3.

Condition	Criteria	Cause	Effect
(11) Users Were Granted Incompatible Functions Certain users' permissions were inappropriately configured in FACES. At the time of our review, there were 14 users with the ability to create fictitious vendors and approve payments to those vendors; 18 users with the ability to initiate and approve payments; 89 users could extend recurring payments and change payment addresses; and 26 employees in CFSA IT department had update access in the production environment.	Mission functions should be separated from IT support functions.[21]	CFSA does not have a well- designed IT security policy that requires periodic review of user roles (Condition #8) for appropriateness over time.	Users with unnecessary permissions, conflicting capabilities, and continuous IT access to the production environment could introduce unintentional errors or facilitate fraudulent actions (e.g., misdirect payments).

[21] U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, app. F at F-18, AC-5(c) (NIST SPECIAL PUB. 800-53, Rev. 4), *available at* http://dx.doi.org/10.6028/NIST.SP.800-53r4 (last visited Nov. 4, 2016).

Condition	Criteria	Cause	Effect
(12) Non-Security Personnel had Security Administrator Privileges There were IT personnel, in non-security positions, with security administrator access within the FACES application. Specifically, we noted eight users who should not have had security administrator privileges allowing them to assign or modify all security categories including financial-related permissions of business users.	Organizations should limit access rights to business requirements and adhere to the principle of least privilege.[22]	IT management indicated that the purpose of additional access by non-security personnel is to test application functionality and confirm issues in the environment in which a reported error occurred.	There are increased risks of unauthorized user access and fraudulent transactions. Additionally, these weaknesses may require CFSA to incur additional expenditures to monitor users with incompatible functions or inappropriate access.
(13) Anonymous User IDs in Production Environment We found two unassigned user IDs that the help desk used to test connectivity in the production environment. These accounts could be used to read and update FACES data without authorization.	CFSA's password policy states that a person accessing electronic mission critical, sensitive, or confidential information is authorized with a unique user ID and password.[23]	IT management said they were unaware permissions allowed read and update access to certain FACES data but agreed that such access privileges are unnecessary to test connectivity.	Unassigned or anonymous accounts circumvent individual accountability by allowing anonymous read and update access to FACES data, which could lead to compromised data integrity.

[22] *Id.* at AC-6.

[23] D.C. CHILD AND FAMILY SERVICES AGENCY, USER PASSWORD POLICY, § IV (Rev. Apr. 26, 2011).

Condition	Criteria	Cause	Effect
(14) Developer Had Access to Production Environment We found an interface software developer who had update access to the production environment and was responsible for operating and monitoring interfaces. Specifically, the developer had update access to interface programs and job schedulers.	Establish roles and responsibilities of IT personnel that clearly reflect overall business needs, IT objectives, as well as relevant personnel's authority, responsibilities and accountability.[24]	CFSA's IT Department did not train another employee with the necessary skills to separate these incompatible functions.	Unapproved and untested interface programming code could be saved to the production software environment or unauthorized payment transactions could be interfaced to the accounting system, which could compromise the integrity of interfaced data.

Source: OIG Analysis

Availability of Data Maintained is at Risk

While CFSA's IT Department has employed many good practices to ensure trouble-free operation of the FACES application and data (e.g., analyzing operational problems, performing maintenance activities, and implementing enhancements), it has not formally documented or consistently performed certain practices to identify risks that could impact the availability of data maintained.

We found CFSA's IT Department had not performed a current risk assessment to identify and mitigate threats to the confidentiality, integrity, and availability of data; had no formal IT controls; and did not have policies on how to implement the Maintenance Stage of the Software Development Life Cycle (SDLC). Furthermore, CFSA's IT Department did not create, maintain, or retain necessary system documentation to support the application; postponed the installation of patches;[25] and did not train or develop a backup for the interface developer.

These conditions did not conform to the control objective for maintenance,[26] which requires data and other relevant business information to be readily available to users when needed.

Table 5 on the following page provides further details of deficiencies we found in the control objective for the maintenance of FACES.

[24] COBIT 5, APO01.02, *Establish roles and responsibilities*.

[25] "Patches" are additional pieces of code that address specific problems or flaws in existing software. Software vendors develop and release patches when vulnerabilities are discovered.

[26] FISCAM defines this as the "availability" business process control objective.

Table 5. Deficiencies Affecting the Maintenance Control Objective

Condition	Criteria	Cause	Effect
(15) No Current Risk Assessments Performed CFSA's IT Department did not perform periodic risk assessments to identify and mitigate threats to the confidentiality, integrity, and availability of data. CFSA's IT management indicated that a risk assessment has not been prepared since CFSA moved to its current location in 2012.	CFSA shall identify, assess, and minimize risk and vulnerabilities that affect the IT systems environment containing protected health information.[27]	CFSA's IT Department did not implement the agency's risk assessment policy.	Without periodic IT risk assessments, CFSA may not be positioned to mitigate existing risks or make timely responses to emerging future risks affecting the confidentiality, integrity, and availability of FACES data.
(16) No Formal IT Controls Implemented CFSA's IT Department did not issue or monitor a risk-based set of written IT controls for the management and operation of CFSA's IT resources.	District agency heads are responsible for establishing controls for the creation of District government records and for ensuring that such records are adequate, proper, and preserved.[28] Review the operation of controls to ensure that controls within business processes operate effectively.[29]	Reliance on certain policies to address regulatory requirements (i.e., Health Insurance Portability and Accountability Act) without performing periodic IT risk assessments contributed to CFSA's lack of formal IT controls.	CFSA may not be well-positioned to effectively mitigate existing risks or make timely responses to emerging risks.

[27] D.C. CHILD AND FAMILY SERVICES AGENCY, INFORMATION TECHNOLOGY RISK ASSESSMENT POLICY, § IV (Rev. Aug. 30, 2011).

[28] 1 DCMR § 1502.1.

[29] COBIT 5, MEA02.02, *Review business process controls effectiveness.*

Condition	Criteria	Cause	Effect
(17) The Maintenance Stage was excluded in the SDLC CFSA's SDLC documentation did not contain policies or controls for the maintenance stage of the life cycle.	"Maintain and perform operational procedures and operational tasks reliably and consistently."[30]	CFSA's IT Department did not adopt an effective project management model to define its role in CFSA's systems maintenance strategy while employing a third-party vendor.	This condition may affect the consistency and reliability of informal practices used to maintain and document the system.
(18) Inadequate System Documentation CFSA's IT Department did not create, maintain, or retain necessary system documentation to support the application in the event that the third-party contractor is unable or unwilling to maintain and update the software. Documentation available for review was not current, cataloged, or organized for ease of use.	When changes are implemented, update accordingly the solution, user documentation, and the procedures affected by the change.[31]	*See* Cause for Condition 17. Additionally, CFSA did not update or obtain from the vendor, system documentation necessary to maintain the application and no custodian was assigned.	CFSA may need to depend on the same outside expert consultant for maintenance of the FACES application. In addition, this condition exposes the CFSA's IT Department to risk of losing market flexibility, which is the ability to switch to in-house maintenance or obtain a competitively priced maintenance contactor in the open market.

[30] COBIT 5, DSS01.01, *Perform operational procedures.*

[31] COBIT 5, BAI06.04, *Close and document the changes.*

Condition	Criteria	Cause	Effect
(19) Deployment of Patches was Postponed CFSA postponed installation of Microsoft-supplied patches to Windows application servers during fiscal year 2013. There was no evidence indicating that CFSA's IT Department reviewed the potential security vulnerabilities addressed by Microsoft patches to determine the potential risks being avoided and what alternative solutions should have been implemented.	Implement and maintain preventive, detective, and corrective measures across the enterprise to protect information systems and technology from malware.[32]	Management postponed the testing and installation of patches due to a planned migration to a new version of the operating system software.	CFSA may have been at risk of malware, which could have disrupted computer operations and facilitated unauthorized access to sensitive information.
(20) No Trained Backup for the Developer We were unable to identify trained backup personnel for the interface developer.	Minimize the reliance on a single individual performing a critical job function through documentation, knowledge sharing, succession planning and staff backup.[33]	CFSA's IT Department did not train another employee with the necessary skills to perform these functions.	Relying on a single individual to perform critical functions places the agency operations at risk when that person becomes unavailable.

Source: OIG Analysis

[32] COBIT 5, DSS05.01, *Protect against malware*. Malware is an abbreviation of the phrase "malicious software."

[33] COBIT 5, APO07.02, *Identify key IT personnel*.

Information Processed Was Not Always Complete

During our review, we found that CFSA lacked controls to: (a) provide independent verification by accounting personnel that the data interfaced to the System of Accounting and Reporting (general ledger) were complete and accurate; (b) identify duplicate payments in FACES; and (c) require FACES users to select service types used to classify and book transactions to the general ledger. These conditions did not conform to the control objective for completeness, which requires that all transactions are input into the system and processed only once.

Table 6 provides further details of deficiencies we found with the completeness control objective.

Table 6. Deficiencies Affecting the Completeness Control Objective

Condition	Criteria	Cause	Effect
(21) AP Subsidiary Ledger was not Reconciled to the General Ledger The CFSA Fiscal Operations Department did not perform periodic reconciliation of FACES accounts payable subsidiary ledger transactions to the general ledger to ensure that all FACES transactions posted correctly in the general ledger and FACES properly initiated payments in the general ledger.	A periodic reconciliation process is the primary control procedure organizations use to check that the general ledger information is complete and accurate.[34]	The CFSA Fiscal Operations Department considered FACES application controls and two manual controls as sufficient to ensure the two systems stayed in agreement.	CFSA may not be able to timely detect and address incomplete data, financial misstatements, or fraudulent transactions.

[34] As set forth in Office of the Chief Financial Officer District-wide policy, "the broad objective of internal controls is to provide management with reasonable assurance that its policies and procedures are being implemented[.]" One specific control objective delineated within the policy is reconciliation, which is used to compare records with other independently kept records. D.C. OFFICE OF THE CHIEF FINANCIAL OFFICER, OFFICE OF FINANCIAL OPERATIONS AND SYSTEMS, POLICIES AND PROCEDURES MANUAL, Vol. I, § 10203000.00 (updated Nov. 21, 2014).

Condition	Criteria	Cause	Effect
(22) No Formal Process to Identify or Prevent Duplicate Payments There was no automated duplicate payment verification process in FACES. There was no provision to enter a vendor's invoice number (other than a freeform notes field). We identified 79 duplicate payments, which totaled approximately $232,000 during the audit period. The Fiscal Operations Department identified two of the largest duplicates prior to the audit and offset them against future payments.	"Manage business process exceptions and errors and facilitate their correction. Include escalation of business process errors and exceptions and the execution of defined corrective actions."[35]	The CIO speculated that the functionality was likely determined to be unnecessary during the application's design.	There is a risk of paying invoices multiple times without timely detection and recovery.

[35] COBIT 5, DSS06.04, *Manage errors and exceptions*.

Condition	Criteria	Cause	Effect
(23) Service Name Was Not a Required Field The service name was not a required field in FACES. Service names are necessary in properly classifying expenses to funding sources. We observed that 8 percent of expenditures (approximately $15.3 million) approved in FACES were not assigned a service name in the audit period.	*See* Criteria for Condition 22.	CFSA's Fiscal Officer stated that payment charges that do not exactly fit a predefined service category should not prevent payment.	Without completing the service name for each payment, there is a risk of improperly classifying payments in the general ledger and making payments from the wrong funding source. This could cause inaccurate management reporting and negatively impact future budgetary requirements.

Source: OIG Analysis

Stored Data Were Not Protected Against Unauthorized Access Risks

We noted improperly implemented or inadequate logical access controls that may permit unauthorized individuals and terminated employees the ability to secretly read and copy stored data and make undetected changes or deletions for either malicious purposes or personal gain. Additionally, not actively managing external data exchanges may allow authorized users inappropriate access to third-party data in violation of CFSA's memoranda of understanding with other District agencies. These conditions did not conform to the control objective for storage,[36] which requires that data and output be protected from unauthorized access.

Table 7 provides further details of the deficiencies we found with the storage control objective.

[36] FISCAM defines this as the "confidentiality" business process control objective.

Table 7. Deficiencies Affecting the Storage Control Objective

Condition	Criteria	Cause	Effect
(24) Password Policy Not Appropriately Configured Our examination of CFSA's Windows security configuration revealed that the system was not appropriately configured to agree with the agency password policy. Specifically, the Windows password length was set to seven characters and there was no limit to the number of invalid or incorrect password attempts that could be made to log into the system.	Per CFSA policy, "[u]sers will select passwords that contain a combined minimum of eight (8) alphanumeric and special characters[. . .]"[37] and user IDs will be "frozen" when five (5) invalid or incorrect password entry attempts have been made."[38]	We attribute these conditions to failure to implement or monitor policy requirements.	Failure to configure the system with the appropriate security settings makes the agency vulnerable to unauthorized access.

[37] D.C. CHILD AND FAMILY SERVICES AGENCY, USER PASSWORD POLICY, § VII(A)(1)(d)(i) (Rev. Apr. 26, 2011).

[38] *Id.* § A(1)(l)(i).

Condition	Criteria	Cause	Effect
(25) Some Terminated and Inactive User Accounts Were Not Disabled in a Timely Manner CFSA did not disable all tested accounts of terminated users according to policy. In addition, we observed that CFSA did not consistently disable inactive user accounts. We sampled 27 users to determine whether their access privileges were disabled in a timely manner. We found that 12 tested terminations (44 percent) were not disabled according to policy. The median time to terminate access was 10 business days. We also found two inactive accounts that were not disabled.	Password policy requires accounts to be disabled within 1 business day of termination[39] and unused accounts are to be canceled or suspended after 90 days of inactivity.[40]	CFSA management stated that the delay in disabling these user accounts was primarily due to late notifications by DCHR and external agencies. Additionally, the system did not automatically deactivate accounts after 90 days of inactivity.	This condition increases the risk of unauthorized access and provides terminated employees an opportunity to impair agency operations or to secretly read and copy sensitive data and make undetected changes or deletions for either malicious purposes or personal gain.[41]

[39] D.C. CHILD AND FAMILY SERVICES AGENCY, EMPLOYEE SECURITY POLICY, § VII(B)(1)(a) (Rev. June 2, 2011).

[40] D.C. CHILD AND FAMILY SERVICES AGENCY, USER PASSWORD POLICY, § VII(A)(1)(h)(i) (Rev. Apr. 26, 2011).

[41] While certain user accounts were not disabled in a timely manner, we did not observe that terminated individuals inappropriately accessed the system during the audit period.

Condition	Criteria	Cause	Effect
(26) Concurrent log-in Sessions Were Not Limited The number of concurrent FACES sessions that users could open was not limited to one.	Management should determine whether concurrent sessions should be permitted by defined account and/or account type.[42]	IT management indicated that they did not consider the concurrent session control when the agency moved to the FACES web version in 2006.	Users can logon at multiple computers but can only actively monitor one location. A workstation that is not actively controlled or locked could be accessed by someone who has not been authenticated.
(27) External Relationships Were Not Properly Managed We were unable to obtain current or signed memoranda of understanding and service level agreements for interagency relationships in 7 of 8 tested cases.	Organizations need to confirm compliance with legal, regulatory and contractual requirements.[43]	CFSA did not assign responsibility for interagency relations to a specific office or official.	CFSA might inconsistently manage its external relationships or may violate agreed-upon obligations, which could affect the confidentiality and use of third-party data.

Source: OIG Analysis

LACK OF EFFECTIVE GOVERNANCE AND THE USE OF A CONSULTANT MAY HAVE RESULTED IN WASTE

Our audit procedures did not identify any occurrences of fraud or abuse, but ineffective governance and an absence of a formal IT strategic plan may have resulted in waste. Additionally, CFSA's procurement of consulting services may have resulted in waste because CFSA paid approximately $1.4 million more than it would have spent using District employees.

CFSA's Governance May Have Resulted in Waste

Ineffective governance may have resulted in waste because CFSA has not adopted an IT governance and management framework to aid in institutionalizing generally accepted IT standards and has not formally developed an IT strategic plan to manage CFSA's IT resources.

[42] U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS, app. F at F-23, AC-10 (NIST SPECIAL PUB. 800-53, REV. 4), *available at* http://dx.doi.org/10.6028/NIST.SP.800-53r4 (last visited Nov. 4, 2016).
[43] COBIT 5, MEA03.03, *Confirm external compliance*.

According to the COBIT Framework, "governance ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritization and decision making; and monitoring performance and compliance against agreed-on direction and objectives."[44] Thus, organizations should create a strategic plan to define, in cooperation with relevant stakeholders, how IT-related goals will contribute to the enterprise's strategic goals.[45]

Nonetheless, the CIO stated he did not recognize the need to develop a formal strategic IT plan. Absent an IT strategic plan, the agency might only respond to immediate operational needs as they arise. Additionally, CFSA may be susceptible to unnecessary or wasteful spending because its IT investment decisions may not be cohesive, risk-based, proactive, or in line with the strategic direction of the agency.

CFSA's Procurement Improperly Evaluated Costs of Using a Consultant

CFSA's Chief Contracting Officer (CCO) did not adequately compare costs or properly support the selection of a third-party consultant in the agency's 2010 procurement to maintain the FACES application. CFSA's IT Department has been using Deloitte to perform maintenance and development services for the FACES application since 1999. Prior to June 5, 2015, when obtaining expert and consulting services, District regulations required the contracting officer to determine in writing why the use of these third-party services, rather than District employees, was in the best interest of the District.[46]

To determine whether CFSA complied with District regulations, we obtained and reviewed the *Determination and Findings* (D&F) *for a Consultant Service* that the CCO prepared to substantiate this procurement. According to the D&F, the CCO determined that it was more economically feasible to obtain system maintenance and development services through a contractor, but our review of the available procurement documentation for the 2010 procurement (summarized in Table 8) does not support that conclusion. Specifically, our review indicated that in the first year of the contract, in contract year (CY) 2011, the District would incur similar costs due to certain training and transition expenses. However, in years 2 and 3 (CY 2012 and CY 2013), contractor costs were substantially more than using District employees.

[44] COBIT Framework, Chapter 6, Separating Governance From Management, Principle 5, page 31.
[45] COBIT 5, APO02.05, *Define the strategic plan and road map*.
[46] 27 DCMR § 1901.5 (as amended by Final Rulemaking Mar. 29, 1996).

Table 8. Cost Comparison of Using D.C. Employees vs. Consultant

Provider and Type	Year 1 (CY 2011[a])	Year 2 (CY 2012[a])	Year 3 (CY 2013[a])	3-Year Cost[b]	Excess Cost
District Employees Cost[c,e]	$1,550,000[d]	$1,184,500	$1,220,035	$3,954,535 A	
Estimated Vendor Reasonable Cost[e]	$1,600,000	$1,648,000	$1,697,440	$4,945,440 B	
	Estimated Excess Cost of Using Consultant: (= B – A)				$990,905
Actual Vendor Contract Cost	$1,750,000	$1,785,000	$1,820,000	$5,355,000 C	
	Actual Excess Cost of Using Consultant (= C – A)				$1,400,465

[a] Contract years run August 1 through July 31 of the year shown.
[b] Base contract cost. Sum of costs in CY 2011, CY 2012, and CY 2013.
[c] Calculated by the CCO. Estimates in Years 2 and 3 include a 3 percent annual increase.
[d] Amount shown is the District Employee Cost of $1,150,000 and a one-time transfer of knowledge cost of $400,000. The $1,150,000 cost amount was used to calculate the Year 2 (CY 2012) estimate.
[e] Estimates in Years 2 and 3 include a 3 percent annual cost-of-living increase.

Source: OIG Analysis of CFSA's D&F for Consulting Services dated September 17, 2009.

The CCO could not locate an analysis on whether it was more economically feasible for the District to use Deloitte in option years 4 and 5 of the contract. The last year of the contract reviewed ended on July 31, 2015.

The CCO stated that there may have been additional quantitative or qualitative information, no longer available or excluded from the D&F, which could have further substantiated the decision. According to the CCO:

- IT staff can generally demand higher salaries than may have been considered in the analysis.
- At the time of the procurement, CFSA was required to reduce its workforce, and obtaining additional full-time employees may have been difficult.
- It may have been difficult to obtain certain management employees with the requisite knowledge and skills to replace contractors without disruption.

Nonetheless, we attribute the improperly substantiated procurement of consulting services to poor planning and management of the contracting and procurement processes and not developing a formalized strategic plan. As a result, we estimated that CFSA's IT Department paid approximately $1.4 million more over the first 3 years of the contract by using a third-party contractor rather than District employees to provide maintenance for the application.

CONCLUSION

CFSA's FACES system plays a critical role in providing for the well-being of abused and neglected children in the District of Columbia. Although the agency has implemented a number of information system controls to ensure data confidentiality, integrity, and availability of its

FACES information for managing the District's child welfare cases, there are still some vulnerabilities with the system and over controls related to governance and contracting for consultants. Until the agency's IT Department takes steps to formalize a number of control processes; better protect the computerized information from inadvertent or deliberate destruction, misuse, unauthorized modification, and inappropriate disclosure; and use a formal IT strategic plan to align IT needs with expenditures, CFSA's data integrity and security is at risk. The agency also risks unnecessary and wasteful spending related to inefficient resource management and inadequate planning.

RECOMMENDATIONS

We recommend that the Acting Director, CFSA:

1. Determine why the contract limit counter was disabled and is no longer properly tracking/tallying expenditures, and ensure that its functionality in FACES is fully restored, if more cost effective than the current manual tracking.

2. Implement input edits on the service date fields to include a valid date format for service periods to ensure that the service start date precedes the service end date and the service dates precede the current date.

3. Implement and monitor policies, procedures, and standards for correcting exception reports generated by FACES. Establish standard timeframes, based on risk, for clearing individual exception reports.

4. Formally develop additional control procedures for security management activities and monitor compliance with current policies and procedures.

5. Restrict the use of generic operating system and database IDs. Otherwise, monitor activities performed using generic ID as necessary.

6. Review the Position Security Map annually, or any time there are systemic changes affecting user permissions, to ensure access remains appropriate and there are no SOD conflicts. Evaluate new user permission requests for conflicts related to SOD. When conflicts will result from the request, obtain approval one level higher than is ordinarily required, and assign responsibility for monitoring controls to timely detect and address inappropriate activities.

7. Establish, implement, and monitor formal operating system and database security procedures that include a periodic review of privileged user account access and activity. Such policies and procedures should: (a) require reviews of user accounts and activities by a knowledgeable person who does not have privileged user access; and (b) clearly define what constitutes suspicious activity and how to review activities for compliance.

8. Implement and monitor policies and procedures to require that operational managers periodically review user access rights to ensure permissions remain appropriate over time. CFSA's fiscal officer should review financially related access at least biannually.

9. Implement an application control that prevents supervisors from approving their own work or editing and approving subordinates' work. Alternatively, if more cost effective, implement a monitoring control for approvals to detect and investigate managers approving their own work.

10. Identify all transactions requiring approval that cannot be sent back to the initiator for correction. Absent a business need to restrict this ability, implement an application control that allows transactions requiring approval to be sent back to the initiator for correction (i.e., usual functionality).

11. Perform a comprehensive review and analysis of the Position Security Map and current permissions to ensure: (a) access is appropriately assigned based on job responsibilities, need-to-know, and need-to-have principles; (b) identification and correction (or monitoring) of any conflicts related to SOD; and (c) IT personnel do not have continuous/unmonitored access to operational capabilities in the production environment.

12. Limit the number of security administrators and trained backup personnel in FACES to those users with a current business need.

13. Evaluate the business need for the continued maintenance of anonymous FACES user accounts. When required, perform periodic reviews of permissions to ensure the accounts cannot anonymously access, create, update, or delete data.

14. Develop and implement controls that establish SOD between program development and computer operator roles or independently monitor the activities of these users and follow up on any suspicious activity.

15. Revise the CFSA Risk Management Office's duties to include oversight of all CFSA IT resources and ensure that risk assessments are conducted according to policy.

16. Formally develop a comprehensive set of IT controls to mitigate risks to the creation and maintenance of records identified through a risk assessment process. Continuously assess and improve established controls to ensure they remain relevant and effective. Periodically monitor the operation of controls by reviewing test evidence to ensure the controls within business processes are operating effectively.

17. Implement SDLC standards using a framework for governing and managing information systems.

18. Develop or obtain from the third-party vendor adequate system documentation to support application maintenance. Update associated documentation when changes are performed. Designate a librarian and backup(s) as custodians of system documentation and provide them proper training on protecting and maintaining system documentation. Implement standards, policies and procedures for naming, indexing, updating editions, and retaining system documentation.

19. Implement patches within a predefined period of their release and maintain evidence indicating which tested patches were approved or denied for the production environment

and when approved patches were applied. Implement alternative security controls when vendor security patches are incompatible with the systems they are to protect.

20. Train backup personnel for all critical job functions to ensure a process does not rely on a single individual.

21. Perform a monthly reconciliation of the FACES accounts payable subsidiary ledger to the general ledger.

22. If cost effective, implement an application control to identify potential duplicate payments prior to approval or utilize manual control procedures to identify and handle duplicates. Consider adding a vendor invoice field to aid in identifying duplicate payments in addition to vendor name, number, service date, and invoice amount. Review duplicate payments the OIG identified for potential collection or offset against future payments.

23. Require service names be entered for all accounts payable transactions; and ensure the list of predetermined service names in FACES accurately includes all activities necessary to correctly book transactions to the correct funding source.

24. Implement or automate documented password policies governing logon attempts, inactive accounts, and password length across all production applications and underlying infrastructure systems.

25. Implement and monitor a procedure to disable access of District employees and contractors' access to FACES within 1 business day after separation and after 90 days of inactivity.

26. Limit the number of concurrent FACES sessions for each user to one, unless there is a business need for additional sessions, or document in agency security policy the accounts that require concurrent access, their business needs, and number of sessions permitted.

27. Designate an official or office to be responsible for IT-related external relationships to ensure they are current and address all exchanges of electronic information between District agencies and third parties. Ensure compliance with contractual obligations is assessed periodically.

28. Adopt an industry-recognized IT governance and management framework to accommodate the development and maintenance of an IT strategic plan, and integrate and institutionalize good business practices that ensure IT resources are appropriately used to support CFSA's business objectives. Develop and maintain an IT strategic plan aligned with CFSA's strategic objectives and budgetary resources.

29. Issue policies and procedures to ensure that future decisions to contract for consulting services are properly substantiated and conform with 27 DCMR § 1901 and other applicable District laws, regulations, and requirements.

AGENCY RESPONSE AND OFFICE OF INSPECTOR GENERAL COMMENTS

CFSA concurred with 17 of our 29 recommendations and outlined actions it believes meet the intent of our recommendations. CFSA's response and planned actions are sufficient to meet the intent of recommendations 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 20, 22, 23, 24, 25, 26, and 27; therefore, we consider these recommendations resolved and open pending completion of planned actions and evidence of stated actions.

For recommendations 1, 2, 15, 17, 18, 19, 21 and 28, CFSA did not concur, but proposed actions sufficient to meet the intent of the recommendations. We also consider these recommendations resolved and open pending evidence of stated actions. For recommendation 10, CFSA did not concur. However, given the action taken, we consider this recommendation resolved and closed. A complete list of the documentation required to close these 25 recommendations is included in Appendix D at the end of this report.

For recommendations 9, 16, and 29, CFSA did not concur or provide a sufficient response for not addressing the recommendation; therefore, we consider these recommendations open and unresolved pending reconsideration from CFSA. For recommendation 9, CFSA indicated that allowing supervisors to initiate and approve their own transactions will remain part of the process. However, CFSA has not implemented any controls to mitigate the risk of fraudulent or erroneous transactions. For recommendation 16, CFSA stated risk-based controls are OCTO's responsibility. However, CFSA did not provide a documented plan to support how the agency will mitigate its risks. Finally, for recommendation 29, CFSA indicated that the decision of the contracting officer is final, regardless of economy or viable alternatives. However, the contracting officer's determination that it was more economically feasible to outsource was not supported by the procurement documentation. We request that CFSA reconsider its position on recommendations 9, 16, and 29 and provide corrective actions within 30 days of the date of this final report.

ACTIONS REQUIRED

We request that within 30 days of receipt of this report, CFSA reconsider and respond to recommendations 9, 16, and 29, and provide the OIG with documentation for the additional recommendations cited in Appendix D.

APPENDIX A. OBJECTIVES, SCOPE, AND METHODOLOGY

We conducted our audit work from April 2013 through December 2016 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.

The audit objectives were to: (1) determine whether the controls surrounding FACES provide for accuracy, authorization, maintenance, completeness, and storage of data; and (2) evaluate the effectiveness of internal controls intended to safeguard against fraud, waste, and abuse.

To determine whether the controls surrounding FACES provide for accuracy, authorization, maintenance, completeness, and storage of data, we interviewed responsible CFSA personnel to obtain a general understanding of the FACES processes used to: a) manage and monitor child welfare cases, and b) administer payments supporting the Agency's programs.

We based our audit program on the *Federal Information System Controls Audit Manual* (FISCAM), which contains guidance for reviewing information system controls that are necessary to ensure data accuracy, authorization, maintenance, completeness, and storage. These five control objectives are used in achieving control over business processes as described in Table 1. We also relied on *Control Objectives for Information and Related Technology* (COBIT) to evaluate whether CFSA followed IT management and governance best practices.

Table 1. Business Process Control Objectives

Control Objective	Definition
Accuracy	Accuracy of data controls "should provide reasonable assurance that transactions are properly recorded, with the correct amount, and on a timely basis (in the proper period); . . . data elements are processed accurately by applications that produce reliable results; and output is accurate."
Authorization (FISCAM – Validity)	A transaction is valid when authorized. Validity controls "should provide reasonable assurance . . . that all recorded transactions actually occurred, . . . relate to the organization, and were properly approved in accordance with management's authorization . . . ."
Maintenance (FISCAM – Availability)	Maintenance of data ensures availability to authorized users. Availability controls "should provide reasonable assurance that application data and reports and other relevant business information are readily available to users when needed."
Completeness	Completeness of data controls "should provide reasonable assurance that all transactions that occurred are input into the system, accepted for processing, processed once and only once by the system, and properly included in output."
Storage (FISCAM – Confidentiality)	Storage of data controls provide for the confidentiality of sensitive and critical data. Confidentiality controls "should provide reasonable assurance that application data and reports and other output are protected against unauthorized access. Examples of confidentiality controls include restricted physical and logical access to sensitive business process applications, data files, transactions, and output, and adequate segregation of duties [SOD]."

Source: OIG, adapted from FISCAM.[47]

[47] U.S. GOVERNMENT ACCOUNTABILITY OFFICE, FEDERAL INFORMATION SYSTEM CONTROLS AUDIT MANUAL (FISCAM) 341-42, GAO-09-232G (Feb. 2009).

APPENDIX A. OBJECTIVES, SCOPE, AND METHODOLOGY

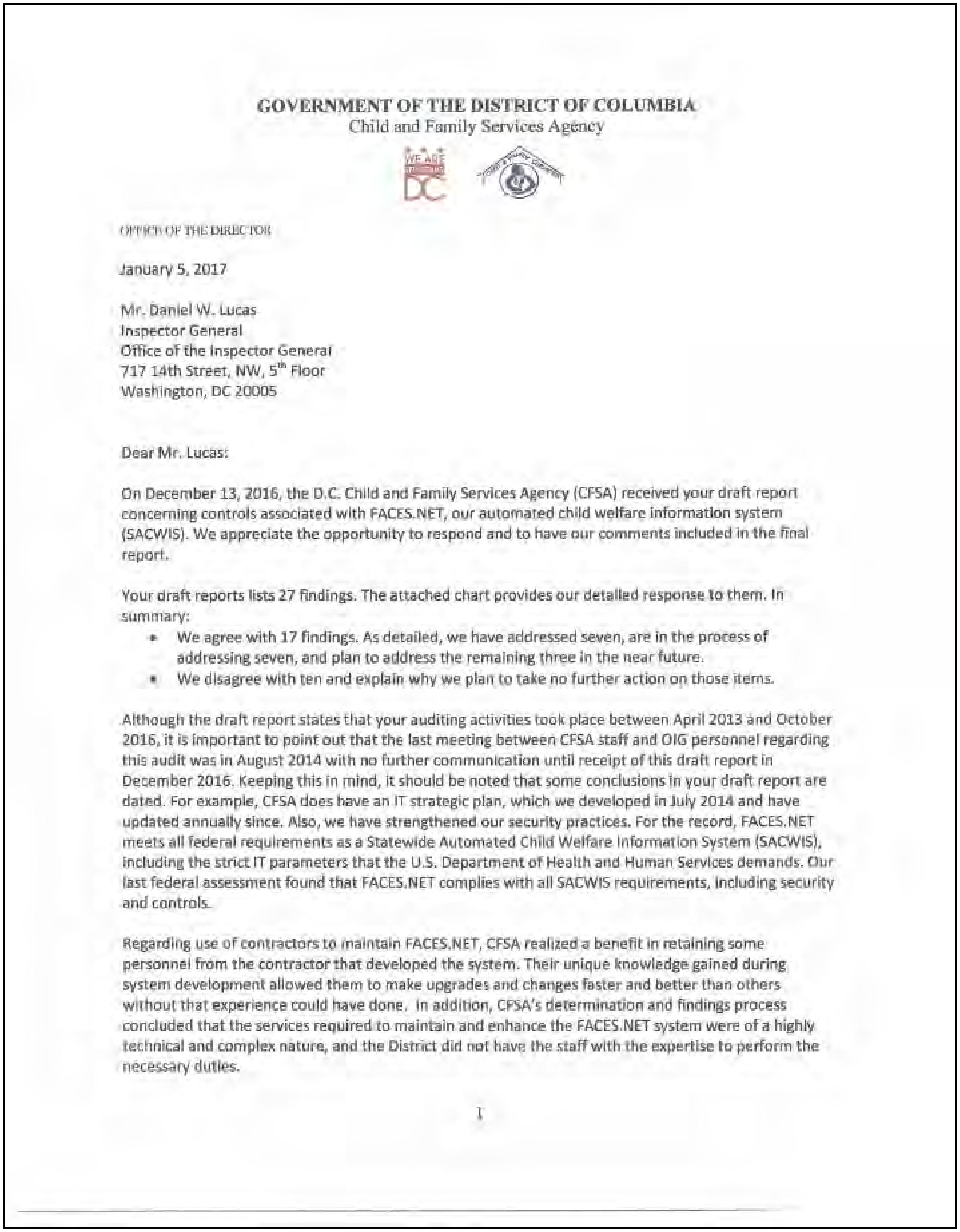
We obtained and reviewed copies of policies and procedures governing the administration of child welfare cases and IT management in order to assess management's directives to define operational standards, establish goals, and assign responsibilities. We reviewed laws and regulations governing the administration of child welfare cases and procurement activities in order to determine whether CFSA complied with statutory and regulatory requirements. We met with Office of the Chief Financial Officer's managers and employees to obtain and review financial information and records related to child welfare payments from FACES. We tested the operating effectiveness of application controls for user permissions, assignment and management of cases, approval of work, updating master data, and payments. We selected and tested controls applied to various categories of IT service activities, including backup and disaster recovery, change management, control environment, logical security, and computer operations.

To evaluate the effectiveness of safeguards against fraud, waste, and abuse, we assessed CFSA's response to our internal control questionnaire, reviewed policies, and observed the performance of procedures. We analyzed the costs of retaining the services of IT contractors in comparison to using District employees and considered the potential for CFSA employees to commit fraud. Our fraud, waste and abuse audit procedures were limited to an evaluation of the design or inconsistent performance within the set of internal controls tested or observed during the audit. We performed our procedures on a test basis and, as such, our tests were not designed to identify all occurrences of fraud, waste and abuse. Therefore, instances of fraud, waste, and abuse may exist that have not been identified.

APPENDIX B. ACRONYMS AND ABBREVIATIONS

CCO	Chief Contracting Officer
CFSA	Child and Family Services Agency, District of Columbia
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
CY	Contract Year
D&F	Determination and Findings
DCMR	District of Columbia Municipal Regulations
FISCAM	Federal Information System Controls Audit Manual
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
SDLC	Software Development Life Cycle
SOD	Segregation of Duties
SP	Special Publication

APPENDIX C. AGENCY'S RESPONSE TO THE DRAFT REPORT



GOVERNMENT OF THE DISTRICT OF COLUMBIA
Child and Family Services Agency

OFFICE OF THE DIRECTOR

January 5, 2017

Mr. Daniel W. Lucas
Inspector General
Office of the Inspector General
717 14th Street, NW, 5th Floor
Washington, DC 20005

Dear Mr. Lucas:

On December 13, 2016, the D.C. Child and Family Services Agency (CFSA) received your draft report concerning controls associated with FACES.NET, our automated child welfare information system (SACWIS). We appreciate the opportunity to respond and to have our comments included in the final report.

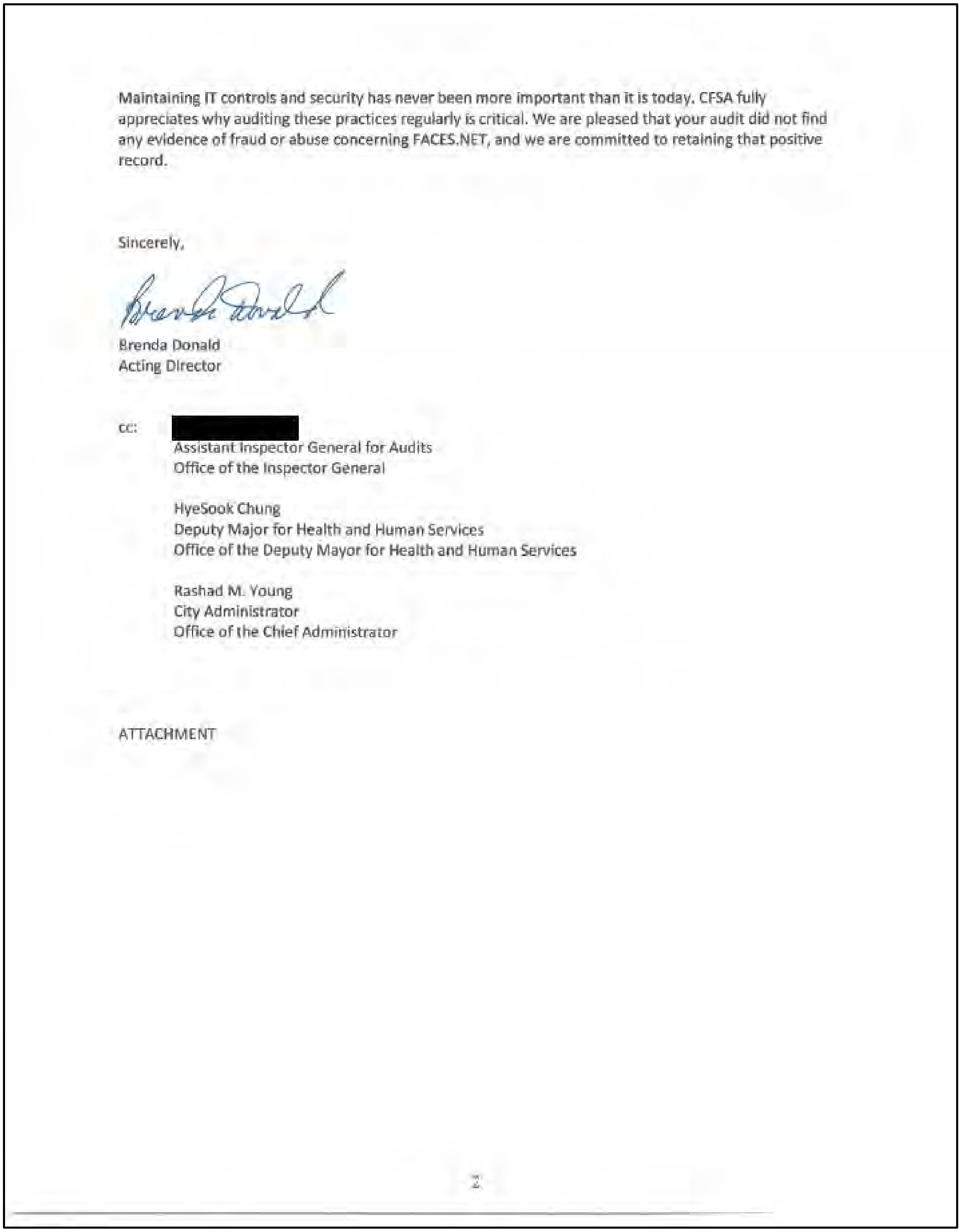
Your draft reports lists 27 findings. The attached chart provides our detailed response to them. In summary:

- We agree with 17 findings. As detailed, we have addressed seven, are in the process of addressing seven, and plan to address the remaining three in the near future.
- We disagree with ten and explain why we plan to take no further action on those items.

Although the draft report states that your auditing activities took place between April 2013 and October 2016, it is important to point out that the last meeting between CFSA staff and OIG personnel regarding this audit was in August 2014 with no further communication until receipt of this draft report in December 2016. Keeping this in mind, it should be noted that some conclusions in your draft report are dated. For example, CFSA does have an IT strategic plan, which we developed in July 2014 and have updated annually since. Also, we have strengthened our security practices. For the record, FACES.NET meets all federal requirements as a Statewide Automated Child Welfare Information System (SACWIS), including the strict IT parameters that the U.S. Department of Health and Human Services demands. Our last federal assessment found that FACES.NET complies with all SACWIS requirements, including security and controls.

Regarding use of contractors to maintain FACES.NET, CFSA realized a benefit in retaining some personnel from the contractor that developed the system. Their unique knowledge gained during system development allowed them to make upgrades and changes faster and better than others without that experience could have done. In addition, CFSA's determination and findings process concluded that the services required to maintain and enhance the FACES.NET system were of a highly technical and complex nature, and the District did not have the staff with the expertise to perform the necessary duties.

APPENDIX C. AGENCY'S RESPONSE TO THE DRAFT REPORT



Maintaining IT controls and security has never been more important than it is today. CFSA fully appreciates why auditing these practices regularly is critical. We are pleased that your audit did not find any evidence of fraud or abuse concerning FACES.NET, and we are committed to retaining that positive record.

Sincerely,

Brenda Donald
Acting Director

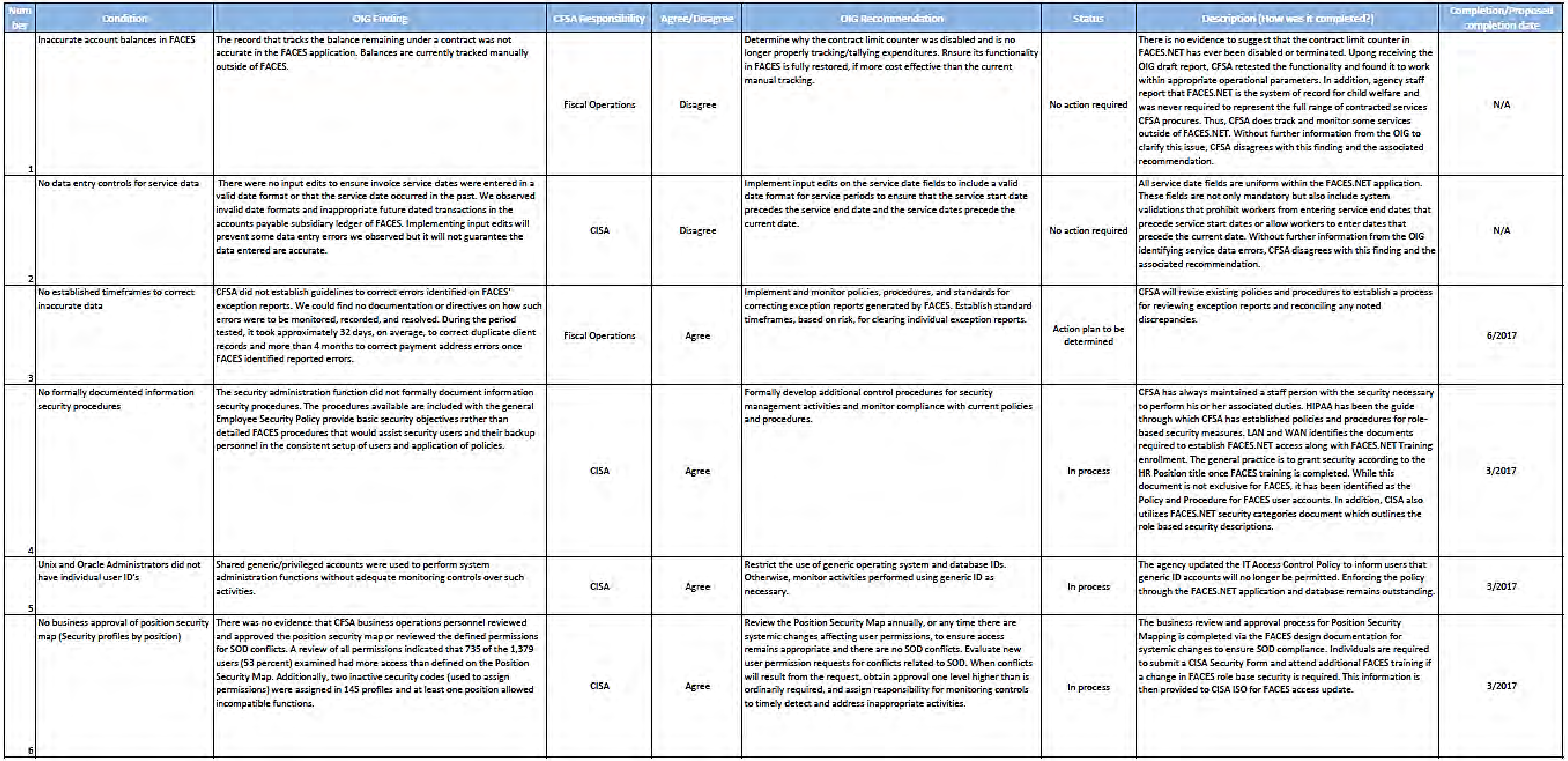
cc: [redacted]
Assistant Inspector General for Audits
Office of the Inspector General

HyeSook Chung
Deputy Major for Health and Human Services
Office of the Deputy Mayor for Health and Human Services

Rashad M. Young
City Administrator
Office of the Chief Administrator

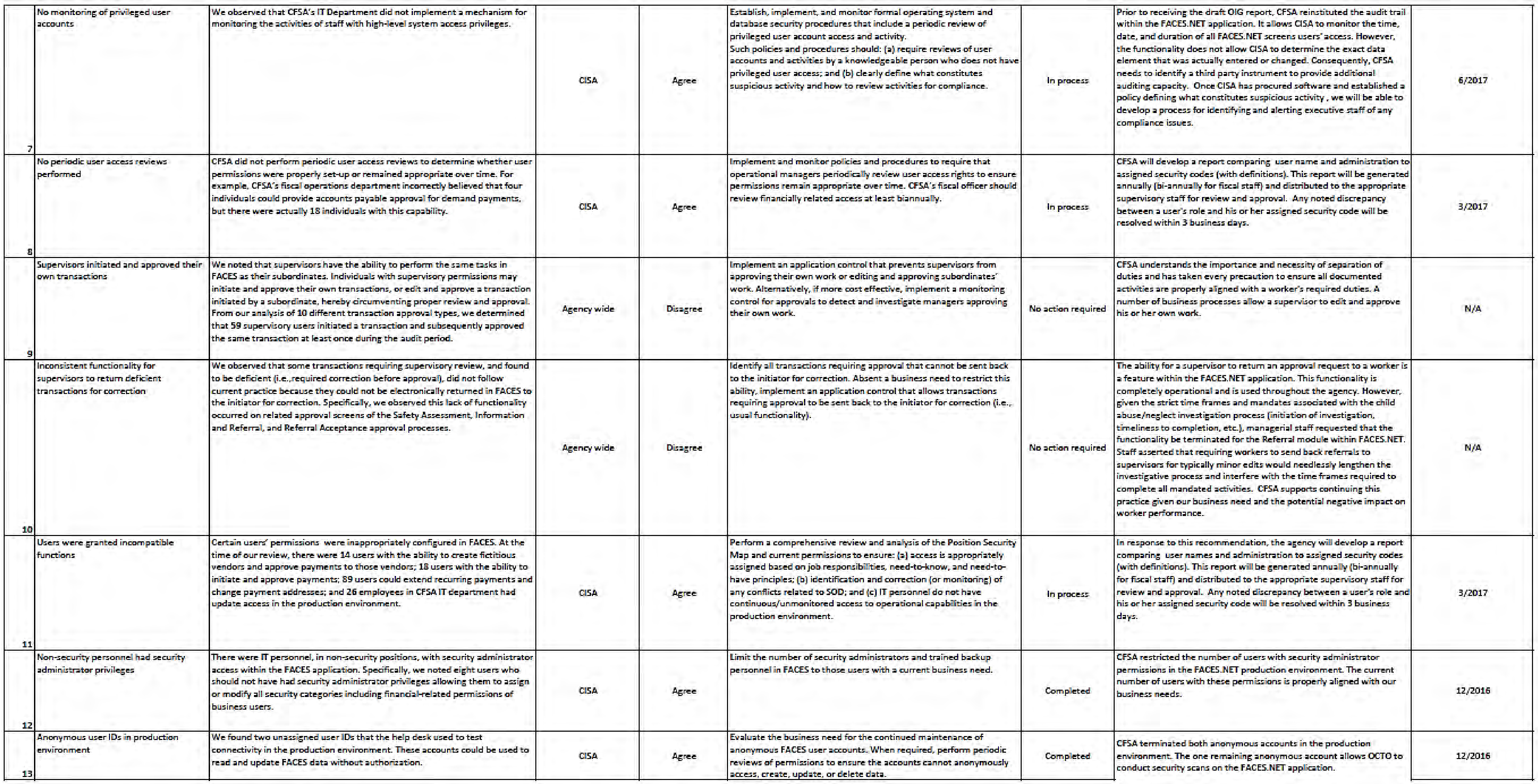
ATTACHMENT

APPENDIX C. AGENCY'S RESPONSE TO THE DRAFT REPORT



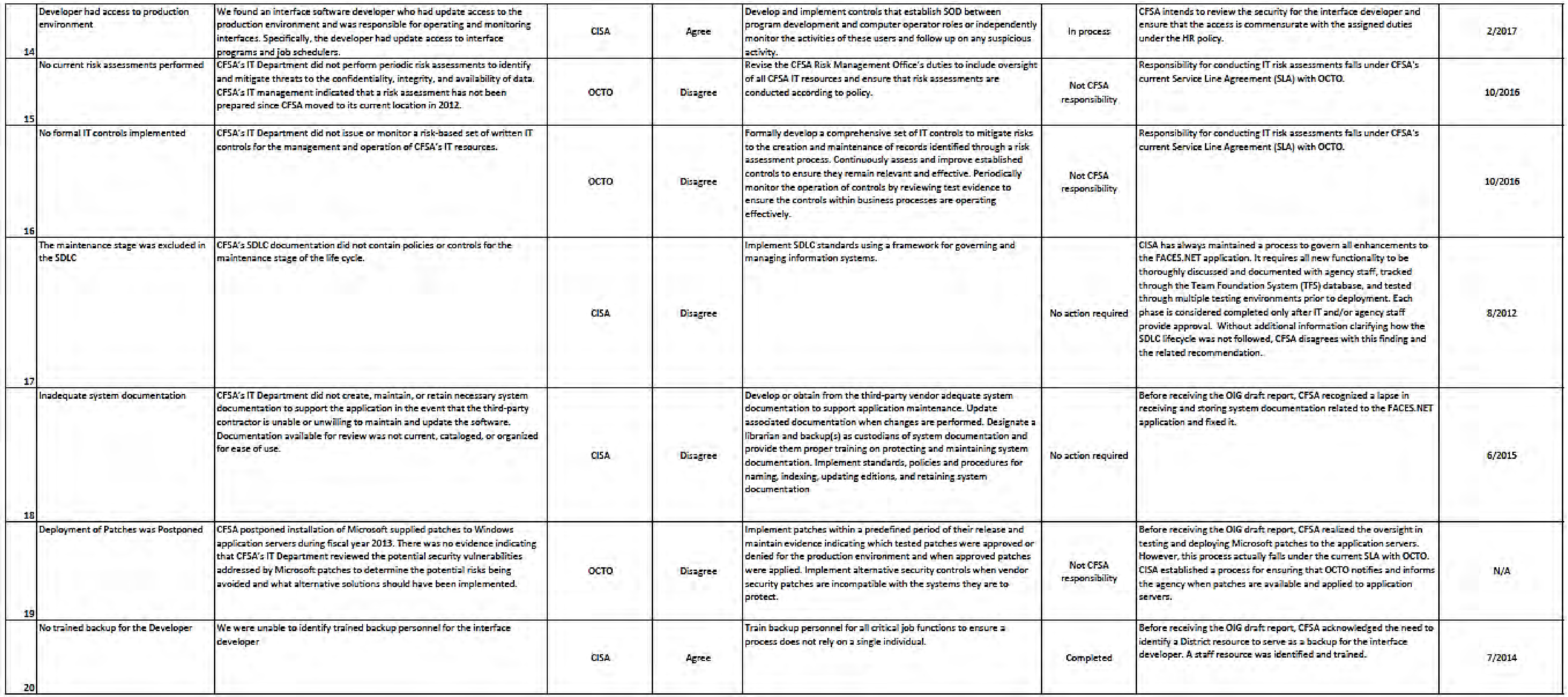
Number	Condition	OIG Finding	CFSA Responsibility	Agree/Disagree	OIG Recommendation	Status	Description (How was it completed?)	Completion/Proposed completion date
1	Inaccurate account balances in FACES	The record that tracks the balance remaining under a contract was not accurate in the FACES application. Balances are currently tracked manually outside of FACES.	Fiscal Operations	Disagree	Determine why the contract limit counter was disabled and is no longer properly tracking/tallying expenditures. Rnsure its functionality in FACES is fully restored, if more cost effective than the current manual tracking.	No action required	There is no evidence to suggest that the contract limit counter in FACES.NET has ever been disabled or terminated. Upong receiving the OIG draft report, CFSA retested the functionality and found it to work within appropriate operational parameters. In addition, agency staff report that FACES.NET is the system of record for child welfare and was never required to represent the full range of contracted services CFSA procures. Thus, CFSA does track and monitor some services outside of FACES.NET. Without further information from the OIG to clarify this issue, CFSA disagrees with this finding and the associated recommendation.	N/A
2	No data entry controls for service data	There were no input edits to ensure invoice service dates were entered in a valid date format or that the service date occurred in the past. We observed invalid date formats and inappropriate future dated transactions in the accounts payable subsidiary ledger of FACES. Implementing input edits will prevent some data entry errors we observed but it will not guarantee the data entered are accurate.	CISA	Disagree	Implement input edits on the service date fields to include a valid date format for service periods to ensure that the service start date precedes the service end date and the service dates precede the current date.	No action required	All service date fields are uniform within the FACES.NET application. These fields are not only mandatory but also include system validations that prohibit workers from entering service end dates that precede service start dates or allow workers to enter dates that precede the current date. Without further information from the OIG identifying service data errors, CFSA disagrees with this finding and the associated recommendation.	N/A
3	No established timeframes to correct inaccurate data	CFSA did not establish guidelines to correct errors identified on FACES' exception reports. We could find no documentation or directives on how such errors were to be monitored, recorded, and resolved. During the period tested, it took approximately 32 days, on average, to correct duplicate client records and more than 4 months to correct payment address errors once FACES identified reported errors.	Fiscal Operations	Agree	Implement and monitor policies, procedures, and standards for correcting exception reports generated by FACES. Establish standard timeframes, based on risk, for clearing individual exception reports.	Action plan to be determined	CFSA will revise existing policies and procedures to establish a process for reviewing exception reports and reconciling any noted discrepancies.	6/2017
4	No formally documented information security procedures	The security administration function did not formally document information security procedures. The procedures available are included with the general Employee Security Policy provide basic security objectives rather than detailed FACES procedures that would assist security users and their backup personnel in the consistent setup of users and application of policies.	CISA	Agree	Formally develop additional control procedures for security management activities and monitor compliance with current policies and procedures.	In process	CFSA has always maintained a staff person with the security necessary to perform his or her associated duties. HIPAA has been the guide through which CFSA has established policies and procedures for role-based security measures. LAN and WAN identifies the documents required to establish FACES.NET access along with FACES.NET Training enrollment. The general practice is to grant security according to the HR Position title once FACES training is completed. While this document is not exclusive for FACES, it has been identified as the Policy and Procedure for FACES user accounts. In addition, CISA also utilizes FACES.NET security categories document which outlines the role based security descriptions.	3/2017
5	Unix and Oracle Administrators did not have individual user ID's	Shared generic/privileged accounts were used to perform system administration functions without adequate monitoring controls over such activities.	CISA	Agree	Restrict the use of generic operating system and database IDs. Otherwise, monitor activities performed using generic ID as necessary.	In process	The agency updated the IT Access Control Policy to inform users that generic ID accounts will no longer be permitted. Enforcing the policy through the FACES.NET application and database remains outstanding.	3/2017
6	No business approval of position security map (Security profiles by position)	There was no evidence that CFSA business operations personnel reviewed and approved the position security map or reviewed the defined permissions for SOD conflicts. A review of all permissions indicated that 735 of the 1,379 users (53 percent) examined had more access than defined on the Position Security Map. Additionally, two inactive security codes (used to assign permissions) were assigned in 145 profiles and at least one position allowed incompatible functions.	CISA	Agree	Review the Position Security Map annually, or any time there are systemic changes affecting user permissions, to ensure access remains appropriate and there are no SOD conflicts. Evaluate new user permission requests for conflicts related to SOD. When conflicts will result from the request, obtain approval one level higher than is ordinarily required, and assign responsibility for monitoring controls to timely detect and address inappropriate activities.	In process	The business review and approval process for Position Security Mapping is completed via the FACES design documentation for systemic changes to ensure SOD compliance. Individuals are required to submit a CISA Security Form and attend additional FACES training if a change in FACES role base security is required. This information is then provided to CISA ISO for FACES access update.	3/2017

APPENDIX C. AGENCY'S RESPONSE TO THE DRAFT REPORT



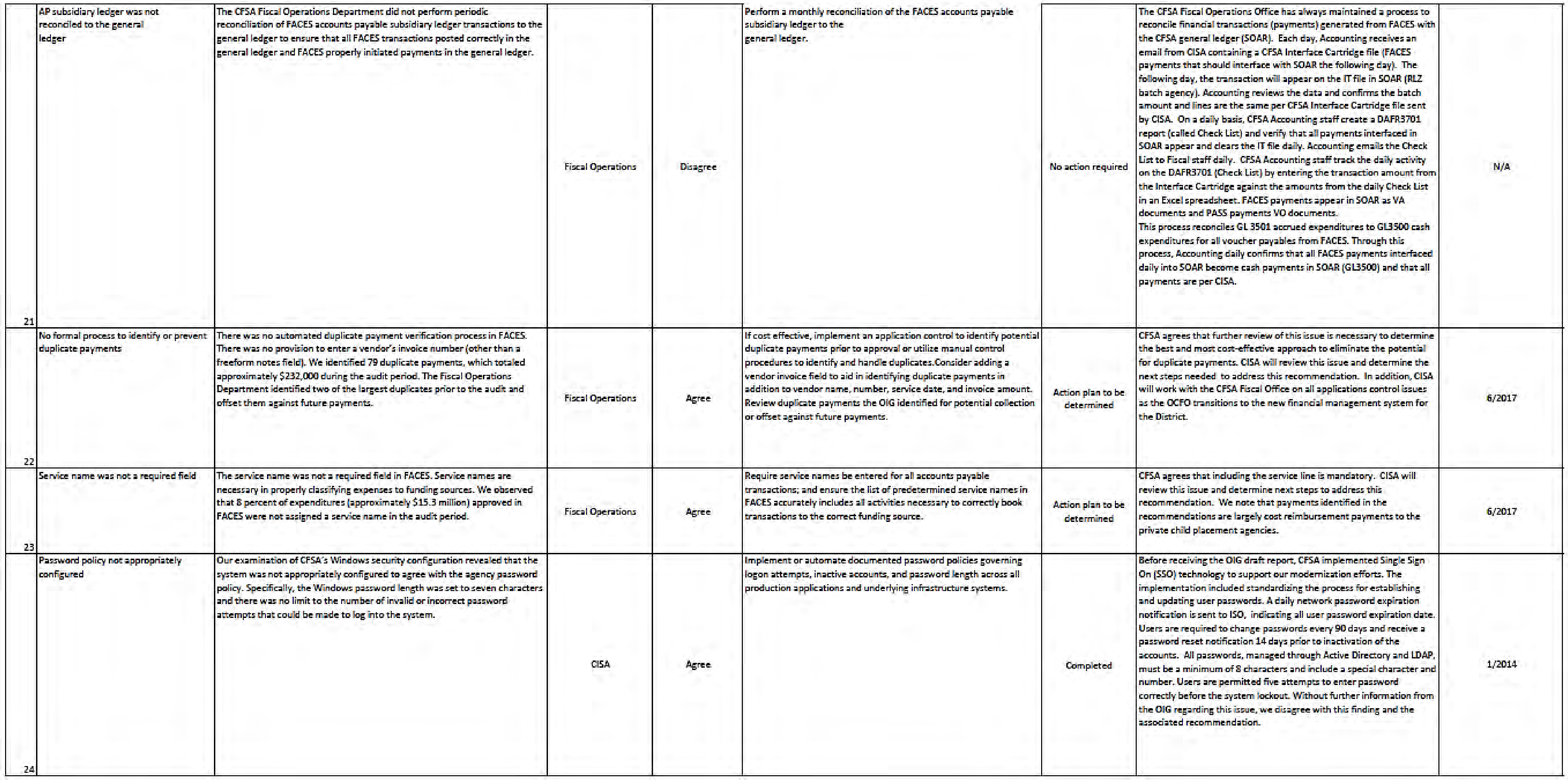
7	No monitoring of privileged user accounts	We observed that CFSA's IT Department did not implement a mechanism for monitoring the activities of staff with high-level system access privileges.	CISA	Agree	Establish, implement, and monitor formal operating system and database security procedures that include a periodic review of privileged user account access and activity. Such policies and procedures should: (a) require reviews of user accounts and activities by a knowledgeable person who does not have privileged user access; and (b) clearly define what constitutes suspicious activity and how to review activities for compliance.	In process	Prior to receiving the draft OIG report, CFSA reinstituted the audit trail within the FACES.NET application. It allows CISA to monitor the time, date, and duration of all FACES.NET screens users' access. However, the functionality does not allow CISA to determine the exact data element that was actually entered or changed. Consequently, CFSA needs to identify a third party instrument to provide additional auditing capacity. Once CISA has procured software and established a policy defining what constitutes suspicious activity , we will be able to develop a process for identifying and alerting executive staff of any compliance issues.	6/2017
8	No periodic user access reviews performed	CFSA did not perform periodic user access reviews to determine whether user permissions were properly set-up or remained appropriate over time. For example, CFSA's fiscal operations department incorrectly believed that four individuals could provide accounts payable approval for demand payments, but there were actually 18 individuals with this capability.	CISA	Agree	Implement and monitor policies and procedures to require that operational managers periodically review user access rights to ensure permissions remain appropriate over time. CFSA's fiscal officer should review financially related access at least biannually.	In process	CFSA will develop a report comparing user name and administration to assigned security codes (with definitions). This report will be generated annually (bi-annually for fiscal staff) and distributed to the appropriate supervisory staff for review and approval. Any noted discrepancy between a user's role and his or her assigned security code will be resolved within 3 business days.	3/2017
9	Supervisors initiated and approved their own transactions	We noted that supervisors have the ability to perform the same tasks in FACES as their subordinates. Individuals with supervisory permissions may initiate and approve their own transactions, or edit and approve a transaction initiated by a subordinate, hereby circumventing proper review and approval. From our analysis of 10 different transaction approval types, we determined that 59 supervisory users initiated a transaction and subsequently approved the same transaction at least once during the audit period.	Agency wide	Disagree	Implement an application control that prevents supervisors from approving their own work or editing and approving subordinates' work. Alternatively, if more cost effective, implement a monitoring control for approvals to detect and investigate managers approving their own work.	No action required	CFSA understands the importance and necessity of separation of duties and has taken every precaution to ensure all documented activities are properly aligned with a worker's required duties. A number of business processes allow a supervisor to edit and approve his or her own work.	N/A
10	Inconsistent functionality for supervisors to return deficient transactions for correction	We observed that some transactions requiring supervisory review, and found to be deficient (i.e.,required correction before approval), did not follow current practice because they could not be electronically returned in FACES to the initiator for correction. Specifically, we observed this lack of functionality occurred on related approval screens of the Safety Assessment, Information and Referral, and Referral Acceptance approval processes.	Agency wide	Disagree	Identify all transactions requiring approval that cannot be sent back to the initiator for correction. Absent a business need to restrict this ability, implement an application control that allows transactions requiring approval to be sent back to the initiator for correction (i.e., usual functionality).	No action required	The ability for a supervisor to return an approval request to a worker is a feature within the FACES.NET application. This functionality is completely operational and is used throughout the agency. However, given the strict time frames and mandates associated with the child abuse/neglect investigation process (initiation of investigation, timeliness to completion, etc.), managerial staff requested that the functionality be terminated for the Referral module within FACES.NET. Staff asserted that requiring workers to send back referrals to supervisors for typically minor edits would needlessly lengthen the investigative process and interfere with the time frames required to complete all mandated activities. CFSA supports continuing this practice given our business need and the potential negative impact on worker performance.	N/A
11	Users were granted incompatible functions	Certain users' permissions were inappropriately configured in FACES. At the time of our review, there were 14 users with the ability to create fictitious vendors and approve payments to those vendors; 18 users with the ability to initiate and approve payments; 89 users could extend recurring payments and change payment addresses; and 26 employees in CFSA IT department had update access in the production environment.	CISA	Agree	Perform a comprehensive review and analysis of the Position Security Map and current permissions to ensure: (a) access is appropriately assigned based on job responsibilities, need-to-know, and need-to-have principles; (b) identification and correction (or monitoring) of any conflicts related to SOD; and (c) IT personnel do not have continuous/unmonitored access to operational capabilities in the production environment.	In process	In response to this recommendation, the agency will develop a report comparing user names and administration to assigned security codes (with definitions). This report will be generated annually (bi-annually for fiscal staff) and distributed to the appropriate supervisory staff for review and approval. Any noted discrepancy between a user's role and his or her assigned security code will be resolved within 3 business days.	3/2017
12	Non-security personnel had security administrator privileges	There were IT personnel, in non-security positions, with security administrator access within the FACES application. Specifically, we noted eight users who should not have had security administrator privileges allowing them to assign or modify all security categories including financial-related permissions of business users.	CISA	Agree	Limit the number of security administrators and trained backup personnel in FACES to those users with a current business need.	Completed	CFSA restricted the number of users with security administrator permissions in the FACES.NET production environment. The current number of users with these permissions is properly aligned with our business needs.	12/2016
13	Anonymous user IDs in production environment	We found two unassigned user IDs that the help desk used to test connectivity in the production environment. These accounts could be used to read and update FACES data without authorization.	CISA	Agree	Evaluate the business need for the continued maintenance of anonymous FACES user accounts. When required, perform periodic reviews of permissions to ensure the accounts cannot anonymously access, create, update, or delete data.	Completed	CFSA terminated both anonymous accounts in the production environment. The one remaining anonymous account allows OCTO to conduct security scans on the FACES.NET application.	12/2016

APPENDIX C. AGENCY'S RESPONSE TO THE DRAFT REPORT



14	Developer had access to production environment	We found an interface software developer who had update access to the production environment and was responsible for operating and monitoring interfaces. Specifically, the developer had update access to interface programs and job schedulers.	CISA	Agree	Develop and implement controls that establish SOD between program development and computer operator roles or independently monitor the activities of these users and follow up on any suspicious activity.	In process	CFSA intends to review the security for the interface developer and ensure that the access is commensurate with the assigned duties under the HR policy.	2/2017
15	No current risk assessments performed	CFSA's IT Department did not perform periodic risk assessments to identify and mitigate threats to the confidentiality, integrity, and availability of data. CFSA's IT management indicated that a risk assessment has not been prepared since CFSA moved to its current location in 2012.	OCTO	Disagree	Revise the CFSA Risk Management Office's duties to include oversight of all CFSA IT resources and ensure that risk assessments are conducted according to policy.	Not CFSA responsibility	Responsibility for conducting IT risk assessments falls under CFSA's current Service Line Agreement (SLA) with OCTO.	10/2016
16	No formal IT controls implemented	CFSA's IT Department did not issue or monitor a risk-based set of written IT controls for the management and operation of CFSA's IT resources.	OCTO	Disagree	Formally develop a comprehensive set of IT controls to mitigate risks to the creation and maintenance of records identified through a risk assessment process. Continuously assess and improve established controls to ensure they remain relevant and effective. Periodically monitor the operation of controls by reviewing test evidence to ensure the controls within business processes are operating effectively.	Not CFSA responsibility	Responsibility for conducting IT risk assessments falls under CFSA's current Service Line Agreement (SLA) with OCTO.	10/2016
17	The maintenance stage was excluded in the SDLC	CFSA's SDLC documentation did not contain policies or controls for the maintenance stage of the life cycle.	CISA	Disagree	Implement SDLC standards using a framework for governing and managing information systems.	No action required	CISA has always maintained a process to govern all enhancements to the FACES.NET application. It requires all new functionality to be thoroughly discussed and documented with agency staff, tracked through the Team Foundation System (TFS) database, and tested through multiple testing environments prior to deployment. Each phase is considered completed only after IT and/or agency staff provide approval. Without additional information clarifying how the SDLC lifecycle was not followed, CFSA disagrees with this finding and the related recommendation.	8/2012
18	Inadequate system documentation	CFSA's IT Department did not create, maintain, or retain necessary system documentation to support the application in the event that the third-party contractor is unable or unwilling to maintain and update the software. Documentation available for review was not current, cataloged, or organized for ease of use.	CISA	Disagree	Develop or obtain from the third-party vendor adequate system documentation to support application maintenance. Update associated documentation when changes are performed. Designate a librarian and backup(s) as custodians of system documentation and provide them proper training on protecting and maintaining system documentation. Implement standards, policies and procedures for naming, indexing, updating editions, and retaining system documentation	No action required	Before receiving the OIG draft report, CFSA recognized a lapse in receiving and storing system documentation related to the FACES.NET application and fixed it.	6/2015
19	Deployment of Patches was Postponed	CFSA postponed installation of Microsoft supplied patches to Windows application servers during fiscal year 2013. There was no evidence indicating that CFSA's IT Department reviewed the potential security vulnerabilities addressed by Microsoft patches to determine the potential risks being avoided and what alternative solutions should have been implemented.	OCTO	Disagree	Implement patches within a predefined period of their release and maintain evidence indicating which tested patches were approved or denied for the production environment and when approved patches were applied. Implement alternative security controls when vendor security patches are incompatible with the systems they are to protect.	Not CFSA responsibility	Before receiving the OIG draft report, CFSA realized the oversight in testing and deploying Microsoft patches to the application servers. However, this process actually falls under the current SLA with OCTO. CISA established a process for ensuring that OCTO notifies and informs the agency when patches are available and applied to application servers.	N/A
20	No trained backup for the Developer	We were unable to identify trained backup personnel for the interface developer	CISA	Agree	Train backup personnel for all critical job functions to ensure a process does not rely on a single individual.	Completed	Before receiving the OIG draft report, CFSA acknowledged the need to identify a District resource to serve as a backup for the interface developer. A staff resource was identified and trained.	7/2014

APPENDIX C. AGENCY'S RESPONSE TO THE DRAFT REPORT



21	AP subsidiary ledger was not reconciled to the general ledger	The CFSA Fiscal Operations Department did not perform periodic reconciliation of FACES accounts payable subsidiary ledger transactions to the general ledger to ensure that all FACES transactions posted correctly in the general ledger and FACES properly initiated payments in the general ledger.	Fiscal Operations	Disagree	Perform a monthly reconciliation of the FACES accounts payable subsidiary ledger to the general ledger.	No action required	The CFSA Fiscal Operations Office has always maintained a process to reconcile financial transactions (payments) generated from FACES with the CFSA general ledger (SOAR). Each day, Accounting receives an email from CISA containing a CFSA Interface Cartridge file (FACES payments that should interface with SOAR the following day). The following day, the transaction will appear on the IT file in SOAR (RLZ batch agency). Accounting reviews the data and confirms the batch amount and lines are the same per CFSA Interface Cartridge file sent by CISA. On a daily basis, CFSA Accounting staff create a DAFR3701 report (called Check List) and verify that all payments interfaced in SOAR appear and clears the IT file daily. Accounting emails the Check List to Fiscal staff daily. CFSA Accounting staff track the daily activity on the DAFR3701 (Check List) by entering the transaction amount from the Interface Cartridge against the amounts from the daily Check List in an Excel spreadsheet. FACES payments appear in SOAR as VA documents and PASS payments VO documents. This process reconciles GL 3501 accrued expenditures to GL3500 cash expenditures for all voucher payables from FACES. Through this process, Accounting daily confirms that all FACES payments interfaced daily into SOAR become cash payments in SOAR (GL3500) and that all payments are per CISA.	N/A
22	No formal process to identify or prevent duplicate payments	There was no automated duplicate payment verification process in FACES. There was no provision to enter a vendor's invoice number (other than a freeform notes field). We identified 79 duplicate payments, which totaled approximately $232,000 during the audit period. The Fiscal Operations Department identified two of the largest duplicates prior to the audit and offset them against future payments.	Fiscal Operations	Agree	If cost effective, implement an application control to identify potential duplicate payments prior to approval or utilize manual control procedures to identify and handle duplicates.Consider adding a vendor invoice field to aid in identifying duplicate payments in addition to vendor name, number, service date, and invoice amount. Review duplicate payments the OIG identified for potential collection or offset against future payments.	Action plan to be determined	CFSA agrees that further review of this issue is necessary to determine the best and most cost-effective approach to eliminate the potential for duplicate payments. CISA will review this issue and determine the next steps needed to address this recommendation. In addition, CISA will work with the CFSA Fiscal Office on all applications control issues as the OCFO transitions to the new financial management system for the District.	6/2017
23	Service name was not a required field	The service name was not a required field in FACES. Service names are necessary in properly classifying expenses to funding sources. We observed that 8 percent of expenditures (approximately $15.3 million) approved in FACES were not assigned a service name in the audit period.	Fiscal Operations	Agree	Require service names be entered for all accounts payable transactions; and ensure the list of predetermined service names in FACES accurately includes all activities necessary to correctly book transactions to the correct funding source.	Action plan to be determined	CFSA agrees that including the service line is mandatory. CISA will review this issue and determine next steps to address this recommendation. We note that payments identified in the recommendations are largely cost reimbursement payments to the private child placement agencies.	6/2017
24	Password policy not appropriately configured	Our examination of CFSA's Windows security configuration revealed that the system was not appropriately configured to agree with the agency password policy. Specifically, the Windows password length was set to seven characters and there was no limit to the number of invalid or incorrect password attempts that could be made to log into the system.	CISA	Agree	Implement or automate documented password policies governing logon attempts, inactive accounts, and password length across all production applications and underlying infrastructure systems.	Completed	Before receiving the OIG draft report, CFSA implemented Single Sign On (SSO) technology to support our modernization efforts. The implementation included standardizing the process for establishing and updating user passwords. A daily network password expiration notification is sent to ISO, indicating all user password expiration date. Users are required to change passwords every 90 days and receive a password reset notification 14 days prior to inactivation of the accounts. All passwords, managed through Active Directory and LDAP, must be a minimum of 8 characters and include a special character and number. Users are permitted five attempts to enter password correctly before the system lockout. Without further information from the OIG regarding this issue, we disagree with this finding and the associated recommendation.	1/2014

APPENDIX C. AGENCY'S RESPONSE TO THE DRAFT REPORT

25	Some terminated and inactive user accounts were not disabled in a timely manner	CFSA did not disable all tested accounts of terminated users according to policy. In addition, we observed that CFSA did not consistently disable inactive user accounts. We sampled 27 users to determine whether their access privileges were disabled in a timely manner. We found that 12 tested terminations (44 percent) were not disabled according to policy. The median time to terminate access was 10 business days. We also found two inactive accounts that were not disabled.	CISA	Agree	Implement and monitor a procedure to disable access of District employees and contractors' access to FACES within 1 business day after separation and after 90 days of inactivity.	Completed	Before receiving the OIG draft report, CFSA implemented a procedure to ensure that user accounts are de-activated upon exit in according with HRA policy. In addition to receiving "Projected CFSA Employee Departure" notifications from HRA, CFSA staff monitor the system and disable accounts with no activity for 90 days. Accounts for internal agency staff are disabled immediately after the exit interview process. However, the agency continues to work with contracted providers to receive notifications about external users that are separated from respective agencies.	1/2014
26	Concurrent log-in sessions were not limited	The number of concurrent FACES sessions that users could open was not limited to one.	CISA	Agree	Limit the number of concurrent FACES sessions for each user to one, unless there is a business need for additional sessions, or document in agency security policy the accounts that require concurrent access, their business needs, and number of sessions permitted.	Completed	CFSA restricted any user from having multiple active sessions of FACES.NET on one device or computer.	6/2013
27	External relationships were not properly managed	We were unable to obtain current or signed memoranda of understanding and service level agreements for interagency relationships in 7 of 8 tested cases.	CFSA	Agree	Designate an official or office to be responsible for IT-related external relationships to ensure they are current and address all exchanges of electronic information between District agencies and third parties. Ensure compliance with contractual obligations is assessed periodically.	Completed	CFSA's Office of Planning, Policy and Program Support has been tasked with the maintainence of all Memorandums of Understanding and Memorandums of Agreements. The agency will ensure that all IT external relationships remain compliant with this policy.	6/2015
28	N/A	Mentioned in the body of the report, but not directly linked to a condition or finding.	Agency wide	N/A	Adopt an industry-recognized IT governance and management framework to accommodate the development and maintenance of an IT strategic plan, and integrate and institutionalize good business practices that ensure IT resources are appropriately used to support CFSA's business objectives. Develop and maintain an IT strategic plan aligned with CFSA's strategic objectives and budgetary resources.	Completed	Under the leadership of the Director, CISA developed and is implementing a four-year IT strategic plan that aligns with CFSA's strategic objectives and budgetary resources. Without further information from the OIG regarding this issue, we disagree with this recommendation.	6/2014
29			Contracts	N/A	Issue policies and procedures to ensure that future decisions to contract for consulting services are properly substantiated and conform with 27 DCMR § 1901 and other applicable District laws, regulations, and requirements.	Completed	CFSA has always complied with District policies and procedures related to procuring consulting services. According to 27 DCMR 1901.5, "the contracting officer shall be responsible for determining whether a request by an agency to contract for expert or consulting services, regardless of dollar amount, is justified under 1901.4 or whether the services must be obtained in accordance with District personnel law and regulations. The contracting officer's determination shall be final. " Without further information from the OIG regarding this issue, we disagree with this recommendation.	6/2015

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	**CFSA Concurs**	**Resolved**	**Documentation Required**	**Target Action Date**
1. Determine why the contract limit counter was disabled and is no longer properly tracking/tallying expenditures, and ensure that its functionality in FACES is fully restored, if more cost effective than the current manual tracking.	No	Yes, resolved and open pending evidence of stated actions.	Provide the results of the contract limit counter assessment reviewed and verified by accounts payable.	Within 30 days of receipt of this report.
2. Implement input edits on the service date fields to include a valid date format for service periods to ensure that the service start date precedes the service end date and the service dates precede the current date.	No	Yes, resolved and open pending evidence of stated actions.	Provide example screenshots showing the functioning of input edits that give notice to users and prevent incorrect service dates.	Within 30 days of receipt of this report.
3. Implement and monitor policies, procedures, and standards for correcting exception reports generated by FACES. Establish standard timeframes, based on risk, for clearing individual exception reports.	Yes	Yes, resolved and open pending completion of planned actions.	Provide evidence of the establishment of standards to process and monitor the correction of exception reports.	6/2017
4. Formally develop additional control procedures for security management activities and monitor compliance with current policies and procedures.	Yes	Yes, resolved and open pending completion of planned actions.	Provide formal internal control procedures for security management.	3/2017
5. Restrict the use of generic operating system and database IDs. Otherwise, monitor activities performed using generic ID as necessary.	Yes	Yes, resolved and open pending completion of planned actions.	Provide updated IT access control policy and current Unix and Oracle access control lists.	3/2017

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	**CFSA Concurs**	**Resolved**	**Documentation Required**	**Target Action Date**
6. Review the Position Security Map annually, or any time there are systemic changes affecting user permissions, to ensure access remains appropriate and there are no SOD conflicts. Evaluate new user permission requests for conflicts related to SOD. When conflicts will result from the request, obtain approval one level higher than is ordinarily required, and assign responsibility for monitoring controls to timely detect and address inappropriate activities.	Yes	Yes, resolved and open pending completion of planned actions.	Provide documentation of the business review of Position Security Map which identifies incompatible permissions.	3/2017
7. Establish, implement, and monitor formal operating system and database security procedures that include a periodic review of privileged user account access and activity. Such policies and procedures should: (a) require reviews of user accounts and activities by a knowledgeable person who does not have privileged user access; and (b) clearly define what constitutes suspicious activity and how to review activities for compliance.	Yes	Yes, resolved and open pending completion of planned actions.	Provide evidence of privileged user monitoring.	6/2017

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	**CFSA Concurs**	**Resolved**	**Documentation Required**	**Target Action Date**
8. Implement and monitor policies and procedures to require that operational managers periodically review user access rights to ensure permissions remain appropriate over time. CFSA's fiscal officer should review financially related access at least biannually.	Yes	Yes, resolved and open pending completion of planned actions.	Provide report comparing usernames and assigned security codes.	3/2017
9. Implement an application control that prevents supervisors from approving their own work or editing and approving subordinates' work. Alternatively, if more cost effective, implement a monitoring control for approvals to detect and investigate managers approving their own work.	No	No, unresolved and open.	Evidence of controls to mitigate the risk of fraudulent or erroneous transactions.	We request that CFSA reconsider its position on this recommendation and provide corrective actions within 30 days of receipt of this report.
10. Identify all transactions requiring approval that cannot be sent back to the initiator for correction. Absent a business need to restrict this ability, implement an application control that allows transactions requiring approval to be sent back to the initiator for correction (i.e., usual functionality).	No	Yes, CFSA accepted the risk that some processes will be better served without this functionally. We consider this resolved and closed.	None	Closed

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	CFSA Concurs	Resolved	Documentation Required	Target Action Date
11. Perform a comprehensive review and analysis of the Position Security Map and current permissions to ensure: (a) access is appropriately assigned based on job responsibilities, need-to-know, and need-to-have principles; (b) identification and correction (or monitoring) of any conflicts related to SOD; and (c) IT personnel do not have continuous unmonitored access to operational capabilities in the production environment.	Yes	Yes, resolved and open pending completion of planned actions.	Provide report comparing usernames and assigned security codes.	3/2017
12. Limit the number of security administrators and trained backup personnel in FACES to those users with a current business need.	Yes	Yes, resolved and open pending evidence of stated actions.	Provide evidence that CFSA restricted the number of users with security permissions in the FACES production environment.	12/2016
13. Evaluate the business need for the continued maintenance of anonymous FACES user accounts. When required, perform periodic reviews of permissions to ensure the accounts cannot anonymously access, create, update, or delete data.	Yes	Yes, resolved and open pending evidence of stated actions.	Provide evidence that CFSA deleted the two anonymous access accounts.	12/2016

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	**CFSA Concurs**	**Resolved**	**Documentation Required**	**Target Action Date**
14. Develop and implement controls that establish SOD between program development and computer operator roles or independently monitor the activities of these users and follow up on any suspicious activity.	Yes	Yes, resolved and open pending completion of planned actions.	Provide results of the review of the security assessment for the interface developer.	2/2017
15. Revise the CFSA Risk Management Office's duties to include oversight of all CFSA IT resources and ensure that risk assessments are conducted according to policy.	No	Yes, resolved and open pending evidence of stated actions.	Provide the most current OCTO risk assessment provided to CFSA Management.	10/2016
16. Formally develop a comprehensive set of IT controls to mitigate risks to the creation and maintenance of records identified through a risk assessment process. Continuously assess and improve established controls to ensure they remain relevant and effective. Periodically monitor the operation of controls by reviewing test evidence to ensure the controls within business processes are operating effectively.	No	No, unresolved and open.	Provide an action plan to ensure controls are defined to mitigate risks identified internally or by OCTO. The plan should demonstrate how management will monitor the effectiveness of their controls.	We request that CFSA reconsider its position on this recommendation and provide corrective actions within 30 days of receipt of this report.
17. Implement SDLC standards using a framework for governing and managing information systems.	No	Yes, resolved and open pending evidence of stated actions.	Provide documented SDLC process.	Within 30 days of receipt of this report.

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	**CFSA Concurs**	**Resolved**	**Documentation Required**	**Target Action Date**
18. Develop or obtain from the third-party vendor adequate system documentation to support application maintenance. Update associated documentation when changes are performed. Designate a librarian and backup(s) as custodians of system documentation and provide them proper training on protecting and maintaining system documentation. Implement standards, policies and procedures for naming, indexing, updating editions, and retaining system documentation.	No	Yes, resolved and open pending evidence of stated actions.	Provide evidence that system documentation exists independent of the third party vendor and is being maintained to support the FACES application.	6/2015
19. Implement patches within a predefined period of their release and maintain evidence indicating which tested patches were approved or denied for the production environment and when approved patches were applied. Implement alternative security controls when vendor security patches are incompatible with the systems they are to protect.	No	Yes, resolved and open pending evidence of stated actions.	Provide documentation showing Windows patches are current.	Within 30 days of receipt of this report.
20. Train backup personnel for all critical job functions to ensure a process does not rely on a single individual.	Yes	Yes, resolved and open pending evidence of stated actions.	Provide name and qualifications of trained backup interface developer.	7/2014

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	**CFSA Concurs**	**Resolved**	**Documentation Required**	**Target Action Date**
21. Perform a monthly reconciliation of the FACES accounts payable subsidiary ledger to the general ledger.	No	Yes, resolved and open pending evidence of stated actions.	Provide evidence of the daily reconciliation of FACES accounts payable subsidiary ledger to the general ledger.	Within 30 days of receipt of this report.
22. If cost effective, implement an application control to identify potential duplicate payments prior to approval or utilize manual control procedures to identify and handle duplicates. Consider adding a vendor invoice field to aid in identifying duplicate payments in addition to vendor name, number, service date, and invoice amount. Review duplicate payments the OIG identified for potential collection or offset against future payments.	Yes	Yes, resolved and open pending completion of planned actions.	Provide action plan to identify duplicate payments and evidence of implementation.	6/2017
23. Require service names be entered for all accounts payable transactions; and ensure the list of predetermined service names in FACES accurately includes all activities necessary to correctly book transactions to the correct funding source.	Yes	Yes, resolved and open pending completion of planned actions.	Provide action plan to make service name mandatory and evidence of implementation.	6/2017

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	CFSA Concurs	Resolved	Documentation Required	Target Action Date
24. Implement or automate documented password policies governing logon attempts, inactive accounts, and password length across all production applications and underlying infrastructure systems.	Yes	Yes, resolved and open pending evidence of stated actions.	Provide evidence that the single sign-on security configuration complies with CFSA's password policy.	1/2014
25. Implement and monitor a procedure to disable access of District employees and contractors' access to FACES within 1 business day after separation and after 90 days of inactivity.	Yes	Yes, resolved and open pending evidence of stated actions.	Provide evidence of a procedure to disable access to District employees after the exit interview process and all users after 90 days of inactivity. Additionally, provide evidence of how contractors are disabled within 1 business day of separation.	1/2014
26. Limit the number of concurrent FACES sessions for each user to one, unless there is a business need for additional sessions, or document in agency security policy the accounts that require concurrent access, their business needs, and number of sessions permitted.	Yes	Yes, resolved and open pending evidence of stated actions.	Provide documentation to support that FACES users can only have one active session at a time.	6/2013

APPENDIX D. ACTIONS REQUIRED FOR DISPOSITION OF RECOMMENDATIONS

Required Action Steps

Recommendation	CFSA Concurs	Resolved	Documentation Required	Target Action Date
27. Designate an official or office to be responsible for IT-related external relationships to ensure they are current and address all exchanges of electronic information between District agencies and third parties. Ensure compliance with contractual obligations is assessed periodically.	Yes	Yes, resolved and open pending evidence of stated actions.	Provide current copies of MOUs for interagency IT agreements.	6/2015
28. Adopt an industry-recognized IT governance and management framework to accommodate the development and maintenance of an IT strategic plan, and integrate and institutionalize good business practices that ensure IT resources are appropriately used to support CFSA's business objectives. Develop and maintain an IT strategic plan aligned with CFSA's strategic objectives and budgetary resources.	No	Yes, resolved and open pending evidence of stated actions.	Provide a copy of the 4-year IT strategic plan and CFSA strategic objectives.	6/2014
29. Issue policies and procedures to ensure that future decisions to contract for consulting services are properly substantiated and conform with 27 DCMR § 1901 and other applicable District laws, regulations, and requirements.	No	No, unresolved and open.	Provide an action plan to ensure future contracting decisions are properly substantiated and conform with District laws, regulations, and requirements.	We request that CFSA reconsider its position on this recommendation and provide acceptable corrective actions within 30 days of receipt of this report.