COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

WENDY L. WATANABE
AUDITOR-CONTROLLER

JUDI E. THOMAS
CHIEF DEPUTY

ASST. AUDITOR-CONTROLLERS

ROBERT A. DAVIS
JOHN NAIMO
JAMES L. SCHNEIDERMAN

October 24, 2012

TO: Supervisor Zev Yaroslavsky, Chairman
Supervisor Gloria Molina
Supervisor Mark Ridley-Thomas
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: Wendy L. Watanabe
Auditor-Controller

SUBJECT: **REVIEW OF THE DEPARTMENT OF CHILDREN AND FAMILY SERVICES' AUTOMATED PROVIDER PAYMENT SYSTEM**

As part of our responsibility to ensure proper safeguarding of County resources, and that departments comply with County fiscal policies and procedures, we reviewed the Department of Children and Family Services' (DCFS or Department) controls over payments processed by the Automated Provider Payment System (APPS or System). Our review included determining if the System's controls were adequate to ensure DCFS only made valid and authorized payments using APPS.

DCFS uses APPS to calculate and pay foster care providers and relative care givers for children placed in their homes. In Fiscal Year 2010-11, DCFS paid over $498 million to foster and kinship care providers through APPS.

Results of Review

DCFS has established appropriate controls over physical access to APPS terminals, and ensuring that the System requires users to re-enter their passwords if there is no activity for a set period of time. However, DCFS needs to strengthen its controls over other areas of APPS payment processing. Specifically:

- DCFS needs to restrict access to APPS. We noted that DCFS did not terminate APPS access for 35 users who transferred jobs or left DCFS. Two of the terminated employees' access rights were used after the employees left DCFS,

and one of these employee's access was used to generate payment vouchers. We also noted that two employees have unneeded access to modify the APPS payment file, which is used to issue approximately $1.3 million in payments daily.

DCFS' attached response indicates that they removed the unneeded APPS access, and determined that vouchers generated with the terminated user's access were valid. DCFS will also change the System and their procedures to restrict APPS access in the future.

- DCFS needs to separate incompatible System duties. We noted that 62 APPS users could both add and modify vendor information on the System, and process foster care vouchers/payments. These duties should be separated.

  DCFS' response indicates they separated the incompatible APPS duties, and are working on System changes to ensure proper separation of duties in the future.

- DCFS needs to ensure child placement/payment information is accurate and authorized before processing APPS payments. We noted 15 problems with the 35 payments reviewed, including data entry errors and placements/payments that were not properly authorized/supported. Some of the errors caused $96,450 in overpayments which DCFS is working to recover.

  DCFS' response indicates that they will enforce existing approval procedures to ensure placement/payment information is accurate, before processing APPS payments. DCFS also resolved the overpayments noted in our review.

- DCFS needs to review and approve changes to payment rates and the vendor table in APPS, and require support for payee mailing addresses. APPS issues $498 million in payments each year, most of which are based on pre-programmed standard rates and addresses in the System's vendor table. We noted that changes to rates and vendor tables are not reviewed. DCFS also did not have documentation to support that 14 (70%) of 20 payments reviewed were mailed to the appropriate address. While we did not identify any inappropriate payments, these issues significantly increase the risk of errors and inappropriate payments.

  DCFS' response indicates they established a formal review and approval process for changes to the payment rate table, and will develop procedures to review and approve changes to vendor names and addresses in the APPS vendor table.

- DCFS needs to resolve payments that are not processed by the System (suspended payments) timely. Five (50%) of ten suspended payments reviewed were unresolved for over a year.

DCFS' response indicates they have instructed staff to monitor and resolve suspended payments on an ongoing basis. They will also work to resolve the five suspended payments noted in our review.

- DCFS needs to prevent duplicate providers in APPS. We noted that APPS does not require a unique provider identifier, such as a State license or Tax Identification Number, resulting in numerous providers having duplicate records on the System. APPS produces a monthly report of possible duplicate providers, but DCFS staff had not reviewed the exceptions in three years.

  DCFS' response indicates that they will enhance the APPS provider search function to help staff avoid creating duplicate providers, and have instructed staff to review and resolve duplicate providers in the exception report. DCFS also indicated that they will evaluate the forms of identification required for out-of-home placements, which may be used as unique identifiers.

Details of our review and recommendations for corrective action are included in Attachment I. While our review did not disclose any inappropriate payments, the weaknesses noted in this report are serious and, if not corrected, could allow inappropriate payments to go undetected.

Review of Report

We discussed the results of our review with DCFS management. The Department's response (Attachment II) indicates general agreement with our findings and recommendations. DCFS' response also describes the corrective actions they have taken, or plan to take, to address the recommendations in our report.

We thank DCFS management and staff for their cooperation and assistance during our review. Please call me if you have any questions, or your staff may contact Robert Campbell at (213) 253-0101.

WLW:JLS:RGC:MP

Attachments

c: Philip L. Browning, Director, Department of Children and Family Services
William T Fujioka, Chief Executive Officer
Public Information Office
Audit Committee

DEPARTMENT OF CHILDREN AND FAMILY SERVICES
AUTOMATED PROVIDER PAYMENT SYSTEM REVIEW

Background

The Department of Children and Family Services (DCFS or Department) uses the Automated Provider Payment System (APPS or System) to calculate and pay foster care providers and relative care givers for children placed in their homes. APPS receives child placement information from the Child Welfare Services/Case Management System (CWS/CMS), calculates provider payments based on the type and length of placement, and transmits payment requests to the County's accounting system (eCAPS) to issue warrants. In Fiscal Year 2010-11, DCFS paid over $498 million through APPS.

Access Controls

Inappropriate User Access

County Fiscal Manual (CFM) Section 8.6.3 requires departments to limit system access based on each user's responsibilities, to reduce the risk of error, fraud, or other inappropriate activity.

We noted that DCFS did not terminate the access for 35 users who transferred jobs or left the Department. In two cases, the terminated employees' APPS log-on identifications (IDs) were used after the employees' termination dates, one of them to generate vouchers, which providers use to request payments. DCFS staff should promptly remove the terminated employees' access, and ensure the payment vouchers were valid.

We also noted that two employees had unneeded access to modify the APPS payment file. This is a significant risk because the payment file is used to issue approximately 1,000 payments, totaling $1.3 million, per day. In addition, 62 APPS users can change payee information in the vendor table, and process foster care vouchers/payments. CFM Section 4.5.10 requires these duties to be separated to reduce the risk of inappropriate payments.

Recommendations

DCFS management:

1. **Remove unnecessary System access, and ensure access is canceled when employees terminate or change jobs.**

2. **Ensure the payment vouchers printed with the terminated employees' IDs were valid.**

3. **Separate vendor table update and payment processing capabilities.**

Access Control Procedures

We identified several administrative and control weaknesses that contributed to the access issues noted above:

- DCFS does not have written policies and procedures to create, limit, and periodically review users' System access as required by CFM Section 8.6.4. In addition to the inappropriate access noted earlier, we noted three active APPS user IDs that were created in error, but had not been removed.

- DCFS does not monitor users with high-level System access as required by CFM Section 8.6.4. Thirteen APPS IDs can modify user access levels and/or update payment rates, and those changes were not monitored, reviewed, or approved by management. Also, two APPS IDs, including one with high-level access, were not assigned to specific employees, and therefore, there was no record of who processed transactions with those IDs. .

- DCFS did not have documented procedures to add, change, or disable APPS access, and 16 (80%) of the 20 users reviewed did not have written authorization for their access level.

- APPS allowed multiple, simultaneous log-ons with a single user ID. The System should only allow one active session per user, to prevent employees from sharing IDs.

- APPS did not require passwords to be reset every 90 days, or be case-sensitive, and include both alpha and numeric characters.

- APPS reporting function could be accessed with a default password that is commonly known by staff. This could result in unauthorized access to reports containing sensitive child placement information.

To ensure that APPS access is authorized and appropriate, DCFS management should implement the following recommendations.

Recommendations

DCFS management:

4. **Establish policies and procedures to create, limit, and periodically review APPS access roles.**

5. **Remove APPS IDs that were created in error.**

6. **Monitor users with high-level System access.**

7. **Ensure each APPS ID is assigned to a specific individual.**

8. **Document procedures to add, change, and disable users in APPS, and ensure staff obtain written authorization for access assignments.**

9. **Limit each user to a single active session, and prevent multiple log-ons.**

10. **Ensure APPS passwords are reset every 90 days, are case-sensitive, and include both alpha and numeric characters.**

11. **Reset the default password to access APPS reports, and require users to reset the default password on their next log-on.**

Payment Processing Controls

Placement/Payment Data Entry

DCFS staff authorize child placements and related payments on hard-copy forms, which two employees enter and approve in CWS/CMS for payment in APPS.

We noted 15 issues for the 35 payments we reviewed. Specifically:

- Three (9%) payments contained data entry errors, resulting in overpayments of $96,450 and underpayments of $9,478. DCFS is working to recover the overpayments and resolve the underpayments.

- Four (11%) payments, totaling $12,059, were not properly authorized on the hard-copy forms.

- Eight (23%) payments, totaling $26,164, did not have hard-copy authorization forms or payment vouchers, which providers sign indicating the child was in their care. Also, a provider did not qualify for one of the unsupported payments, resulting in a $240 overpayment.

DCFS should ensure that information entered in CWS/CMS is accurate and authorized before processing APPS payments, and maintain supporting documents. Management should also resolve the over and under payments noted in our review.

Recommendations

DCFS management:

12. **Ensure staff verify that information entered in CWS/CMS is accurate and authorized, and maintain supporting documents for all transactions.**

13. **Resolve the over and under payments noted in our review.**

Standard Payment Rates

Most payments are calculated using the State standard rates stored in APPS. When the State changes the rates, DCFS is notified and should update APPS accordingly.

We noted that APPS rates are updated by one employee, and the updates are not reviewed or approved by management. This significantly increases the risk for error, and over and under payments. As mentioned, these rates are used to calculate most of the $498 million per year in provider payments.

While we did not note any rate errors in the payments we tested, DCFS management needs to review and approve rate updates in APPS before they take effect.

Recommendation

14. **DCFS management review and approve rate updates in APPS.**

Suspended Payments

APPS has controls to suspend and prevent payments with potential errors from being issued, such as payments for care provided over a year earlier, and payments with conflicting information. These are listed on the Suspended Payments Report for staff to investigate and resolve.

We noted that DCFS staff do not always resolve suspended payments timely or accurately. Five (50%) of the ten suspended payments reviewed were unresolved for more than a year. In one case, staff working a suspended payment incorrectly eliminated an overpayment that a provider should have repaid. We also noted that staff failed to keep worked suspense reports, as required by DCFS procedures, and that the procedures do not explain how to resolve all types of suspended payments, and need to be updated.

Recommendations

DCFS management:

15. **Resolve the five suspended payments noted in our review.**

16. **Monitor suspended payments to ensure they are resolved timely and accurately, and retain worked suspense reports.**

17. Update procedures for working suspended payments.

Payee Addresses

As mentioned earlier, some DCFS staff can both change APPS payee information and process foster care payments. This could allow an employee to change a payee's address, and issue a payment to that changed address. We also noted other control weaknesses over APPS payee information that could allow inappropriate payments to occur:

- DCFS does not require supervisory review/approval to update APPS vendor table information, used to mail payments, as required by CFM Section 4.5.10.

- DCFS does not have procedures for updating APPS payees, and staff do not always retain documentation for payee address changes. Specifically, 14 (70%) of 20 payments reviewed were sent to addresses for which DCFS had no documentation. In addition, staff told us they sometimes change payee addresses based on telephone conversations, without adequately verifying the caller's identity.

- The APPS vendor table contains duplicate entries for several providers, because the System does not require a unique identifier, such as a State license or tax identification/social security number. While APPS produces a monthly report of potential duplicate providers, DCFS staff have not reviewed the exceptions in three years. We tested five of the 404 providers on the report, and noted that four (80%) were duplicates and should have been removed from APPS.

Although we did not identify any invalid payments, the weaknesses noted above could allow inappropriate payments to occur. DCFS management should require supervisory approval, and establish uniform procedures, including specific documentation requirements for APPS vendor table updates. Management should also require a unique identifier in APPS to help prevent duplicate vendor table entries, and ensure staff resolve all potential duplicates on the monthly report.

Recommendations

DCFS management:

18. Establish uniform procedures, including supervisory approval and documentation requirements, for APPS vendor table updates.

19. Require a unique identifier in APPS for providers.

20. Ensure staff resolve potential duplicate providers on the APPS report.

System Reports

CFM Sections 8.5.3 and 8.5.4 require that system reports provide needed information to ensure input transactions are processed accurately.

We noted that APPS automatically produces and stores approximately 500 different reports, some multiple times per month, but DCFS management indicated that most of the reports are never used. DCFS management should review APPS reports to determine whether there is a business need for them, and eliminate unneeded reports.

Recommendation

21. DCFS management review APPS reports to determine whether there is a business need for them, and eliminate unneeded reports.

IT Risk Assessment

Board Policy 6.107 requires departments to assess information security risks on critical IT services, as part of the Auditor-Controller's Internal Control Certification Program (ICCP). Departments must certify that proper controls are in place, or that action is being taken to correct any weaknesses or vulnerabilities.

DCFS identified APPS as a critical IT system, so the weaknesses/vulnerabilities noted in our review should have been detected when completing the ICCP. However, DCFS' most recent certification indicates that the appropriate controls were in place and reported no exceptions.

To help DCFS managers evaluate and improve internal controls over APPS, management should ensure staff perform and document an information security risk assessment by properly completing the ICCP.

Recommendation

22. DCFS management ensure staff perform and document an APPS IT risk assessment by properly completing the Internal Control Certification Program.

County of Los Angeles
DEPARTMENT OF CHILDREN AND FAMILY SERVICES
425 Shatto Place, Los Angeles, California 90020
(213) 351-5602

PHILIP L. BROWNING
Director

Board of Supervisors
GLORIA MOLINA
First District
MARK RIDLEY-THOMAS
Second District
ZEV YAROSLAVSKY
Third District
DON KNABE
Fourth District
MICHAEL D. ANTONOVICH
Fifth District

September 19, 2012

TO: Wendy L. Watanabe
Auditor-Controller

FROM: Philip L. Browning
Director

RESPONSE TO AUDITOR-CONTROLLER'S AUTOMATED PROVIDER PAYMENT SYSTEM

Enclosed is the Department of Children and Family Services' response to the recommendations contained in the Auditor-Controller's Review of the Automated Provider Payment System. We agree with the recommendations and have taken corrective action to address and implement all recommendations contained in your report.

If you have any questions or require additional information, please contact Cynthia McCoy-Miller, Administrative Deputy III, Bureau of Finance and Administration, at (213) 351-5847.

PLB:CMM
TF:MH

Enclosure

c: Cynthia McCoy-Miller, Administrative Deputy III
Thomas Fraser, Manager, Internal Controls Section

DEPARTMENT OF CHILDREN AND FAMILY SERVICES

RESPONSE TO AUDITOR-CONTROLLER
AUTOMATED PROVIDER PAYMENT SYSTEM (APPS)
PAYMENT PROCESSING CONTROLS REVIEW

AUDITOR-CONTROLLER RECOMMENDATION #1

Remove unnecessary System access, and ensure access is canceled when employees terminate or change jobs.

DCFS Response:

We agree. Department of Children and Family Services (DCFS) Revenue Enhancement (RE) and Business Information Systems (BIS) staff conducted a joint review of all APPS users, removed users who no longer need access, and strengthened registration and notification processes when the new APPS Web System went "live" on September 26, 2011.

Internal Services Department (ISD) and BIS staff implemented the Single Sign On user authentication solution in the APPS Web System, which will automatically restrict access to any user who is not listed in the ISD Active Directory. Any employee leaving County service is reflected in the County's Electronic Human Resources System (eHR); this system is linked to ISD's Active Directory. The implementation date was August 31, 2012.

BIS staff is currently developing a Management Directive (MD) to ensure APPS user access rights are consistently updated. The policy includes managers' responsibilities for immediately notifying employee job status changes to the DCFS Security Officer and outlines the mandated quarterly review of all APPS users. The target implementation date is October 31, 2012.

BIS and ISD staff will explore options to develop functionality in the APPS Web System that will serve as an automated tracking and notification mechanism as part of the APPS Phase III effort. The proposed upgrade will consist of a daily run of the APPS users against the County's eHR System and the departmental Master Roster System (MRS) to detect users who are promoted, transferred, or moved to another office/unit within the Department and subsequently cancel their user access. The target implementation date is December 31, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #2

Ensure the payment vouchers printed with the terminated employees' IDs were valid.

DCFS Response:

We agree. On August 21, 2012, RE staff completed a review of payment vouchers identified by the Auditor-Controller's (A-C) staff and verified that all of the vouchers are valid.

In addition, BIS staff will use the Single Sign On user authentication solution, in conjunction with the quarterly review of APPS Certified Users, to ensure the timely deactivation of users who no longer have a need for APPS access. The target implementation date is October 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #3

Separate vendor table update and payment processing duties.

DCFS Response:

We agree. Effective January 25, 2011, RE management re-assigned staff to ensure that there is a clear separation of duties between employees who conduct vendor table updates and process payments. In order to corroborate the separation of duties, BIS staff generated a current APPS Certified Users List for the purposes of conducting follow-up and ensuring the access rights and privileges are up-to-date and still applicable to an employee's duties.

BIS staff is currently developing a MD. The directive includes managers' responsibilities for immediately notifying the employee's job status changes to the DCFS Security Officer and outlines the mandated quarterly review of all APPS users to ensure APPS User access rights are consistently updated. The target implementation date is October 31, 2012.

As part of the APPS Phase II effort, in order to facilitate the ongoing assignment shifts directly in the APPS Web System, BIS and ISD staff are working jointly to develop a Security Module that will use role-driven profiles to ensure separation of duties and limit a user's access according to pre-determined roles and responsibilities. The target implementation date is January 31, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #4

Establish policies and procedures to create, limit, and periodically review APPS access roles.

DCFS Response:

We agree. BIS staff is currently developing a MD that outlines registration, approval procedures, and a mandated quarterly review of the APPS Certified Users. The MD will also address managers' reporting responsibilities to ensure user access rights and privileges remain consistent with the employee's roles and responsibilities. The target implementation date is October 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #5

Remove APPS IDs that were created in error.

DCFS Response:

We agree. BIS staff removed the three APPS users that were created in error.

In order to ensure that no duplicate user accounts are created in the APPS Web System, BIS staff will ensure the correct employee ID is entered in the APPS table when a new user account is added to the APPS Web System. If an error is not detected in this stage of the process, the Single Sign On user authentication solution will detect any employee ID discrepancy and will not allow the user to access the APPS Web System until corrective action is taken.

As part of the APPS Phase II Security Module planned activities, BIS and ISD staff are working jointly to add a search and retrieve capability in APPS that is linked directly to ISD's Active Directory. This functionality will eliminate the potential for errors when creating new user accounts since it will no longer require manual data entries and ensure that no duplicate accounts are created in the system. The target implementation date is January 31, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #6

Monitor users with high-level System access.

DCFS Response:

We agree. BIS staff is currently developing a MD that outlines registration, approval procedures, and a mandated quarterly review of the APPS Certified Users. The quarterly review of the APPS Certified Users will entail a comprehensive review of all active users, including users with high level System access. The target implementation date is October 31, 2012.

In addition, as part of the APPS Phase II effort, BIS and ISD staff are working jointly to explore options for adding audit trail functionality to the APPS Web System to capture all user and system generated actions/activities for auditing purposes. BIS staff will report their joint findings and propose a course of action based on research results. The target implementation date is January 31, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #7

Ensure each APPS ID is assigned to a specific individual.

DCFS Response:

We agree. Effective March 2011, BIS staff deactivated all generic user IDs except for four generic accounts that are needed to run critical interface programs. Since the Single Sign On user authentication solution is driven by employee ID, the APPS Web System will not allow the four generic accounts to be used for anything else other than running the specific interface programs. BIS staff is in the process of determining if the interface IDs are still required in the new International Business Machines (IBM) environment. The target implementation date is October 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #8

Document procedures to add, change, and disable users in APPS, and ensure staff obtains written authorization for access assignments.

DCFS Response:

We agree. BIS staff reviewed the APPS Users List to ensure that hard copy registration forms for all active users were in file when the new APPS Web System went "live" on September 26, 2011. Currently, the DCFS Security Officer will only process requests for APPS access when a completed and approved registration form is submitted by the user.

BIS staff is currently developing a Management Directive that outlines registration, approval procedures, and mandated quarterly reviews of the APPS Certified Users. The Management Directive will also address managers' reporting responsibilities to ensure user access rights and privileges remain consistent with the employee's roles and responsibilities. The target implementation date is October 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #9

Limit each user to a single active session, and prevent multiple log-ins.

DCFS Response:

We agree. As part of the APPS Phase II effort, BIS and ISD staff are working jointly to explore options for system functionality that will limit users to a single active session in the APPS Web System. BIS staff will report their joint findings and propose a course of action based on research results. The target implementation date is January 31, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #10

Ensure APPS passwords reset every 90 days, are case-sensitive, and include both alpha and numeric characters.

DCFS Response:

We agree. BIS and ISD staff implemented the Single Sign On user authentication solution in the APPS Web System. With the Single Sign On in place, APPS users are required to reset passwords every 90 days and it enforces strong password naming conventions by only allowing passwords that meet the case-sensitive, alpha and numeric characters criteria. The implementation date was August 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #11

Reset the default password to access APPS reports, and require users to reset the default password on their next login.

DCFS Response:

We agree. BIS and ISD staff are working jointly to implement the Single Sign On user authentication solution to the APPS Reports System. This added system functionality will implement the 90-day password reset

AUDITOR-CONTROLLER RECOMMENDATION #12

Ensure staff verify that information entered in CWS/CMS is accurate and authorized, and maintain supporting documents for all transactions.

DCFS Response:

We agree. DCFS administrative and regional managers will instruct staff to review the existing Procedural Guide E090-0590, Foster Care

Placement/Replacement, to reinforce second-level approval by eligibility supervisors for all ongoing payment requests and reinforce the maintenance of supporting documents in case files. In addition, RE management has established quality assurance reviews that will ensure the integrity of CWS/CMS data by reviewing all new Foster Care placements. The target implementation date is October 31, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #13

Resolve the over and under payments noted in our review.

DCFS Response:

We agree in part. RE staff reviewed the cited cases and determined that one of the reported overpayments was processed with a negotiated special daily rate and is not an overpayment. RE provided the A-C with supporting documentation. However, the other overpayment cited was determined to be a valid overpayment and was resolved. In addition, the identified underpayment was processed with a special out-of-state daily rate and will be resolved. DCFS administrative and regional managers will reinforce existing procedures to ensure that negotiated special daily rate placements are processed using the existing 30.4 daily rate formula. The target implementation date is October 31, 2012.

Additionally, BIS staff reviewed the payment issues cited in the A-C report and concluded that the APPS Web System is working properly as designed.

In addition, in order to detect potential discrepancies, BIS and ISD staff are working jointly to review existing placement updates that go from CWS/CMS to APPS and identify possible areas where an automated alert notification may be useful. This proposed upgrade will provide users with immediate feedback on possible errors at the initial point of data entry. BIS staff will report their joint findings and propose a course of action based on research results. The target implementation date is June 30, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #14

DCFS management review and approve rate updates in APPS.

DCFS Response:

We agree. Effective February 2012, BIS established a formal review and approval process for all table rates by requiring an ISD Service Request and user acceptance sign off before rate changes are implemented in the APPS Web System. This process was initiated upon receipt of a California Department of Social Services' All County Letter (ACL). The ACL provides detailed information concerning rate amount changes, effective dates and affected population(s).

As part of the APPS Phase II effort, BIS and ISD staff are working jointly to develop a Rate Maintenance Module that will facilitate online second level review and approval process to ensure that rates remain consistent with the State-issued ACLs and DCFS policy directives. This module will also include an automated process for calculating and applying approved rate changes. The target implementation date is June 30, 2013.

DCFS currently has established payment cap amounts for ongoing payment requests processed with non-table rates [i.e., Grandfather (GF), Host County (H), Regional Center/Dual Agency FC (RF) and Regional Center/Dual Agency Group Home (RG)]. Since these amounts are entered manually by the users, any payment request that exceeds the payment cap amount is suspended and requires a secondary level review before a disposition is made. As part of the APPS Phase II effort, BIS and ISD staff are working jointly to add online functionality to facilitate the second level review and approval of these suspended payments. The target implementation date is June 30, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #15

Resolve the five suspended payments noted in our review.

DCFS Response:

We agree. RE staff will resolve the five suspended payments noted on the review. The target completion date is September 30, 2012.

AUDITOR-CONTROLLER RECOMMENDATION #16

Monitor suspended payments to ensure they are resolved timely and accurately, and retain worked suspense reports.

DCFS Response:

We agree. As of January 2010, RE management instructed staff to review and resolve the "held" payments listed in the "Cases Suspended on APPS for More Than 30 Days" (DBB30701) report on an ongoing basis and maintain the annotated reports for five years.

AUDITOR-CONTROLLER RECOMMENDATION #17

Update procedures for working suspended payments.

DCFS Response:

We agree. RE management will revise Procedural Guide E080-0520, Address Change, which includes guidelines for working suspended payments due to

address changes. RE management will also revise procedures to ensure cases suspended for more than 30 days in the APPS Web System are researched and resolved. The target implementation date is December 31, 2012.

As part of the Phase II effort, BIS and ISD staff are working jointly to add front-end functionality to the APPS Web System so that authorized users will be able to identify and release payments directly online. The planned system upgrade will require a second level approval. The target implementation date is June 30, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #18

Establish uniform procedures, including supervisory approval and documentation requirements, for APPS vendor table updates.

DCFS Response:

We agree. RE management will develop a procedural guide to establish uniform procedures for reviewing and approving vendor name and address changes. These procedures will strengthen the existing vendor verification process in the APPS Web System. The target implementation date is December 31, 2012.

As part of the APPS Phase II effort, BIS and ISD staff are working jointly to explore options to automate vendor updates directly from CWS/CMS to the APPS Web System. BIS will report their joint findings and propose a course of action based on research results. The target implementation date is December 31, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #19

Assign each provider a unique identifier in APPS.

DCFS Response:

We agree in part. As a standard practice, vendors are assigned a unique vendor number in APPS. For legal purposes, DCFS has an ongoing business need to make exceptions to this rule. However, multiple vendor number requests undergo an established review and approval process to ensure that the specified legal requirements are met.

In order to avoid duplication due to user error, BIS staff will enhance existing client and vendor name search functionality in the APPS Web System as part of the APPS Phase II effort. The target implementation date is January 31, 2013.

AUDITOR-CONTROLLER RECOMMENDATION #20

Ensure staff resolve potential duplicate providers on the APPS report.

DCFS Response:

We agree. As of May 2010, RE management instructed Resource Management Unit staff to review the "Monthly Duplicate Vendor" report on a monthly basis to research and resolve any duplicate providers identified in the report. As indicated in the response for Recommendation 19, DCFS has an ongoing business need to issue duplicate vendor numbers to providers who reside in the same household. As such, it may appear that these providers are duplicate records. In these instances, where a duplicate record is valid, DCFS maintains supporting documentation to substantiate the issuance of multiple records.

AUDITOR-CONTROLLER RECOMMENDATION #21

DCFS management review APPS reports to determine whether there is a business need for them, and remove unneeded reports.

DCFS Response:

We agree. Upon the implementation of the APPS Web System in September 2011, RE and Fiscal management reviewed all APPS reports and determined that 353 reports were obsolete and removed them from the APPS Report System. Staff is currently utilizing the remaining reports on an ongoing basis.

AUDITOR-CONTROLLER RECOMMENDATION #22

DCFS management ensure staff perform and document an APPS IT risk assessment by properly completing the Internal Control Certification Program.

DCFS Response:

We agree. BIS management completed the FY 2010-2011 APPS Internal Control Certification Program, identified 12 weaknesses, and submitted the Summary of Internal Control Weaknesses and Improvement Plans form. The implementation date was January 31, 2011.