

**COLORADO DEPARTMENT
OF
HUMAN SERVICES
COUNTY FINANCIAL
MANAGEMENT SYSTEM**

JUNE 2000

Members of the Legislative Audit Committee:

This report contains the results of the agreed-upon procedures performed on the County Financial Management System at the Colorado Department of Human Services. This audit was conducted pursuant to Section 23-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government.

This report presents our findings, conclusions and recommendations, and the responses of the Colorado Department of Human Services.

KPMG LLP

August 2, 2000

**LEGISLATIVE AUDIT COMMITTEE
2000 MEMBERS**

Representative Jack Taylor
Chairman

Representative Carl Miller
Vice-Chairman

Senator Norma Anderson
Senator Doug Lamborn
Senator Doug Linkhart
Senator Peggy Reeves
Representative Sue Windels
Representative Brad Young

Office of the State Auditor Staff

J. David Barba
State Auditor

Joanne Hill
Deputy State Auditor

Brenda Berlin
Contract Monitor

KPMG LLP Staff

Edwin E. Holt
Partner

Cody Daniels
Senior Manager

Michael Sultan
Senior Consultant

Charles Epp
Senior Consultant

Colorado Department of Human Services County Financial Management System

Table of Contents

	Page
Report Summary	1
Recommendation Locator	5
Organization and Functions of the Colorado Department of Human Services	6
Auditors' Findings and Recommendations and Colorado Department of Human Services' Responses	11
Appendix I – Agreed-Upon Procedures Report	22
Distribution Page	29

Colorado Department of Human Services County Financial Management System

Report Summary

Authority, Standards, Purpose and Scope

The procedures performed on the Colorado Department of Human Services (CDHS or Department) County Financial Management System (CFMS) were conducted under the authority of Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct performance audits of all departments, institutions and agencies of state government. The Agreed-Upon Procedures Report was prepared under Statement on Standards for Attestation Engagements (SSAE 4), *Agreed-Upon Procedures Engagements*, and can be found in Appendix I of this document. This report was prepared in connection with the Agreed-Upon Procedures and reflects comments, findings and recommendations noted during performance of the agreed-upon procedures.

Our procedures included obtaining CDHS's documented policies and procedures related to the input, processing and output of data in CFMS and policies and procedures related to application change management and security administration over CFMS. We compared the documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented. In addition, we tested several items related to CFMS transactions, application change management and security administration to determine compliance with documented policies and procedures. Our procedures were performed solely to assist the State Auditor in evaluating the effectiveness of certain controls surrounding CFMS. We make no representations regarding the sufficiency of the procedures either for the purpose for which the Agreed-Upon Procedures Report has been requested or for any other purpose.

This report contains nine recommendations for improving the internal controls related to the input, processing and output of information in CFMS and internal controls related to application change management and security administration over CFMS. We would like to acknowledge the efforts and assistance extended by staff at the Colorado Department of Human Services and the Colorado counties who use CFMS. The following summary provides highlights of the comments, findings and recommendations contained in the report.

Summary of Major Comments

The County Financial Management System serves as the Department's data repository, accumulating all benefit and benefit-related data from the legacy systems, County Employee Data Store (CEDS) and the county systems. CFMS is used to account for approximately \$750 million dollars annually in benefit and benefit-related expenditures. The CFMS general ledger houses fiscal and financial data for most of the public assistance programs administered within CDHS.

CFMS, an Oracle application and database, includes the following modules: General Ledger, Purchasing, Accounts Payable and Accounts Receivable. Additionally, several benefit legacy systems interface with CFMS. The legacy systems function as the original source of entry for benefit data, facilitating eligibility and authorization for public assistance program service and benefits. Once entered and processed at the county level, data from the legacy systems is uploaded to CFMS through an open interface.

Policies and Procedures

We noted areas of CFMS where CDHS does not have formal policies and procedures, has incomplete or limited policies and procedures or does not consistently follow policies and procedures. Policies and procedures are critical in establishing an infrastructure for a sound internal control environment. In the absence of formally documented policies and procedures, clear guidance on acceptable practices is not in place to evaluate current activities.

We recommend CDHS ensure all CFMS functional areas have adequate formalized documented policies and procedures; policies and procedures should contain sufficient information to enable personnel to understand, control and operate CFMS. CDHS should perform a comprehensive review of existing policies and procedures; where deemed inadequate, new formal policies and procedures should be developed and implemented. Further, CDHS should review policies and procedures periodically to ensure they are current in light of prevailing business practices. Finally, CDHS should establish a process to monitor compliance with policies and procedures.

Change Management and Database Administration

Our procedures included testing of the process used to make modifications to the CFMS application (application change management) and administration of the CFMS database. These functions are administered by an outside technology services company, DynCorp.

Regarding application change management and database administration, we noted findings in the following areas:

- Database Access
- Application Change Management
- Database Administration Policies and Procedures
- UNIX Administration
- Use of Audit Capabilities Surrounding the Oracle Database

These findings are further detailed below.

Database Access

We noted several instances where access to the CFMS database was unauthorized or inappropriate. Unauthorized or inappropriate access to the database increases the risk that changes will be made that compromise the integrity of the information contained in the database.

We recommend CDHS require DynCorp (the technology services outsourcing company) to review the current database access structure to ensure that appropriate segregation of duties exists in order to exclude the possibility for a single individual to subvert a critical process. In addition, we recommend the Department establish procedures that require appropriate authorization of logical access to sensitive or critical information. We further recommend as part of a formalized database administration security policy, that CDHS change database passwords periodically. These control procedures help reduce the risk that users are granted unauthorized access or access that is incompatible or inappropriate for their job responsibilities.

Application Change Management

The current outsourcing arrangement between CDHS and DynCorp does not specify responsibility for application change management, although DynCorp is performing the application change management function. In addition, we noted several instances where the policies and procedures related to application change management were not followed on a consistent basis. Strict definition of, responsibility for and adherence to application change management policies and procedures help to reduce the risk of unauthorized or unintended changes to the CFMS application, database or operating system.

We recommend the Department consider a modification of its service-level agreement with DynCorp to include responsibilities regarding application change management. The responsibility and adherence to stated policies should be definitively and specifically assigned in the agreement. We recommend the Department address this issue before the next contract extension.

Additionally, we recommend CDHS require DynCorp to strengthen adherence to its application change management policies and procedures to reduce the risk of unauthorized or unintended changes to the CFMS application, database or operating system.

Database Administration Policies and Procedures

We noted CDHS does not have policies and procedures governing database administration and security. Policies and procedures are critical in establishing an infrastructure of control. In the absence of formally documented policies and procedures, clear guidance on acceptable practices for which to evaluate current activities has not been established.

We recommend CDHS work with DynCorp to develop and/or formalize policies and procedures for all functional areas relevant to the administration of the CFMS database. Procedure manuals should contain sufficient information to enable personnel to understand, control and operate CFMS.

UNIX Administration

We noted CDHS does not have a designated CFMS UNIX administrator position, and has not since the inception of CFMS. UNIX is the operating system used to control CFMS workstations and servers. The UNIX administrator is responsible for overseeing all functions related to UNIX. The role of the UNIX administrator is paramount to helping ensure the effective control and efficiency of the CFMS operating system.

We recommend CDHS designate a UNIX administration position and fill the position appropriately, either in-house or through the outsourcing arrangement with DynCorp. It is likely this position would be outsourced to DynCorp based on the nature of the services provided by DynCorp. We recommend the Department designate a UNIX administration role and, if appropriate, include the position in the service-level agreement between CDHS and DynCorp. The service-level agreement should specify the role and responsibilities of the UNIX administrator and should include appropriate funding of the position in the fees paid to DynCorp.

Use of Audit Capabilities Surrounding the Oracle Database

We noted CDHS is not currently utilizing Oracle audit functionality, AuditTrail®. Sound security policies and procedures should include a formal and executed plan to monitor database access. In the absence of appropriate monitoring, unauthorized or unintentional changes to the database may go undetected. As

AuditTrail® is currently installed, in order to facilitate the audit functionality, the Department need only modify the current database settings.

We recommend CDHS consider utilizing AuditTrail®, an Oracle functionality that provides a tracking mechanism for changes made directly to the CFMS database. Changes made directly to the CFMS database are not subject to application-level audit trails that capture change information for routine transaction flows. Additional functionality, such as that provided by AuditTrail®, is necessary to capture complete information regarding database changes.

The audit functionality can be used selectively for defined tables, or sets of information. Database tables that hold critical data or which should be selectively or infrequently modified should be considered for audit tracking. Because the use of this function will impact system performance, management should use this function on a selective basis.

Application User Access Security

We noted several instances where user access to the CFMS application was unauthorized or inappropriate. Unauthorized or inappropriate access to the CFMS application increases the risk that changes will be made that compromise the integrity of the information in the CFMS application.

We recommend CDHS strengthen adherence to user access setup policies and procedures, eliminate all generic user IDs with published passwords and review user access periodically for appropriateness and to verify that generic IDs are not in existence. These recommendations will help reduce the risk of unauthorized access, as well as the risk of access granted to a user that is inconsistent, inadequate or improper for that user's specific job responsibilities and to maintain accountability for CFMS access.

Segregation of Duties

We noted at both the Department and counties that personnel perform conflicting functions. Duties should be segregated to reduce the risk of fraud or abuse. We noted several positions related to CFMS input, processing and output that had recently become vacant or had remained unfilled for several months. It is our understanding that, in order to maintain certain processes, the Department and counties used existing personnel to perform functions normally assigned to the vacant positions.

We recommend CDHS perform a periodic review of all open positions within the Department with CFMS responsibilities to ensure all critical duties are performed in a timely manner while maintaining an appropriate segregation of duties. In addition, all positions should have a designated substitute to ensure that critical duties are performed as necessary during an employee absence. Designated substitute or back-up personnel should be employees who do not perform conflicting functions.

As it relates to open positions at the county level, although county management is responsible maintaining an effective internal control environment within the county, the Department is responsible for promoting the effective administration of the programs it supports. These responsibilities extend to the use of CFMS for the input, processing and output of data as well as compliance with user access security over CFMS. We recommend the Department make the county aware of the instances noted at the county where segregation of duties was compromised and help ensure that the situation has been adequately resolved.

A summary of the Department's responses to the above comments can be found in the Recommendation Locator that follows.

Recommendation Locator

Recommendation No.	Page No.	Recommendation Summary	Agency Addressed	Agency Response	Implementation Date
1	12	Develop, formalize and monitor policies and procedures related to data input, processing and output.	Department of Human Services	Agree	December 31, 2000
2	14	Review current database access structure and establish procedures that require appropriate authorization of logical access.	Department of Human Services	Agree	December 31, 2000
3	15	Modify agreement with DynCorp to include responsibility for application change management.	Department of Human Services	Agree	December 31, 2000
4	16	Require DynCorp to strengthen adherence to application change management policies and procedures.	Department of Human Services	Agree	December 31, 2000
5	16	Develop, formalize and monitor policies and procedures related to database administration.	Department of Human Services	Agree	June 30, 2001
6	17	Provide for a UNIX administrator.	Department of Human Services	Agree	September 1, 2000
7	18	Consider utilization of database audit functionality.	Department of Human Services	Agree	October 31, 2000
8	19	Strengthen adherence to application user access security policies.	Department of Human Services	Agree	December 31, 2000
9	21	Review positions and responsibilities to ensure that segregation of duties is maintained.	Department of Human Services	Agree	September 30, 2000

Organization and Functions of the Colorado Department of Human Services

State law created the Colorado Department of Human Services on July 1, 1994, to manage, administer, oversee and deliver human services in Colorado. The law combines the former Departments of Social Services and Institutions with the Alcohol and Drug Abuse Division from the Department of Health. Today, CDHS consists of slightly more than 7,500 county and state employees. It provides services through 63 county or district departments of social services, 2 state mental health institutes, 10 youth corrections facilities, 5 nursing homes, 28 vocational rehabilitation offices, 3 regional centers for persons with developmental disabilities and numerous community-based public and private providers. In addition, CDHS contracts with several agencies such as community mental health centers, area agencies on aging and community centered boards to provide human services. CDHS also administers and provides oversight for a variety of federally funded programs.

The County Financial Management System Project

The County Financial Management System serves as the Department's data repository, accumulating all benefit-related data from the legacy systems, County Employee Data Store (CEDS) and the county systems. CFMS is used to account for approximately \$750 million dollars annually in benefit and benefit-related expenditures.

CFMS is an Oracle application and database that was implemented in July 1999. The application currently includes the following Oracle modules: General Ledger, Purchasing, Accounts Payable and Accounts Receivable. In addition, a payroll module, County Employee Data Store, has been modified to simulate an Oracle application.

Several benefit legacy systems interface with CFMS. They are:

- Client Oriented Information Network (COIN)
- Colorado Automated Food Stamp System (CAFSS)
- Colorado Welfare Eligibility and Service Tracking (CWEST)
- Low Income Energy Assistance Program (LEAP)
- Child Health Automated Tracking System (CHATS)
- COIN Accounts Receivable System (CARS)
- Automated Claims Tracking System (ACTS)
- Automated Child Support Enforcement System (ACSES)

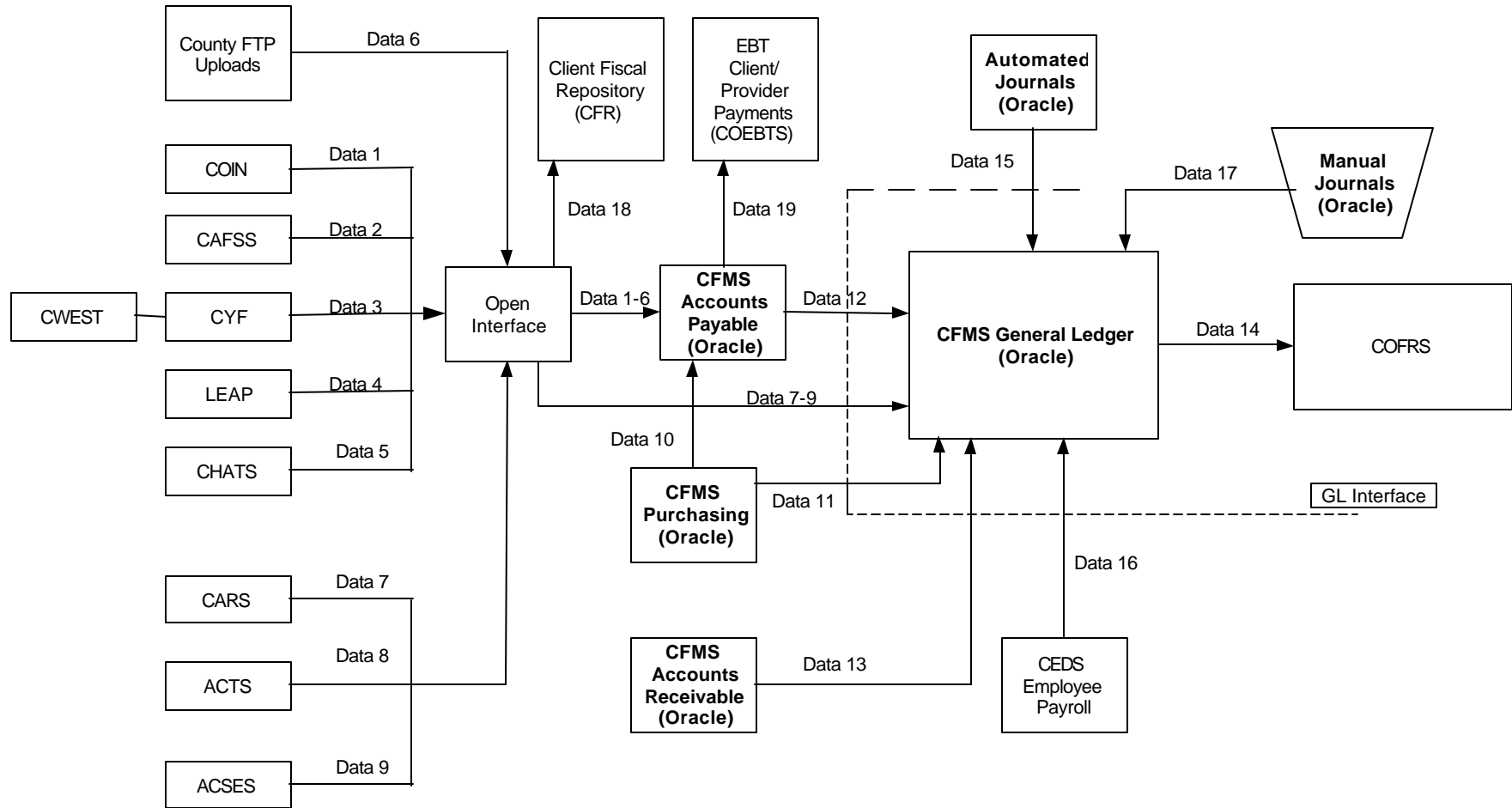
The benefit legacy systems function as the original source of entry for benefit data, facilitating eligibility and authorization for public assistance program service and benefits. Once entered and processed at the county level, data from the legacy systems is uploaded to CFMS through an open interface. It is at this point that data is considered "input" to CFMS and is further processed by CFMS and included in CFMS output. The CFMS general ledger houses all fiscal and financial data for all public assistance programs administered within CDHS. Information from the CFMS general ledger is ultimately downloaded to the Colorado Financial Reporting System (COFRS) for state and federal reporting.

CFMS was originally designed to provide the Department a fully functional county fiscal management system and to eliminate the use of the Automated Personnel Payroll System-Administrative Cost System (APPLS-ACS) and the Colorado Automated Payment System (CAPS). The Department recognized the need for CFMS to help formalize information that was previously vested in few individuals, to consolidate and reduce workloads to prevent loss of information and to provide a system that adequately supported the mission of the Department. The primary objectives of CFMS are to:

- interface with existing legacy benefit systems;
- interface with future benefit systems (currently under development);
- automate interfaces between systems;
- reduce duplicate entry where possible;
- provide more timely information.

A graphical depiction of CFMS and related legacy systems is shown on the following page.

CFMS Business Process Flow



See the following page for description of systems.

CFMS Business Process Flow – Explanation of Data Elements

- Data 1 (COIN) – Financial flow for Client Oriented Information Network, used for the set up and maintenance of Medicaid/public assistance financial benefit eligibility.
- Data 2 (CAFSS) – Financial flow for Colorado Automated Food Stamp System, used for set up and maintenance of food stamp financial benefit eligibility.
- Data 3 (CWEST) – Financial flow for Colorado Welfare Eligibility and Service Tracking, used for set up and maintenance of welfare financial eligibility. This data transmits via an account code translation through the Child Youth Family system currently, but originates within the CWEST system. The CYF application will replace CWEST.
- Data 4 (LEAP) – Financial flow for Low Income Energy Assistance Program, used for set up and maintenance of low-income client heating assistance eligibility.
- Data 5 (CHATS) – Financial flow for Child Health Automated Tracking System, used for set up and maintenance of childcare financial eligibility.
- Data 6 – Eight counties currently upload data via FTP files into CFMS directly. These counties include Adams, Arapahoe, Boulder, El Paso, Jefferson, Larimer, Mesa and Pueblo.
- Data 7 (CARS) – Financial flow for COIN Accounts Receivable System, used for the maintenance / tracking / collection of overpayments and other adjustments associated with COIN.
- Data 8 (ACTS) – Financial flow for Automated Claims Tracking System, used for maintenance / tracking / collection of overpayments and other adjustments associated with CAFSS.
- Data 9 (ACSES) – Financial flow Automated Child Support Enforcement System, used for set up and management of child support collections.
- Data 10 – Financial flow related to purchase order encumbrances for government vendor and contract purchasing. We noted that the PO module is currently used for a single type of child welfare program, IV-D, County Administrative and County Service Contracts.
- Data 11 – Financial flow related to purchase order encumbrances for government vendor and contract purchasing.
- Data 12 – Financial flow related to client / provider and related expenses / payments, as well as encumbrance liquidation.
- Data 13 – Financial flow related to miscellaneous provider and administrative receipts.
- Data 14 – Financial flow of General Ledger journals to Colorado Financial Reporting System, used for reporting to the state of Colorado.
- Data 15 – Manual journals directly entered into CFMS General Ledger, including allocations, budgets, share calculations, recurring journals and settlements.
- Data 16 – Financial flow related to employee payroll.
- Data 17 – Manual journals directly entered into CFMS General Ledger, including allocations, budgets, share calculations, recurring journals and settlements.
- Data 18 – Financial data flow for benefit transactions and related information to the CFR, functioning as a data warehouse.
- Data 19 – Financial data flow for benefit transactions and related information to the COEBTS, for further processing to Citibank for payment.
- GL Interface – Any automated data feeds are imported first into a General Ledger Interface table, initiating a data import validation routine, and upon completion, data is input to the General Ledger.

This page intentionally left blank.

CFMS is used primarily to accumulate benefit and benefit-related expenditure data from the counties. However, the majority of counties have little direct use of CFMS. As noted previously, the benefit-related input at the county level is achieved through legacy systems. In addition, most counties have their own independent systems to perform other common functions such as general ledger, purchasing, accounts payable and accounts receivable. Information from these independent systems is downloaded or manually re-keyed to CFMS. The independent county systems are not depicted in the preceding graphic.

The Department is currently developing two new benefit systems, Colorado Benefits Management System (CBMS) and Colorado Youth and Families system (CYF). CYF is currently used on a limited basis as a pass-through for information from the CWEST system acting as an interface to CFMS. The Department plans for these systems to replace the legacy benefit systems currently in use (COIN, CAFSS, CWEST, LEAP, CHATS, CARS and ACTS). As noted above, they will provide the source of original entry for benefits transactions and will interface with CFMS.

Auditors' Findings and Recommendations and Colorado Department of Human Services' Responses

Policies and Procedures

Background

Policies and procedures are critical in establishing an infrastructure for a sound internal control environment. In the absence of formally documented policies and procedures, clear guidance on acceptable practices is not in place to evaluate current activities. Procedure manuals should contain sufficient information to enable personnel to understand, control and operate CFMS.

Our procedures included obtaining CDHS's documented policies and procedures related to the input, processing and output of data from CFMS and policies and procedures related to application change management and security administration over CFMS. We compared the documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented. In addition, we tested several items related to CFMS transactions, application change management and security administration to determine compliance with documented policies.

Findings

We noted CDHS does not have formal policies and procedures in the following areas related to CFMS:

- **Authorization to access output** – One of the primary goals of CFMS is to make more information available to users in a more timely manner in the form of on-line inquiries and ad-hoc reports. With the increase in the amount of information provided by CFMS comes the responsibility to develop policies and procedures to effectively manage the accessibility of this information. We noted policies and procedures related to output accessibility authorization for CFMS and the Client Fiscal Repository (CFR) have not been formally documented.
- **Reconciliation of CEDS (County Employee Data Store) / county payroll output** – Reconciliation of data between source documents/systems and reporting systems is a primary control used to ensure that all data has been processed completely and accurately. While policies and procedures exist related to reconciliation of output in all other transaction flows related to CFMS, CDHS does not have policies and procedures related to the reconciliation of CEDS output.

In addition, we noted CDHS has incomplete or limited policies and procedures in the following area related to CFMS:

- **Input completeness and accuracy for transactions input through the open interface (benefit transactions), CEDS transactions and State journal entries** – The policies and procedures related to the input of transactions to CFMS do not address procedures to ensure the completeness and accuracy of the transaction input. Current policies and procedures do not describe the individuals responsible for the verification of completeness and accuracy nor do they address the specific procedures and reports used to perform this function.

Finally, we noted CDHS does not consistently follow policies and procedures in the following areas related to CFMS:

- **County input authorization** – Input authorization policies and procedures exist at the county level but we noted they are not consistently followed. During the course of our procedures, we noted the two invoices selected for test work at the county level did not contain the appropriate authorization prior to input to CFMS as required by documented policies and procedures.
- **Input error correction for transactions input through the open interface (benefit transactions)** – Input error correction policies and procedures are not followed on a consistent basis. During the course of our procedures, we noted journal vouchers were not processed to move three of the four transactions from the default error correction account to the correct general ledger account as required by documented policies and procedures.
- **Accuracy and completeness of output for transactions input through the open interface (benefit transactions)** – Output accuracy and completeness policies and procedures for the open interface exist but we noted they are not followed consistently. During the course of our procedures, we noted monthly reconciliation of the open interface transactions to the general ledger was not performed in a timely manner as required by documented policies and procedures. We noted that although the reconciliation has been completed through April 2000, the reconciliation process was just recently performed in aggregate for the period of July 1999 through April 2000. The transactions for that period represented approximately \$357 million of benefit and benefit-related expenditures.

Recommendation No. 1

We recommend the following:

- Develop and/or formalize policies and procedures for all CFMS functional areas; policies and procedures should contain sufficient information to enable personnel to understand, control and operate CFMS.
- Perform a comprehensive review of existing policies and procedures; where deemed inadequate, new formal policies and procedures should be developed and implemented.
- Perform periodic review of policies and procedures to ensure they are current in light of prevailing business practices.
- Establish a process to monitor compliance with policies and procedures.

Colorado Department of Human Services' Response

Agree. Formal, current comprehensive policies and procedures will be completed for all CFMS functional areas. In addition, a process will be established whereby compliance with policies and procedures is monitored on a periodic basis. A staff member will be assigned to this project in September with anticipated completion by December 31, 2000.

Change Management and Database Administration

Background

CDHS has contracted with DynCorp, a technology services company, to provide database administration support and related services, including maintenance of the operating system and any changes associated with the CFMS applications, database and operating system. These services are collectively referred to as Database Administration and Application Change Management. The service contract between the Department and DynCorp commenced in November 1998. The contract has a provision for four one-year renewal options, potentially extending these services through December 2004.

DynCorp's responsibility related to database administration covers the physical design and management of the database. It also includes the evaluation, selection and implementation of the Database Management System (DBMS). DBMS is software that controls the organization, storage, retrieval, security and integrity of data in a database. It accepts requests from the application and instructs the operating system to transfer the appropriate data. DBMS lets information systems be changed more easily as the organization's requirements change. New categories of data can be added to the database without disruption to the existing system. The major features of a DBMS include:

- 1) *Data Security* – The DBMS can prevent unauthorized users from viewing or updating the database.
- 2) *Data Integrity* – The DBMS can ensure that no more than one user can update the same record at the same time and ensures that the database does not keep duplicate records.
- 3) *Interactive Query* – Most DBMS provide query languages and report writers that let users interactively interrogate the database and analyze its data. This important feature provides management with the ability to grant users access to information, as needed.
- 4) *Data Independence* – With a DBMS, the details of the data structure are not stated in each application program. The program asks the DBMS for data by field name, but without a DBMS, a programmer must reserve space for the full structure of the record in the program. Any change in data structure would require changing all application programs.

Another primary area of responsibility of DynCorp is administration of the change management process for the applications, operating system and database. Change management, in general, encompasses the process of identifying, reviewing, approving, categorizing, prioritizing and executing changes to the CFMS environment. The execution of approved change requests should be done in a manner that effectively prevents or significantly reduces the risk that unauthorized or unintentional changes are made to the CFMS environment. This is particularly critical for CDHS, an organization responsible for the timely disbursement of a high volume of welfare and related Human Services commitments. Best practices dictate that the change management process is administered through the use of dedicated version control software.

Included in our procedures were the review and testing of application change management and database administration, two of the areas administered by DynCorp. Adequate controls surrounding application change management reduce the risk of unintentional or unapproved modifications of systems and data, potentially causing a system to be unavailable for its intended purpose. Adequate database administration provides the efficient and effective performance of the associated user applications and operating system.

Regarding application change management and database administration, we noted findings in the following areas:

- Database Access
- Application Change Management
- Database Administration Policies and Procedures
- UNIX Administration
- Use of Audit Capabilities Surrounding the Oracle Database

Complete descriptions of the findings in these areas, our recommendations and CDHS's responses are detailed below.

Database Access

Findings

We noted the following related to unauthorized database access:

- DynCorp programmers/developers have access to the CFMS production environment. Because programmers/developers can effectively change the way an application processes data, best practices dictate that programmers/developers have access only to a test environment, not the production environment where data integrity can be compromised.
- Two CDHS employees have database level access that was not supported by an approved access setup form.
- Database passwords are not changed on a routine basis. Best practices dictate that database passwords be changed at least every 30 days.
- Three UNIX user ID's contain passwords that had not been changed since CFMS went into production in July 1999. Best practices dictate that UNIX passwords be changed at least every 30 days.

The database contains information that is deemed critical or sensitive in nature, including master files of vendors, benefit recipient data and payroll records. Due to the sensitive nature of the information, access to the database should be closely controlled and monitored. Inadequate security control increases the risk of users with access and capabilities not compatible with their job responsibilities, inappropriate access to information resources, compromised data integrity and unauthorized modification of data or programs.

Recommendation No. 2

We recommend CDHS require DynCorp to review the current database access structure to ensure that appropriate segregation of duties exists in order to exclude the possibility for a single individual to subvert a critical process. In addition, we recommend the Department establish procedures that require appropriate authorization of logical access requests to sensitive or critical information. We further recommend as part of a formalized database administration security policy, that CDHS change database passwords periodically to provide additional access control. These control procedures help reduce the risk that users are granted unauthorized access or access that is incompatible or inappropriate for their job responsibilities.

Colorado Department of Human Services' Response

Agree. CDHS will establish a security plan that ensures adequate segregation of duties in order to exclude the possibility for a single individual to subvert a critical process. Procedures will be established that require password changes every 90 days. The security plan will be developed by October 31, 2000 and implemented by December 31, 2000.

Application Change Management

Findings

We noted the following related to application change management:

- The current outsourcing arrangement between CDHS and DynCorp does not specify responsibility for application change management, although DynCorp is performing the application change management function.
- Of 15 application change requests selected for testing, 7 of the 15 did not have documentation, and another 7 of the 15 had incomplete documentation. Required documentation as stated in CDHS policies and procedures includes change request approval, evidence of successful testing, approved request to migrate change to production and evidence of successful migration to production.
- CDHS's application change management policies and procedures indicate that version control software is used for the tracking of application and related changes resulting from approved change requests. Currently, DynCorp is not using version control software.

Change management performed at the application, database and operating system level should be tightly monitored and controlled and should be definitively and specifically assigned. Appropriate change management policies and procedures help reduce the risk of unauthorized or unintentional modification of systems and data, helping to ensure continuity of operations as well as data integrity and accuracy. An effective application change management process helps to ensure that all changes are intentional, authorized and controlled. A major component of an effective application change management process is version control software, which is designed to track, monitor and control configuration baseline integrity and establish an infrastructure for programmed access authorization controls over the change management system.

Recommendation No. 3

We recommend the Department consider a modification of its service-level agreement with DynCorp to include responsibilities regarding application change management. The responsibility and adherence to stated policies should be definitively and specifically assigned in the agreement. We recommend the Department address this issue before the next contract extension.

Colorado Department of Human Services' Response

Agree. The very aggressive project implementation schedule which was required did not allow for a pilot stage. As a result, during the several month period subsequent to implementation, numerous discoveries were made which resulted in a frenetic pace of analysis, development, testing and placing new reports and edits into the production system. While formal documentation of changes has been lacking, the control over the system has been strengthened. Change management software has been procured and a formal change management system will be in place within approximately six months. However, centralized

approval for change management was established during January/February 2000, and no production change is allowed without written approval from the project manager. Discussion with DynCorp regarding the administration of the system has already taken place and this will be a topic for contract clarification at the December 31st renewal deadline. Ultimate authority over change management will reside with CFMS project management and enforcement of the methodology will be the responsibility of DynCorp staff.

Recommendation No. 4

Additionally, we recommend CDHS require DynCorp to strengthen adherence to its application change management policies and procedures to reduce the risk of unauthorized or unintended changes to the CFMS application, database or operating system.

Colorado Department of Human Services' Response

Agree. This recommendation follows naturally and is addressed in our response to recommendation number 3.

Database Administration Policies and Procedures

Findings

We noted CDHS does not have policies and procedures governing database administration and security. Policies and procedures are critical in establishing an infrastructure of control. In the absence of formally documented policies and procedures, clear guidance on acceptable practices for which to evaluate current activities has not been established.

The ongoing presence and function of a formally defined process of database administration and related change management, with clear assignment of these responsibilities, ensures the continuing operation of CFMS and ensures that all system changes are intentional and authorized. Defined and assigned responsibilities reduces the risk of unintentional system modification and risk of unscheduled system unavailability.

Recommendation No. 5

We recommend CDHS work with DynCorp to develop and/or formalize policies and procedures for all functional areas relevant to the administration of the CFMS database. Procedure manuals should contain sufficient information to enable personnel to understand, control and operate CFMS.

Colorado Department of Human Services' Response

Agree. CDHS is in the process of developing departmental standards for database administration at the present time. Once those standards are finalized, database administration of CFMS will conform to them. In the interim, prudent practice coupled with invocation of automated scheduling software (underway) is in place. These standards will be completed and adopted by June 30, 2001.

UNIX Administration

Findings

We noted CDHS does not have a designated CFMS UNIX administrator position, and has not since the inception of CFMS. UNIX is the operating system used to control CFMS workstations and servers. The UNIX administrator is responsible for overseeing all functions related to UNIX. The role of the UNIX administrator is paramount to helping ensure the effective control and efficiency of the CFMS operating system.

UNIX is a multi-user, multi-tasking operating system that is widely used as a control program in workstations and servers. It's generally known for a variety of versions, as compared to other operating systems. The UNIX operating system is a critical component to the effective operation of CFMS. The UNIX administrator oversees and maintains the operating system, installs patches, monitors system performance, analyzes trends that can significantly affect system performance and provides feedback to continued effective operation. Properly defined and executed UNIX system administration reduces the risk of inadequate tracking and maintenance of CFMS. Additionally, it reduces the risk of unscheduled system unavailability.

Recommendation No. 6

We recommend CDHS designate a UNIX administration position and fill the position appropriately, either in-house or through the outsourcing arrangement with DynCorp. It is likely this position would be outsourced to DynCorp based on the nature of the services provided by DynCorp. We recommend the Department designate a UNIX administration role and, if appropriate, include the position in the service-level agreement between CDHS and DynCorp. The service-level agreement should specify the role and responsibilities of the UNIX administrator and should include appropriate funding of the position in the fees paid to DynCorp.

Colorado Department of Human Services' Response

Agree. The Department requested funding for a full time UNIX administrator as of FY 00-01 decision item. The funding was approved but at a drastically reduced level so as to allow only a few hours of UNIX administration per month. As of September 1, 2000, the Department has used the available funding and leveraged existing departmental resources to perform the duties critical to this function. The Department will continue to request funding for a full time UNIX administrator for future fiscal years.

Use of Audit Capabilities Surrounding the Oracle Database

Findings

We noted CDHS is not currently utilizing Oracle audit functionality, AuditTrail®. Sound security policies and procedures should include a formal and executed plan to monitor database access. In the absence of appropriate monitoring, unauthorized or unintentional changes to the database may go undetected. As AuditTrail® is currently installed, in order to facilitate the audit functionality, the Department need only modify the current database settings.

Recommendation No. 7

We recommend CDHS consider utilizing AuditTrail®, an Oracle functionality that provides a tracking mechanism for changes made directly to the CFMS database. Changes made directly to the CFMS database are not subject to application-level audit trails that capture change information for routine transaction flows. Additional functionality, such as that provided by AuditTrail®, is necessary to capture complete information regarding database changes.

The audit functionality can be used selectively for defined tables, or sets of information. Database tables that hold critical data or which should be selectively or infrequently modified should be considered for audit tracking. Because the use of this function will impact system performance, management should use this function on a selective basis.

Colorado Department of Human Services' Response

Agree. Generally, the audit function maintains a transactional level record of all database activity. As a result there can be considerable overhead in terms of processor time and/or disk storage space which can degrade end user performance. The Department has requested that an analysis of the potential performance cost and disk overhead be performed and that this be done in relation to the projected system load in comparison to original capacity requirement estimates. The CFMS executive management team will be presented with the result and will make a policy determination related to the full or partial utilization in comparison to the potential risks of not utilizing the audit feature. The cost benefit analysis will be completed by October 31, 2000.

Application User Access Security

Background

CDHS has designated a single security administrator through which all CFMS application access requests are to be processed. CDHS submits application access requests through the CDHS Help Desk. The Application Information Access form includes a listing of the required access responsibilities as well as a signature from that individual's supervisor or manager, indicating approval of the requested access responsibilities. The form has pre-listed the more commonly used access responsibilities, while higher access responsibilities that are less commonly granted must be manually noted on the form. Employee job changes, terminations and related modifications are also to be administered through the Help Desk using the same procedure.

Security at any level of a computer system has many facets. The application level of a system is of critical importance as the majority of users and data input is typically done at this level. Facets of security include the following:

- 1) Secrecy and confidentiality – Data should not be disclosed to anyone not authorized to access it.
- 2) Accuracy, integrity and authenticity – Accuracy and integrity mean data cannot be maliciously or accidentally corrupted or modified. Authenticity is a variant on this concept and provides a way to verify the origin of the data.
- 3) Availability and recoverability – Systems keep working and data can be recovered efficiently and completely, with no loss of accuracy or integrity, in case of data loss.

CDHS executes application level security via assignment of user rights that are part of a defined Oracle access known as a “responsibility.” Setting up a new user requires: 1) defining an individual user, and 2) assigning an access responsibility to that user. CDHS assigns defined responsibilities to application privileges that define the functional capabilities that the user may execute, for example, invoice input, journal input or journal approval and posting.

CFMS data is accessed and modified primarily through the related applications, as opposed to accessing the database directly. Strong administration of user access reduces the risk of unauthorized access as well as the risk of access granted to a user that is inconsistent or improper for that user’s specific job responsibilities.

Findings

Our procedures included obtaining available documentation related to application user access security policies and procedures and testing a sample of application users to determine if CDHS granted access that is consistent with documented policies.

Within the area of user access security, we noted the following:

- Eight of 25 users did not have appropriate authorization for the responsibilities they were granted.
- One super user and one system administrator were among the users noted above who did not have appropriate authorization for the responsibilities they were granted. Super users and system administrators have enhanced access to the system, allowing them to perform any and all operations on the computer. Super user and system administrator access should be granted selectively and extra precaution should be used to ensure that access is appropriate.
- One of three CEDS (county payroll) users selected did not have approval for CEDS access on their access setup forms.
- Two of 23 system administrators had not accessed CFMS in over 120 days. Best practices dictate that access not used for 120 days be reviewed and access be revoked as necessary.
- Three generic ID’s with published passwords allowing access to CFMS applications. Best practices dictate that generic ID’s should not be used.

Unauthorized or inappropriate access to CFMS applications increases the risk that data is accessed, viewed or modified in a manner that is unintentional or unauthorized. Such access can result in concerns regarding the accuracy, integrity and authenticity of the underlying financial data. In addition, systems may be rendered inoperable and unavailable as a result of unauthorized or unintentional access to systems and data.

Recommendation No. 8

In order to help reduce the risk of unauthorized access, as well as the risk of access granted to a user that is inconsistent, inadequate or improper for that user’s specific job responsibilities and to maintain adequate accountability for CFMS access, we recommend CDHS do the following:

- Strengthen adherence to user access setup policies and procedures.
- Eliminate all generic user IDs with published passwords.

- Review user access periodically to determine appropriateness and to verify that generic IDs are not in existence.

Colorado Department of Human Services' Response

Agree. A security plan which addresses all items in the recommendation will be developed by October 31, 2000 and implemented by December 31, 2000.

Segregation of Duties

Background

One of the basic principles of internal controls is segregation of duties. The principle of segregation of duties refers to the idea that conflicting functions within a workplace should be performed by separate individuals. Separate individuals should perform the initiation, approval, custody and record-keeping functions of a given transaction. In this, segregation of duties attempts to prevent the interaction of key positions that could potentially have a detrimental effect on the organization. People within the organization (insider threats) are the largest category of risk to the integrity of an organization. The principles of segregation are designed to prevent fraud or abuse unless collusion occurs.

Findings

Based on the performance of our procedures, we noted the Department and counties do not have adequate segregation of duties. We noted several positions related to CFMS input, processing and output which had recently become vacant or had remained unfilled for several months. It is our understanding that, in order to maintain certain processes, the Department and counties used existing personnel to perform functions normally assigned to the vacant positions. The specific duties that were or became vacant during the period covered by our procedures and the related findings are as follows:

- CDHS Cost Accountant – Responsible for input of CFMS cost allocation and share calculation entries

Cost allocation and share calculation entries are statistical entries that transfer or divide accumulated costs to the appropriate general ledger accounts and among the federal, state and county shares. Normally the cost accountant prepares and enters the transactions and the manager reviews, approves and posts the transactions. We noted the manager of local government accounting input, reviewed and posted the cost allocation and share calculation entries. An individual at CDHS separate from the individual entering these transactions did not review the entries prior to the running of mass allocations and posting to the general ledger.

- CDHS Budget Accountant – Responsible for input of CFMS budget entries

Normally the budget accountant prepares and enters the transactions and the manager reviews, approves and posts the transactions. We noted the manager of local government accounting input, reviewed and posted the budget entries. An individual at CDHS separate from the individual entering these transactions did not review the entries prior to the posting of these entries to the general ledger.

- CDHS Electronic Benefit Transfer (EBT) Accountant – Responsible for EBT administration and legacy code translation correction

The program accountant that processes the journals to correct errors caused by incorrect translations is now also correcting the translation in the absence of an EBT Accountant. An individual performing a separate review would help to ensure that translations are occurring and corrected in a timely manner.

- County Controller – Responsible for review and approval of finance department transactions

The county controller normally reviews and approves expenditures on the voucher information report to assure that expenditures are appropriate. In one of the counties where we performed procedures, we noted the county controller position was vacant from April 2000-June 2000. During the vacancy the individuals that entered the invoices for payment performed this review.

Recommendation No. 9

We recommend CDHS perform a periodic review of all open positions within the Department with CFMS responsibilities to ensure all critical duties are performed in a timely manner while maintaining an appropriate segregation of duties. In addition, all positions should have a designated substitute to ensure that critical duties are performed as necessary during an employee absence. Designated substitute or back-up personnel should be employees who do not perform conflicting functions.

As it relates to open positions at the county level, although county management is responsible for maintaining an effective internal control environment within the county, the Department is responsible for promoting the effective administration of the programs it supports. These responsibilities extend to the use of CFMS for the input, processing and output of data as well as compliance with user access security over CFMS. We recommend the Department make the county aware of the instances noted at the county where segregation of duties was compromised and help ensure that the situation has been adequately resolved.

Colorado Department of Human Services' Response

Agree. Responsibility for the County Controller resides with the County Director. We will share the breach of segregation of duties with the County Director. We are aware that the County Controller position has been filled. The CDHS positions listed: CDHS Cost Accountant, CDHS Budget Accountant and CDHS Electronic Benefit Transfer Accountant have been filled. Field Audits will include testing to check for segregation of duties on future audits. The CDHS security plan will encompass segregation of duties by segregating the post and approve function. However, counties with fewer than five employees may request a waiver from the separation of duties standards by implementing alternative internal control procedures. The alternative control procedures must be outlined in a waiver request that is submitted and approved by the CDHS Division of Accounting. This information will be shared with the County Directors by September 30, 2000.

Appendix I

Agreed-Upon Procedures Report

Office of the State Auditor:

We have performed the procedures enumerated below, which were agreed to by the Office of the State Auditor, solely to assist you in evaluating the effectiveness of certain controls in the County Financial Management System at the Colorado Department of Human Services for the period from May 1, 2000 through June 30, 2000. This agreed-upon procedures engagement was performed in accordance with attestation standards established by the American Institute of Certified Public Accountants. The sufficiency of these procedures is solely the responsibility of the specified users of this report. Consequently, we make no representations regarding the sufficiency of the procedures described below either for the purpose for which this report has been requested or for any other purpose.

Section I

Process Flow

1. Document high-level business process flows for the General Ledger module, with supporting narrative, of the County Financial Management System (CFMS) that is utilized by the Colorado Department of Human Services (CDHS).

We obtained and read available documentation on the CFMS business process flows. In addition, we interviewed CDHS and county employees and contractors who provide the business and technical support to CFMS. Based on the documentation we received and information derived from the interviews, we documented the business process flows for the General Ledger of CFMS.

2. Analyze the completed business process flow diagrams and associated narratives and identify control processes that have been implemented by CDHS.

We obtained and read available documentation on the CFMS business process flows. In addition, we interviewed CDHS and county employees and contractors who provide the business and technical support to CFMS. Based on the documentation we received and information derived from the interviews, we identified the control processes implemented by CDHS.

Input Controls

3. Obtain and read CFMS policies and procedures related to the authorization of input transactions. Interview personnel performing transaction input and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with documented policies and procedures.

We obtained and read available documentation on CFMS policies and procedures related to the authorization of input transactions. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee the transaction input process. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed that actual procedures utilized for county transaction input authorization are not consistent with those documented. Specifically, instances were noted where county transactions do not include proper departmental approval.

We observed that actual procedures utilized for open interface, County Employee Data Store (CEDS) and State journal entry transaction input authorization are consistent with those documented.

4. Select 25 transactions and determine if transactions were properly authorized for input.

We selected 25 transactions to determine if selected transactions were properly authorized for input. Of the 25 transactions selected, two county transactions were not properly authorized for input, as invoices did not include required departmental approval.

5. Obtain and read CFMS policies and procedures related to transaction input error correction procedures. Interview personnel performing input error correction procedures and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to transaction input error correction. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee the input error correction process. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed that actual procedures utilized for open interface transaction input error correction are not consistent with those documented. Specifically, erred transactions are not being corrected as required by policy. Instead, erred transactions for open interface transactions are recorded in a default general ledger account to allow uninterrupted processing, however, transactions are not subsequently moved to the correct general ledger account.

We observed that actual procedures utilized for CEDS, State journal entry and county transaction input error correction are consistent with those documented.

6. Select 25 transactions and determine if transactions were subject to input error correction procedures and the resolutions were appropriately documented.

We selected 25 transactions to determine if selected transactions were subject to input error correction procedures. Of the 25 transactions selected no input errors were noted. We selected four additional input transactions where errors were known to have occurred. Of the four erred transactions selected, all four were discovered and appropriately documented. However, three of the erred transactions were recorded in a default general ledger account and were not subsequently moved to the correct general ledger account.

7. Obtain and read CFMS policies and procedures related to input completeness and accuracy. Interview personnel performing transaction input and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to input completeness and accuracy. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee the transaction input process. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed actual procedures utilized for transaction input completeness and accuracy are consistent with those documented.

Processing Controls

8. Obtain and read policies and procedures related to the acceptance and processing of approved transactions through CFMS. Interview personnel performing transaction processing and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to acceptance and processing of transactions. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee transaction processing. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed that actual procedures utilized for acceptance and processing of transactions are consistent with those documented.

9. Select 25 transactions and determine if approved transactions were accepted and processed by CFMS.

We selected 25 transactions to determine if selected transactions were accepted and processed by CFMS; no exceptions were noted.

10. Obtain and read policies and procedures related to the one-time processing of transactions through CFMS. Interview personnel performing transaction processing and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to the one-time processing of transactions. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee transaction processing. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed that actual procedures utilized for the one-time processing of transactions are consistent with those documented.

11. Select 25 transactions and determine if transactions were processed by CFMS only once.

We selected 25 transactions to determine if selected transactions were processed by CFMS only once; no exceptions were noted.

12. Obtain and read policies and procedures related to rejected transaction reporting by CFMS. Interview personnel performing transaction processing and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to rejected transaction reporting. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee transaction processing. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed that actual procedures utilized for rejected transaction reporting are consistent with those documented.

13. Select 25 transactions and determine if rejected transactions were reported by CFMS.

We selected 25 transactions to determine if selected transactions had errors which were reported by CFMS. Of the 25 transactions selected, no errors were noted. We selected four additional transactions where errors were known to have occurred. Of the four erred transactions selected, all four were discovered and reported by CFMS.

14. Obtain and read policies and procedures related to the posting of transactions to the appropriate general ledger account. Interview personnel performing transaction processing and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to the posting of transactions to the appropriate general ledger account. In addition, we interviewed CDHS and county employees and contractors who are responsible for and/or oversee transaction processing. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed that actual procedures utilized for the posting of transactions to the appropriate general ledger account are consistent with those documented.

Output Controls

15. Obtain and read policies and procedures related to the authorization of access to CFMS output. Interview personnel performing the output process and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to the authorization of access to output. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee the output process.

We observed that documented policies and procedures related to the authorization of access to output do not exist. As policies and procedures are not documented, through our interviews with CDHS personnel, we gathered information regarding the procedures prescribed by management related to authorization of access to output. We compared the current procedures utilized by personnel to those prescribed by management.

We observed that actual procedures utilized for authorization of access to output are not consistent with those prescribed by management.

16. Select 25 transactions and determine if the output was only accessible to authorized personnel.

We selected 25 transactions to determine if output of selected transactions was accessible only to authorized personnel. Of the 25 transactions selected, the output of one transaction was not limited to authorized personnel, as the individual's user form did not include appropriate access authorization.

17. Obtain and read policies and procedures related to CFMS output completeness and accuracy. Interview personnel performing the output process and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to output completeness and accuracy. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee the output process. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented for open interface, State journal entry and county transaction output completeness and accuracy.

We observed that actual procedures utilized for open interface transaction output completeness and accuracy are not consistent with those documented. Specifically, a policy requiring monthly reconciliation to verify the completeness and accuracy of transaction output is not being performed in a timely manner.

We observed that actual procedures utilized for State journal entry and county transaction output completeness and accuracy are consistent with those documented.

We observed that documented policies and procedures utilized for CEDS transaction output completeness and accuracy do not exist. As policies and procedures are not documented, through our interviews with CDHS personnel, we gathered information regarding the procedures prescribed by management related to CEDS transaction output completeness and accuracy. We compared the current procedures utilized by personnel to those prescribed by management and found that actual procedures utilized are consistent with those prescribed.

Security Controls / Software Change Controls

18. Obtain and read policies and procedures related to application user access rights and application security administration within CFMS. Interview personnel performing application security and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to application user access rights and security administration. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee application security. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed that actual procedures utilized for application user access rights and security administration are not consistent with those documented. Specifically, instances were noted where the individuals' user forms did not include appropriate authorization for the module to which they were granted access.

19. Select 25 CFMS application users' access rights and determine if the user's access was appropriately authorized.

We selected 25 application users' access rights to determine if the user's access was appropriately authorized. Of the 25 users' access rights selected, 8 did not have appropriate authorization for the modules to which they were granted access.

20. Obtain documentation on CFMS database administrators' access rights and database security administration and determine if database administrators' access was appropriately authorized.

We obtained documentation on the four individuals with access to the database. Of the four individuals, two did not have appropriate authorization for access to the database.

21. Obtain and read policies and procedures related to application change management within CFMS. Interview personnel performing application changes and compare documented policies and procedures to the current practices utilized by personnel to determine if the actual procedures utilized are consistent with those documented.

We obtained and read available documentation on CFMS policies and procedures related to application change management. In addition, we interviewed CDHS and county employees and contractors who perform and/or oversee application change management. Based on the information derived from the interviews and CDHS documentation, we compared the current procedures utilized by personnel to the policies and procedures documented.

We observed that actual procedures utilized for application change management are not consistent with those documented. Specifically, instances were noted where application change documentation was missing or incomplete.

22. Select 15 CFMS software changes and determine if selected application changes were appropriately authorized and properly migrated into the CFMS production environment.

We selected 15 CFMS application changes to determine if selected application changes were appropriately authorized and properly migrated into the CFMS production environment. Of the 15 application changes selected, 7 had no documentation of an approved and processed change request and an additional 7 had incomplete documentation of an approved and processed change request.

Section II

Additional Testing

1. Regarding the control processes documented in procedure #7, Section I, select 25 transactions and determine if the transactions, which were input, were complete and accurate.

We selected 25 transactions to determine if input was complete and accurate for selected transactions; no exceptions were noted.

2. Regarding the control processes documented in procedure #14, Section I, select 25 transactions and determine if the transactions were posted to the appropriate accounts and properly recorded in the general ledger.

We selected 25 transactions to determine if selected transactions were posted to the appropriate account and properly recorded in the general ledger; no exceptions were noted.

3. Regarding the control processes documented in procedure #17, Section I, select 25 transactions and determine if the data input and processed by CFMS was complete and accurate in output reports.

We selected 25 transactions to determine if selected transactions were complete and accurate in output reports; no exceptions were noted.

We were not engaged to, and did not, perform an examination, the objective of which would be the expression of an opinion on the effectiveness of the controls over CFMS for the input, processing and output of data. Accordingly, we do not express such an opinion. Had we performed additional procedures, other matters might have come to our attention that would have been reported to you.

This report is intended solely for the information and use of the Office of the State Auditor, and is not intended to be and should not be used by anyone other than these specified parties. However, upon release of the Legislative Audit Committee, this report is a matter of public record and its distribution is not limited.

KPMG LLP

June 30, 2000

Distribution

Copies of this report have been distributed to:

Legislative Audit Committee (12)

Department of Human Services (8)

Joint Budget Committee (2)

Department of Personnel
d.b.a. General Support Services
Executive Director (2)
State Controller (2)

Honorable Bill Owens, Governor

Office of State Planning and Budgeting (2)

Depository Center, Colorado State Library (4)

Joint Legislative Library (6)

State Archivist (permanent copy)

National Conference of State Legislatures

Legislative Oversight Committee

Legislative Legal Services

Auraria Library

Colorado State University Library

Copies of the report summary have been distributed to:

Members of the National Legislative Program Evaluation Society

Members of the Colorado General Assembly

National Association of State Auditors, Comptrollers and Treasurers

Report Control Number 1275