

# Special Report

*Department of Human Services  
Arkansas Client Eligibility System  
Information System Controls Audit*

---



---

ARKANSAS DIVISION OF LEGISLATIVE AUDIT

November 7, 2002



Sen. Kevin A. Smith  
Senate Co-Chair  
Rep. Danny W. Ferguson  
House Co-Chair  
Sen. Henry "Hank" Wilkins, IV  
Senate Co-Vice Chair  
Rep. Tommy Roebuck  
House Co-Vice Chair

# Arkansas



Charles L. Robinson, CPA, CFE  
Legislative Auditor

## LEGISLATIVE JOINT AUDITING COMMITTEE DIVISION OF LEGISLATIVE AUDIT

Members of the Legislative Joint Auditing Committee:

We have performed an audit of the Arkansas Client Eligibility System (ACES) in use from December 19, 2001 to February 15, 2002, the last day of our audit fieldwork. We conducted our audit in accordance with generally accepted governmental auditing standards.

Our objectives were to examine and evaluate the adequacy of the operating and administrative procedures, practices and policies to obtain reasonable assurance that sufficient controls exist over ACES to: protect the application and database from unauthorized access; provide for the continuation of computer processing capabilities; ensure proper management of program change requests, ensure the accurate and complete transfer of all files into and out of ACES; and ensure that the input, processing and output of data is accurate and complete.

Our audit procedures consisted of designing, performing and evaluating the results of tests of these controls. We believe our audit provides a reasonable basis for our opinion.

Because of inherent limitations of controls, errors or fraud may occur and not be detected. Also, projection of this evaluation to future periods is subject to the risk that audit procedures performed may become inadequate because of changes to these controls.

The conclusions and recommendations resulting from our review are contained in the attached report. We trust the information in this report will assist you in your legislative decision-making process.

DIVISION OF LEGISLATIVE AUDIT

A handwritten signature in blue ink, appearing to read "Charles L. Robinson".

Charles L. Robinson, CPA, CFE  
Legislative Auditor

February 15, 2002  
IS0000101

## EXECUTIVE SUMMARY

This report includes our evaluation of the controls over the Arkansas Client Eligibility System (ACES) and the related EBT (Electronic Benefits Transfer) function. The Department of Human Services (DHS) relies on ACES to determine client eligibility for federal assistance programs. During our audit, we reviewed policies and procedures relating to ensuring appropriate input, processing and output of data; managing system development and program changes; providing data access security; proper system backup procedures are in place and utilized; and ensuring appropriate measures are in place for disaster recovery.

The report includes recommendations to improve management of ACES. Priority items needing attention include developing a contingency plan for this application, improving controls over data access security, encryption of passwords, and backup of the ACES transaction file.

DHS management generally agrees with our recommendations. The purpose of this report is to provide our analysis, findings, and recommendations regarding our audit of the ACES application. A project is currently underway to upgrade to a windows based on-line real time application that would replace ACES. The ACES system was selected for this audit because it is considered the implementation point and determines eligibility for federal assistance programs. ACES is utilized in 85 county offices throughout the state of Arkansas. Each county processes applicants and determines eligibility for assistance. Our audit resulted in the following significant findings:

- Programmers with update ability in ACES.
- Terminated employees with data file access.
- Passwords are stored in clear text.
- Data integrity edits not working properly.
- ACES transaction file not being backed up.
- No contingency plan in place.
- Lack of balancing controls for application input/output files.

## **I. BACKGROUND**

ACES is the software used by the Department of Human Services (DHS) to determine client eligibility, provide case management and reporting for Medicaid and Temporary Employment Assistance (TEA). ACES was developed in-house by the Office of Program, Planning and Development in 1986. ACES was maintained by DHS until 1996, when program maintenance and future enhancements were outsourced to Thompson-Ramo-Woolridge Inc. (TRW), an independent contractor. TRW's workforce consists of approximately 63 programmers, quality assurance and administrative personnel.

The application resides on the Department of Information System's (DIS) mainframe. The application stores benefit recipients' current and historical data to be used for claims processing, research and administrative reporting. ACES sends recipient benefit information to the Electronic Benefits Transfer (EBT) processor monthly. The EBT system produces benefit cards on new recipients and loads benefit values for new and continuing recipients. This computer application interfaces with the Medicaid claims processing system (MMIS), Social Security, Foster Care billing, Nursing Home billing, Daycare billing and the Employment Security Division.

## **II. OBJECTIVES**

Our objectives were to examine and evaluate the adequacy of the operating and administrative procedures, practices and policies to obtain reasonable assurance that sufficient controls exist over ACES to:

- Protect the application and database from unauthorized access
- Provide for the continuation of computer processing capabilities
- Ensure proper management of program change requests
- Ensure the accurate and complete transfer of all files into and out of ACES
- Ensure that the input, processing and output of data is accurate and complete

### III. SCOPE AND METHODOLOGY

Our audit focused on the daily operations of DHS and TRW and the responsibility of each regarding ACES. Our audit procedures included interviewing key personnel, reviewing relevant policy and procedure documentation, identifying and assessing the adequacy of general and application controls, and testing the relevant controls.

General controls comprise the processing environment including management of computer resources, file access, change control, contingency planning and backup of critical files. Application controls are specific to an application and ensure only authorized data is processed, processing is complete and accurate and output is reliable. Effective general controls form the foundation for effective application controls.

Because of inherent limitations of controls, errors or fraud may occur and not be detected. Also, projection of this evaluation to future periods is subject to the risk that audit procedures done may become inadequate because of changes to these controls. We believe that our audit provides a reasonable basis for our opinion.

### IV. CONCLUSION

As a result of our examination and testing, several significant deficiencies in controls were identified. These deficiencies along with our recommendations are listed in the remainder of this report. In our opinion, these deficiencies should be addressed to ensure the integrity of the system.

### V. FINDINGS AND RECOMMENDATIONS

#### 1. Programmers with update ability in ACES.

An ACES application programmer has the ability to initiate financial transactions in ACES. Sound information system controls dictate that proper segregation of functions should be maintained between users of ACES and the information system personnel responsible for the development and maintenance of the system. Segregation of functions

---

...these deficiencies should be addressed to ensure the integrity of the system.

---

---

An ACES application programmer has the ability to initiate financial transactions in ACES.

---

is not achieved if application programmers have the ability to initiate transactions in the ACES system.

We recommend that controls be installed to prevent application programmers from having the ability to create or change transactions in the ACES system.

***Agency Response:***

*“The agency will implement a process where all individuals on the ACES/FACTS/WISE security file will be matched against a file of current State employees. Individuals not found on the State employee file will be deleted. ”*

**2. Terminated employees with data file access.**

There are several active logon ids belonging to users who are terminated employees of DHS. This situation will allow these terminated employees the ability to create and view transactions in ACES. Sound security principles dictate that terminated employees access abilities be removed in a timely manner.

We recommend that DHS do a periodic review of all user accounts to ensure that only authorized individuals have the ability to access ACES.

***Agency Response:***

*“The agency will implement a process where all individuals on the ACES/FACTS/WISE security file will be matched against a file of current State employees. Individuals not found on the State employee file will be deleted. There are actually two levels of security for ACES, one of which is not addressed in this finding– in addition to the application security in ACES, ACF/2 security is required to gain access to ACES files (e.g. even if a person has a valid ACES User ID and password, but that person’s ACF/2 ID has been removed, the person cannot access ACES). ACF/2 ID’s are checked against employee termination files every two weeks.”*

---

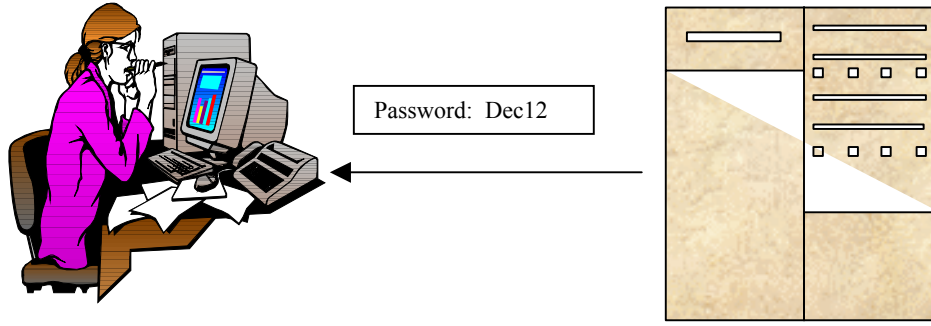
There are several active logon ids belonging to users who are terminated employees of DHS.

---

**3. User passwords are stored in clear text.**

Data stored in clear text format can be read by an individual with access to the data as illustrated below.

**User viewing password in clear text**



**DIS Mainframe Computer**

Data that is encrypted is transformed into an unreadable form that can only be deciphered by an authorized individual with an electronic key. ACES stores passwords and other pertinent user data in a clear text format in the security master file. This situation will allow TRW programmers with access to the security master file the ability to obtain passwords for all user accounts. Proper security over ACES cannot be assured if there are methods to gain knowledge of other users' passwords.

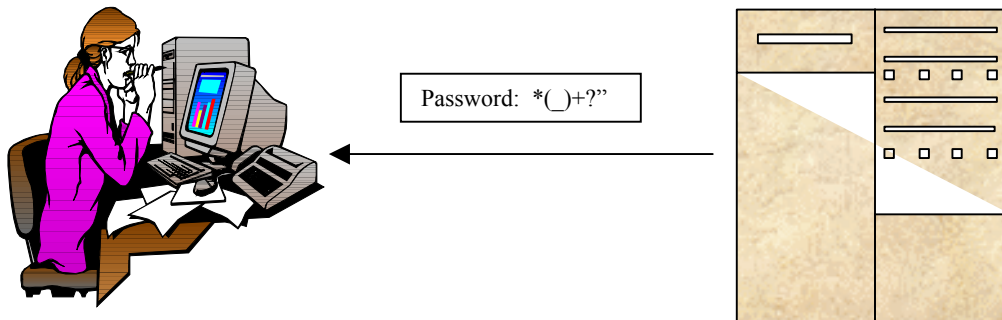
We recommend DHS establish procedures to have the system passwords encrypted or otherwise protected against disclosure. An example of a user viewing encrypted data is illustrated below.

---

Proper security over ACES cannot be assured if there are methods to gain knowledge of other users' passwords.

---

**User viewing password in encrypted format**



**DIS Mainframe Computer**

***Agency Response:***

*“The agency will analyze the scope of the problem and determine the most cost effective solution. However, it should be noted, as above, that there is a second level of security imposed by ACF2, which does use encrypted passwords.”*

**4. Data integrity edits need improvements.**

The application date field on the Income Medicaid Application Update (WIMA) screen and the begin date field on the Transition Employment Assistance (TEA) screen will accept any data value placed into these fields. This situation will allow transactions to be backdated, causing the length of the benefit eligibility period to be calculated incorrectly, which could result in an overpayment to a benefit recipient. Sound information system controls dictate that input screen controls (edits) be in place to detect errors and maintain data integrity.

We recommend that DHS add edits to these date fields to prevent an overpayment to a benefit recipient.

***Agency Response:***

*“There are situations where it is necessary for the application date and the Transitional Medicaid Begin Date need to be back dated. For example, if a hearing is requested and the findings are in favor of the client, the county may be ordered to make the date of application or eligibility date retroactive to the original date. However, the agency will assess this practice and determine if these types of updates should be restricted to administrator level staff.”*

**5. No contingency plan.**

A contingency plan includes procedures for providing hardware, software, supplies and personnel to operate the backup computer facilities or restore the primary computer facilities in the event of a major interruption or disaster. The ACES

---

...situation will allow transactions to be backdated... which could result in an overpayment to a benefit recipient.

---

application, which is processed at the DIS Data Center, relies upon DIS's Contingency Plan. DIS's Contingency Plan contains emergency call lists, organizational charts and procedures, but does not address recovery of computer processing or backup computer facilities. This situation could cause the state to be without ACES computer processing for an extended period of time in the event of a disaster or major interruption.

We recommend that DHS management work with DIS management to develop computer recovery procedures in the Contingency Plan and that the plan be periodically tested.

***Agency Response:***

*“DHS management will work with DIS to develop an appropriate Contingency Plan.”*

**6. No balancing controls on files received from or sent to other applications.**

The ACES system interfaces (transmits data) with various other applications. Balancing procedures should be performed to ensure the accuracy and completeness of these transmissions of data between applications. The balancing process is normally performed as follows:

- a) The data from the sender contains a totals control record that has the quantity and dollar amount for the data being transmitted.
- b) The receiver recalculates the quantity and dollar amount of the data and accepts the data if these amounts equal the totals control record amounts.

There are no balancing controls at any interfacing points between ACES and other applications.

We recommend that DHS management develop some method that would guarantee the accurate and complete interface of files.

---

...Contingency Plan...does not address recovery of computer processing or backup computer facilities...could cause the state to be without ACES computer processing for an extended period...

---

---

There are no balancing controls at any interfacing points between ACES and other applications.

---

***Agency Response:***

*“The agency will work with TRW to identify interfaces where such a balancing process is appropriate and implement these processes when feasible.”*