Department of Human Services

Automated Child Support Enforcement System (ACSES)

December 1, 1996 to July 18, 1997

Richard L. Fair
State Auditor
Enclosed is our report on the audit of the Department of Human Services, Automated Child Support Enforcement System (ACSES) for the period December 1, 1996 to July 18, 1997.

If you would like a personal briefing, please call me at (609) 292-3700.

Peter M. Guilfoyle
Assistant State Auditor
September 23, 1997
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>2</td>
</tr>
<tr>
<td>Conclusions</td>
<td>3</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Access Controls</td>
<td>4</td>
</tr>
<tr>
<td>Security Administrator</td>
<td>4</td>
</tr>
<tr>
<td>Security Policies and Standards</td>
<td>6</td>
</tr>
<tr>
<td>TP 8 Security Software</td>
<td>7</td>
</tr>
<tr>
<td>Year 2000 Plan</td>
<td>8</td>
</tr>
<tr>
<td>Automated Features</td>
<td>9</td>
</tr>
</tbody>
</table>
Scope

We have completed an audit of the state’s Automated Child Support Enforcement System (ACSES) for the period December 1, 1996 to July 18, 1997. Our audit evaluated application controls and selected general controls involved in the processing of child support and enforcement data. More specifically, the audit included the examination of application security, logical access control, application design and development (including change and problem management) and application processing controls (including validations and edits). We also reviewed the disaster recovery plan and test recently performed for the BULL operating platform and the Year 2000 plan for the ACSES system.

We did not evaluate the propriety of the specific ACSES transactions, such as whether the appropriate transaction was used or whether the appropriate person performed and approved the transaction for processing. Nor did we determine whether transactions processed through the system were accurate or related to each agency’s programs.

Objectives

The objectives of our audit included determining whether ACSES ensured child support and enforcement data were reliable, valid, and were properly safeguarded. Year 2000 planning for the ACSES application was reviewed to determine if the plan is current and the necessary processes are being implemented to ensure ACSES will be ready to process data in the next millennium. The results of the BULL disaster recovery test, which specifically included the ACSES application, was reviewed to determine if the test was satisfactory and in accordance with the plan, and provides assurances that the plan is satisfactory in the event of a real disaster.
This audit was conducted pursuant to the State Auditor’s responsibilities as set forth in Article VII, Section 1, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with Government Auditing Standards, issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by the Computer Security Handbook, Generally Accepted Principles and Practices for Securing Information Technology Systems and selected Federal Information Processing Standards (FIPS) issued by the National Institute of Standards and Technology (NIST); Year 2000 Compliance issued by the General Accounting Office (GAO) and Institute of Internal Auditors (IIA) and selected computer application guidelines and training material issued by the MIS Training Institute (MIS).

In preparation for our testing, we studied system user, operation, and facility guides, contract deliverable documentation, system programmers' code (COBOL 74 and 85), circular letters promulgated by the State Comptroller, and policies of the Administrative Office of the Courts, the Division of Family Development and the Office of Telecommunications and Information Systems. Provisions that we considered significant were documented and compliance with those requirements was verified by interview and observation and through our sampling of ACSES transactions.

A nonstatistical sampling approach was used. Our samples of ACSES transactions were designed to provide conclusions about the integrity of the data as well as internal control attributes. Sampled transactions were judgmentally selected.
We found that the Automated Child Support Enforcement System (ACSES) does have basic preventative, detective or corrective controls to ensure the accuracy, reliability and safeguarding of child support and financial data, and adherence with management's policies and procedures. However, we did note significant control weaknesses warranting management’s attention. Additionally, we question whether the current system will be ready for the Year 2000 rollover which raises going concern issues as the system will not be able to function properly if the issues are not addressed.

Specifically, in each of the areas tested, we noted improvements which should be made. These improvements include the following.

C Access controls including security policies and procedures need to be maintained, updated and promulgated. These polices need to address the proper segregation of duties for security administration.

C Good management policies and practices on the program and project levels for ACSES Year 2000 projects need to be promulgated and enforced.

C Enhancements to allow ACSES to provide on-line processing and on-line financial reporting should be implemented.
Access Controls

Access controls are intended to prevent and detect unauthorized access and use of computer files, programs, resources and documentation. Access to computer data and its resources should be controlled to protect them from unauthorized use, damage, loss or modification which can ultimately result in the loss or misuse of assets or the processing of invalid or inaccurate data.

Security Administrator

The security administrator function is responsible for implementing, maintaining and enforcing the computer security and policies of an organization. This function should be centralized and independent of programming and data processing personnel. In a decentralized processing environment, such as ACSES, there is a need for a centralized security administrator function to effectively monitor computer processing activities.

Management does not have an independent security administrator for the ACSES computer system. No one regularly reviews user activity for instances of improper access and use. Centrally, a systems programmer, whose responsibilities also include maintaining and monitoring Transaction Processor (TP 8) system software (programs and utilities), is responsible for the maintenance of the security software and security databases as well as having custody of violations reports. This represents a lack of segregation of duties. By granting excessive access, programmers who have the technical expertise could exploit program weaknesses or make unauthorized modifications to the system that may go undetected.

At the local level, the county welfare and probation offices' County Security Administrators (CSA) are assigned the responsibility of security administration including monitoring computer activities and setting up user identifications (UIDs) and access privileges. A
review of county user id records indicates that access privileges are not properly assigned. CSAs had additional ACSES privileges allowing them to perform non-security functions. At the probation offices, 24 of the 25 CSAs had the authority to update ACSES case data (demographics) and financial records. Similar results were noted in our analysis of the welfare agencies where 32 of the 41 CSAs had additional ACSES privileges. Granting persons who protect the computer data, the ability to modify and update accounting and case data records represents a conflict of duties and increases the risk of unauthorized access, use and modification of sensitive data.

**Recommendation**

We recommend that ACSES management assign the duties of security administrator for ACSES to a person who is separate from systems programmers and system users. The function of the security administrator should be performed by an independent person within a centralized unit of the organization. The security administrator should be delegated the authority to monitor and scrutinize ACSES system access and to deny or terminate privileges and logon id's when they violate reasonable standards for proper control.
A n effective control environment requires the development and maintenance of adequate security standards, policies and procedures. Implementing security standards is necessary to ensure the control environment protects access to the computer system.

Security Policies and Standards

ACSES management is responsible for administering the access control environment for processing performed by its computer applications. This includes the ACSES computer application which resides on the BULL mainframe at the HUB data center. ACSES functions in a decentralized environment requiring the need for sound security policies and procedures. This type of environment provides control at the user agency and is managed by the security system software.

ACSES management lacks adequate security policies and standards that specify how security is to be implemented. Although a security handbook was issued in March 1988, it has not been updated and does not address many critical issues, such as proper password control and proper assignment of privileges.

Management’s failure to provide sufficient policies and standards increases access control risk due to the lack of proper computer security awareness. In a computer system environment that processed approximately $545 million of transactions for the fiscal year ending June 30, 1997, a sound security policy is necessary to provide guidance in the protection of computer data and its resources.

Recommendation

We recommend that ACSES management develop and promulgate adequate policies and standards to enforce security and enhance controls. The policy should be disseminated as an authoritative directive or circular letter to all ACSES system users including client and user agencies. This directive should provide guidelines to client agencies regarding computer security and include, but not be limited to, general security controls, administrative controls and logical (access)
controls. These policies and standards should also be periodically reviewed and updated.

TP 8 Security Software

The ACSES application operates in the BULL operating system environment where security begins with the operating system and continues with the Transaction Processor 8 (TP 8) for the online environment. TP 8 has been enhanced by security software that is an internally developed product designed to fill the utilization and access control needs of the Division of Family Development (DFD). The current system was initially developed by DFD and is maintained by OTIS Technical Services. Programming enhancement and modification requests are made by OTIS under the direction of DFD.

An effective control system in a computer processing environment requires the implementation of adequate logical (access) controls. Such controls are designed to protect the computer system against unauthorized admission and use. Security software automates access controls by identifying and verifying user attempts to gain access to computer data and its resources.

The current security software provides only basic security controls and lacks critical automated features to adequately protect the system. The security software does not do the following: prevent the user from creating a password that is the same as their user identification; prevent the user from selecting a new password which is the same as the old; provide for the encryption of passwords; generate a log or report of security events; limit unauthorized access attempts to the system; nor prevent a user from processing transactions under another user’s worker id. These procedures are needed to prevent and detect unauthorized access and improper use of data.
**Recommendation**

We recommend that ACSES management evaluate the current security software and add the necessary features that would ensure computer data and its resources are protected and attempts to breach security do not go undetected.

½

**Year 2000 Plan**

Implementing a structured planning approach and rigorous program management can decrease risks associated with the Year 2000 crisis.

Most computer systems, including ACSES store and refer to dates as a six digit number. The year is referred to by the last two digits and there is no reference to the century. Thus, when the calendar moves from 1999 to 2000, the year element of dates will change from "99" to "00". Although some ACSES programs and data fields have been changed to correct this problem, many still need to be identified and corrected. The calculations that are performed using a two digit year code will generate results that will range from misleading to disastrous, as the system will imply that the "true" year is 1900 instead of 2000. This will have obvious effects on processing which is date dependent.

ACSES is a complex computer application comprised of numerous programs, data bases and interfaces with other computer systems. ACSES performs various automated functions through a series of programs that accept and analyze data and determine the appropriate actions based on case conditions in accordance with pertinent laws, regulations and rules. The current system is made up of over 900 programs and contains over 480,000 lines of code.

Although staff has analyzed possible solutions, at the date of this writing management had not made a final decision as to how the ACSES year 2000 problem will be resolved.
Adequate planning and assessment for ensuring the ACSES system is Year 2000 compliant is necessary to provide an economical, auditable and controllable application into the next century. Implementing a structured planning approach and rigorous program management can decrease risks associated with the Year 2000 crisis.

**Recommendation**

We recommend that ACSES management develop and implement an ACSES Year 2000 plan immediately while promulgating and enforcing good management practices on the program and project levels. Time is of the essence as the application should be in place and working by the 31st of December 1998 to allow for proper processing of future dates and to ensure that the system copes with the changes correctly in the year before the change of century.

\[ 1/4/2 \]

**Automated Features**

Installing automated features to the State’s automated child support enforcement system increases the effectiveness and efficiencies of the system.

ACSES is the state’s automated system used to enforce child support cases. Developed more than a decade ago, ACSES has provided the state with an effective child support collection and enforcement system. However, due to advances in data processing technology and system integration, ACSES design can be considered obsolete.

The objectives of system design, development and maintenance controls in a computer processing environment are to implement and maintain a system that will meet the information and operating needs of management and ensure the reliability and efficiency of the system. ACSES lacks several automated features that would contribute to its efficiency and effectiveness.

There are no automated interfaces between ACSES and certain related state data systems such as the Family Automated Case Tracking System (FACTS)
and Medicaid. The “Report of the Joint Advisory Committee (JAC) on Child Support Enforcement estimates that approximately 160,000 child support cases will be processed during fiscal year 1997. An automated interface could eliminate the need for unnecessary duplications of data entry and would reduce the risk of human error in the process. Additionally, this automation would allow ACSES and Medicaid agencies to meet federal mandates.

In addition, ACSES does not provide online features and capabilities that could increase work efficiency.

- Staff are unable to determine the current status of transactions and accounts due to lack of real-time data processing.
- Case data and histories are not available when needed due lack of online access to archived data.
- Cumulative fiscal data required for financial reporting is not readily available for fiscal unit staff due to the lack of on-line financial reporting functions.
- System test personnel are unable to readily obtain key case data necessary for testing due to the lack of online case data retrieval capabilities.

Enhancing ACSES to include automated and online processing features in an environment that relies on computer processed data decreases the risk of errors and oversights during data entry while increasing the efficiency of the system.

**Recommendation**

We recommend that ACSES management study the cost benefit of an automated interface between ACSES and existing data systems including FACTS and Medicaid and implement enhancements to ACSES providing for on-line processing and on-line financial reporting functions.