April 29, 1998

RE: A Review of the Child and Adult
Protective System at the Department of
Protective and Regulatory Services

Members of the Legislative Audit Committee:

Our review of the general automation environment and the Child and Adult Protective System at the Department of Protective and Regulatory Services (Department) revealed some weaknesses, but overall the financial data and related reports used to manage the programs can be relied upon for decision-making.

The Child and Adult Protective System (CAPS) tracks allegations of abuse, investigations of abuse, and provision of services to approximately 800,000 children, adults, and families annually. CAPS, including the hardware and infrastructure to support approximately 6000 caseworkers, was implemented at a cost of approximately $65 million. CAPS replaced an antiquated paper-based service delivery system. CAPS allows the Department to be more responsive to requests for information regarding all aspects of service delivery.

Objectives and Scope

The objective of our work at the Department was to determine the reliability of CAPS and the reports generated from its data. To attain this objective we performed a review of (1) the computer general controls and (2) the CAPS application controls. In order to further assess reliability of CAPS, data testing of services provided for Purchase Services for fiscal year 1997 and payments for those services was performed.

This audit was conducted in accordance with Generally Accepted Governmental Auditing Standards with the exception that we did not obtain written comments from management regarding our observations or proposed recommendations. However, we did obtain verbal concurrence from the Department. The Department has indicated that it will take the necessary corrective actions.

Summary of Issues

- **Improvements need to be made to the computer security administration function.**

  Having formal security policies and diligent security administration helps ensure the integrity of computer data vital to managing the programs and providing services to clients. Adherence to a thorough set of security policies and procedures provides additional assurance that violations are detected before data integrity is affected.

SAO Report No. 98-039

During our review of the computer security administration function several weaknesses were noted. However, having a security administration function and performing security administration are strengths in themselves. While the CAPS contractor who performs security administration duties has adequate access to computer system information, the Department employee with security administrator responsibilities lacks sufficient access to perform critical duties commonly associated with security administration. Also, some of the traditional security administrator duties, such as reviewing and investigating invalid computer access attempts, are not being performed by either the contract security administrator or the Department security administrator. The investigation of invalid access attempts is important because it is critical that the Department ensure unauthorized personnel are not attempting to obtain access to the system.

Additionally, no other Department personnel are sufficiently trained as a backup to perform the key security duties in the event the primary Department security administrator is not available. Turnover in the Department security administrator position during the time of our fieldwork resulted in some key duties not being performed. We also noted that lists of official employment terminations and transfers are not verified against changes to computer user account privileges to ensure that terminated employees accounts are disabled. Computer accounts of terminated employees are not suspended until after the employee's last day on the payroll, which may be later than the employee's last day physically on the job. There have also been instances in which the accounts of terminating employees have remained active after termination due to a failure of field supervisors to request removal of the account.

To better monitor computer security, the Department should:

−   Expand the responsibilities of the security administration job, along with expanded access abilities, in order to more closely monitor the security of the Department systems, including CAPS.

−   Include in the expansion of these duties the review and investigation of access violations and the monitoring of employee terminations and transfer records as compared to changes in computer access capabilities.

We commend the Department for adopting a *Security Policy and Control Manual* and filling the Security Administrator position that became vacant during our fieldwork. The Department is in the process of implementing the manual and extracting/disseminating the user security policies.

- **Selection of System Development Methodology should be communicated.**

  The lack of communication about and training in the use of the application development methodology increases the risk of inconsistency in attention to details in the design process. It also increases the risk that analysis and development processes will vary substantially between projects, potentially resulting in systems that are inefficient, may not meet the users needs, and/or have increased costs for maintenance.

  CAPS was developed using the Foundation/Method 1 system development methodology. While the Department has adopted Foundation/Method 1 as its official system development methodology, the decision has not been communicated to the entire development staff. This lack of communication also indicates that not all development staff have been trained in the proper use of the methodology.

  We recommend that the Department communicate the decision to adopt the Foundation/Method 1 development methodology to all development staff. We also recommend that development staff members be trained in the proper use of the methodology for the tasks that they will be performing or managing others in performing.

We appreciate the courtesy and cooperation of the Department's management and employees in assisting us in obtaining information.

Sincerely,

Lawrence F. Alwin, CPA
State Auditor

khm

cc: Mr. James Hine, Executive Director
        Mr. Bowden Hight, Deputy Director for Information Technology
        Ms. Jeannie Henderson, CPA, Director of Internal Audit
        Members, Texas Board of Protective and Regulatory Services