

**STATE OF SOUTH CAROLINA**

**INDEPENDENT AUDITORS' REPORT ON  
COMPLIANCE AND ON INTERNAL CONTROL OVER  
FINANCIAL REPORTING BASED ON AN AUDIT OF  
GENERAL PURPOSE FINANCIAL STATEMENTS  
PERFORMED IN ACCORDANCE WITH  
*GOVERNMENT AUDITING STANDARDS***

**JUNE 30, 1998**

## CONTENTS

## PAGE

INDEPENDENT AUDITORS' REPORT ON COMPLIANCE AND ON INTERNAL CONTROL OVER FINANCIAL REPORTING BASED ON AN AUDIT OF GENERAL PURPOSE FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH <i>GOVERNMENT AUDITING STANDARDS</i>	1
<b>REPORTABLE CONDITIONS</b>	
GAAP CLOSING PACKAGES	
Fixed Asset	
Archives and History	3
Department of Corrections	3
Grants and Entitlements	
Department of Health and Environmental Control	3
Department of Health and Human Services	3
<b>OTHER MATTERS</b>	
RECONCILIATIONS	
Department of Social Services	5
DATA PROCESSING	
Access to System Resources	
Budget and Control Board - Division of Operations - Office of Information Resources	6
Office of Information Resources – Financial Data Services	6
Disaster Recovery/Business Continuity	
Budget and Control Board – Division of Operations - Office of Information Resources	7
Information Security Policy	
Office of the State Treasurer	9
Notification of Terminated or Transferred Employees	
Department of Revenue	10
SUMMARY OF PRIOR YEAR FINDINGS	10
<b>MANAGEMENTS' RESPONSES</b>	11

INDEPENDENT AUDITORS' REPORT ON COMPLIANCE AND ON INTERNAL CONTROL  
OVER FINANCIAL REPORTING BASED ON AN AUDIT OF GENERAL PURPOSE  
FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH  
GOVERNMENT AUDITING STANDARDS

The Honorable James H. Hodges, Governor  
and  
Members of the General Assembly  
State of South Carolina  
Columbia, South Carolina

We have jointly audited the general purpose financial statements of the State of South Carolina as of and for the year ended June 30, 1998, and have issued our report thereon dated December 2, 1998, which was qualified because insufficient audit evidence exists to support the State of South Carolina's disclosures with respect to the year 2000 issue. We did not jointly audit the financial statements of certain blended component units and agencies of the primary government, which statements reflect the indicated percent of total assets and other debits and total revenues, respectively, of the Special Revenue (21% and 14%), Enterprise (99% and 89%), Internal Service (73% and 86%), Pension Trust (100% and 100%), Investment Trust (100% and 100%), Higher Education (100% and 100%), and Agency (69% of assets and other debits) Funds, General Fixed Assets Account Group (12% of assets and other debits), and the General Long-Term Obligations Account Group (14% of assets and other debits). We also did not jointly audit the financial statements of the discretely presented component units. Those financial statements were audited by other auditors, including the Office of the State Auditor and Deloitte & Touche LLP acting separately, whose reports have been furnished to us, and our opinion, insofar as it relates to the amounts included for those component units and agencies, is based solely upon the reports of other auditors. Deloitte & Touche LLP acting separately has examined 100% and 100% of the total assets and other debits and total revenues, respectively, of the Investment Trust Fund. The Office of the State Auditor acting separately has examined 31% and 35% of the total assets and other debits and total revenues, respectively, of the Higher Education Funds. Except as discussed in the first sentence, we conducted our audit in accordance with generally accepted auditing standards and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

The Honorable James H. Hodges, Governor  
and  
Members of the General Assembly  
State of South Carolina

### Compliance

As part of obtaining reasonable assurance about whether the State of South Carolina's general purpose financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grants, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards*.

### Internal Control over Financial Reporting

In planning and performing our audit, we considered the State of South Carolina's internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing our opinion on the general purpose financial statements and not to provide assurance on the internal control over financial reporting. However, we noted certain matters involving the internal control over financial reporting and its operation that we consider to be reportable conditions. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of the internal control over financial reporting that, in our judgment, could adversely affect the State of South Carolina's ability to record, process, summarize, and report financial data consistent with the assertions of management in the general purpose financial statements. Reportable conditions are described on pages 3 and 4 of this report.

A material weakness is a condition in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts that would be material in relation to the general purpose financial statements being audited may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Our consideration of the internal control over financial reporting would not necessarily disclose all matters in the internal control that might be reportable conditions and, accordingly, would not necessarily disclose all reportable conditions that are also considered to be material weaknesses. However, we believe that none of the reportable conditions described above is a material weakness.

We also noted other matters involving the internal control over financial reporting that are described on pages 5 to 10 of this report.

This report is intended solely for the information and use of the State of South Carolina, the cognizant audit agency, and other federal and state agencies and is not intended to be and should not be used by anyone other than these specified parties.

Columbia, South Carolina  
December 2, 1998

Columbia, South Carolina  
December 2, 1998

**REPORTABLE CONDITIONS**

## **GAAP CLOSING PACKAGES**

The Office of the Comptroller General (Comptroller General) obtains certain generally accepted accounting principles (GAAP) information from agency prepared closing packages to prepare the State's general purpose financial statements. Section 1.8 of the Comptroller General's GAAP Closing Procedures Manual requires that each agency's executive director and finance director accept responsibility for submitting closing package forms that are accurate, complete and prepared in accordance with instructions. The quality of the information agencies submit through the closing package process directly affects the quality of the State's general purpose financial statements and other information included in the State's Comprehensive Annual Financial Report. Therefore, it is essential that closing package information be accurate, complete and submitted to the Comptroller General in a timely manner.

The following is a summary of closing package errors and internal control weaknesses noted during the audit of the general purpose financial statements. Adjustments were made to the general purpose financial statements to correct the closing package errors.

### **Fixed Assets**

#### **Archives and History**

The agency constructed a new building, which was completed and occupied by April 1998. However, the agency did not reclassify the remaining construction in progress to buildings and improvements. This error resulted in an understatement of buildings and improvements and overstatement of construction in progress.

See agency response at page 11.

#### **Department of Corrections**

The Department reported retainage payable of \$498,905 as outstanding construction commitments. As a result, outstanding construction commitments were overstated by \$498,905.

See agency response at page 12.

### **Grants and Entitlements**

#### **Department of Health and Environmental Control**

The agency did not include certain estimated Women, Infants, and Children (WIC) payables on the grants analysis worksheet. As a result, deferred revenue was overstated.

See agency response at page 13.

#### **Department of Health and Human Services**

The agency reported non-grant funds relating to admission tax and investment earnings on bingo on the closing package as federal contributions, donations, and awards.

The agency did not report estimated medicaid accounts receivable for the prior fiscal years ended 1996 and 1997 on the grants and entitlements closing package. These omissions resulted in an understatement of accounts receivable and federal revenues for both fiscal years.

See agency response at page 14.

## **RECOMMENDATIONS**

Agencies must ensure that GAAP closing packages are prepared and completed in accordance with the Comptroller General's GAAP Closing Procedures Manual instructions. Therefore, we recommend agencies implement procedures to ensure that employees responsible for completing and reviewing the closing packages are knowledgeable about GAAP and familiar with closing package instructions. In reviewing closing packages for completion in accordance with the GAAP Closing Procedures Manual instructions, the reviewer should trace closing package amounts to source documentation. Proper review reduces the potential for errors and omissions and increases the efficiency of the closing package process. We also recommend that when agencies have questions pertaining to closing package instructions or have difficulty completing the closing packages, they contact the Office of the Comptroller General – Central State Finance Division.

**OTHER MATTERS**

## **RECONCILIATIONS**

The purpose of the statewide joint audit of the State is to ascertain whether the general purpose financial statements of the State of South Carolina have been presented fairly in accordance with generally accepted accounting principles (GAAP) and whether the State has complied with laws and regulations that may have a material effect on the general purpose financial statements. As part of this process, agencies are required to maintain complete and accurate records supporting the financial activities processed through the Statewide Accounting and Reporting System (STARS) and the closing packages they submit. Section 2.1.7.20.C of the STARS manual states "Monthly reconciliations for revenues, expenditures and ending cash balances must be performed..." The STARS reports generally used to perform the reconciliations include the General Fund Control and Cash Status Report (CSA 404CR), Statement of Estimated and Actual Revenue (CSA 406CR), and Summary of Expenditures – by Object (CSA 424CM). In addition, Section 2.1.7.20.C requires agencies with federal funds to perform monthly reconciliations of the CSA 467CM (Trial Balance by Subfund, Project, and GLA).

### **Department of Social Services**

The Department does not reconcile its accounting records to the CSA 467CM report for some of its federal programs. In response to a prior year management letter comment (FY1995) the Department implemented procedures to ensure that its five largest federal programs were reconciled monthly. However, the Department is not performing timely reconciliations for all other federal programs.

We recommend the Department prepare monthly reconciliations of agency accounting records to the STARS reports in a timely manner. The reconciliations should be documented in writing in an easily understandable format with all supporting working papers maintained for audit purposes with the signatures of the preparer and reviewer and the dates of preparation and review. The reconciliations of parallel systems assures that transactions are accurately processed by both the agency and the Office of the Comptroller General, strengthens the internal accounting controls for both the agency and the State, and assures proper classification of transactions presented in the State's general purpose financial statements.

See agency response at page 15.

## DATA PROCESSING

### Access to System Resources

#### **Budget and Control Board - Division of Operations - Office of Information Resources**

Unauthorized or unintentional changes to production data or programs could occur due to an excessive number of individuals having special security privileges. Specifically, we noted that 31 individuals retain full access (SYSTEM SPECIAL) and 37 individuals retain group designated full access (GROUP SPECIAL) within the security access software (RACF).

The SPECIAL attribute gives the user the ability to define, modify, list, and delete resources (e.g. users, groups, data and program files). A user with the SPECIAL attribute can perform changes to databases through security (RACF) commands, but should not have direct update capability to these files. A user with the SPECIAL attribute can assign any user attribute (including the SPECIAL user attribute) to other RACF-defined users. Although users with the SPECIAL attribute do not have automatic access to data sets and general resources, they have the ability to grant themselves such access. The SYSTEM SPECIAL attribute can be used to access user profiles, group profiles, data, and program files for any of the agencies processed on the mainframe at the Office of Information Resources. The GROUP SPECIAL attribute limits the user to access user profiles, group profiles, data, and program files for resources defined to the associated group.

Special privileges which allow security administration capabilities should be limited to individuals with security administration responsibilities. In general, this is the primary security administrator and a back-up. As such, the risk of unauthorized or unintentional changes is reduced.

We recommend that the SYSTEM SPECIAL and GROUP SPECIAL attributes be limited to primary and back-up security administrators and technical support personnel. Specifically,

- The SYSTEM SPECIAL privilege should be limited to the primary RACF security and technical support teams with overall responsibility for the mainframe environment and the RACF security product, and
- The GROUP SPECIAL privilege should be limited to agency security teams.

As a result, agencies will be unable to access other agencies' resources, and unauthorized or unintentional changes to programs or key data will be limited.

See agency response at pages 16 to 18.

#### **Office of Information Resources – Financial Data Services**

Unauthorized or unintentional changes to production resources for the Comptroller General's Office could occur as security restrictions are inappropriate. Specifically, we noted the following:

- Three programmers have the ability to perform Group Security Administration functions for their department which allow each of them to set up new users and change user profiles within their department. This combination of access does not create compatible job responsibilities. Specifically, these individuals have the ability to make changes to group resources (e.g. program code and data) without detection.

- Several individuals have inappropriate access to perform sensitive CICS transactions (e.g. CEMT and CECL) within RACF.
- Password configuration standards are not set to ensure new passwords are created on a periodic basis. Per discussions with IT personnel, the password history is not maintained as users would continue to enter new passwords until they could enter the old password anyway thus circumventing the control. It should be noted that this behavior is in direct violation with the security policy and should be communicated as such.
- Periodic reviews of application security are currently not being performed. As a result, users may retain inappropriate access to perform sensitive transactions without being detected.

To ensure that unauthorized or unintentional changes to production resources do not occur, consider the following:

- Perform a periodic review of users with RACF Group Security Administration (Group Special) access to ensure that users with the ability to perform this function are appropriate. Restrict programmers from performing security administration functions, as this creates incompatible job responsibilities. Departmental managers should assign a capable employee in their department, without programming responsibilities, to perform the security administration function.
- Perform a periodic review of users with the capability to perform key management CICS transactions to ensure appropriateness.
- Enable the parameter in RACF that maintains password history. Users would then be required to choose a password different from the password previously used.
- Periodically distribute a list to each department detailing individuals with access to key data and transactions. Request that department managers review the listing and indicate the appropriateness of each user's access.

See agency response at pages 16 to 18.

### **Disaster Recovery/Business Continuity**

#### **Budget and Control Board – Division of Operations - Office of Information Resources**

The Office of Information Resources (OIR) has developed a statewide disaster recovery plan to be used by all agencies supported by OIR and its affiliates. However, this plan has not been updated or tested in several years.

Per review of the statewide disaster recovery plan, the following concerns were noted:

- The plan includes teams with representatives from OIR for dealing with each aspect of a disaster. However, the teams do not include representatives from any of the agencies relying on the plan.
- The plan does not include detailed descriptions for what each team is responsible for in the event of a disaster.

- The plan does not include a detailed list of critical hardware and software or an indication of the priority for restoring platforms and applications.
- There are no procedures governing how and when the plan will be updated.
- There are no agency business continuity considerations indicating user input from the agencies relying on the plan.

During our review, we noted that OIR is in the process of consolidating the data centers for all State agencies into one central processing site. OIR has indicated that at the time of consolidation, a new comprehensive disaster recovery plan will be developed and tested on an annual basis. However, until then, a disaster at the State may result in data processing systems being unavailable for an extended period of time. Additionally, the agencies we reviewed (Comptroller General's Office, Treasurer's Office, and Department of Revenue) do not have up-to-date, customized business continuity plans that are compatible with the statewide disaster recovery plan. Business continuity is the ultimate responsibility of each individual agency.

As the data centers are consolidated for the state agencies, consider implementing and testing a disaster recovery/business continuity plan which:

- Includes a formal Business Impact Assessment, conducted by senior user and IS management, to determine the critical systems to be protected, and the associated information resources that need to be safeguarded by contingency plans.
- Ensures the key data processing applications can be restored within a period of time that does not result in significant interruptions to the operations of the State.
- Prioritizes the recovery of the State's application systems in accordance with importance to continued business operations.
- Identifies the resources necessary for recovery. Resources should include people, as well as terminals, personal computers, calculators, printers, desks, chairs, and office supplies.
- Documents the manual processes that need to be maintained during the outage to ensure that application data integrity can be reinstated and synchronized once the systems are recovered and operational.

In the interim, each agency should ensure that the current disaster recovery and business continuity plan is tested and updated based on those tests. The development of a strong, cohesive disaster recovery/business continuity plan is an on-going effort that takes a substantial amount of time and resources. As the new consolidated data center and its recovery plans are being developed, it is imperative that the State still protect itself against a disaster.

See agency response at pages 16 to 18.

## **Information Security Policy**

### **Office of the State Treasurer**

During our review of information security for the Office of the State Treasurer, we noted that a formal information security policy has not been developed. There are limited policies and procedures in place addressing certain aspects of security, however, no comprehensive security policy has been developed and distributed to users in the Treasurer's Office. As a result, responsibilities for information security may not be established or may not be adequately communicated to all employees.

In order to ensure that important business systems are reasonably protected from potential exposures, information security policies and procedures should be developed and communicated to all personnel. An effective written information security policy is important to ensure that information systems' resources are effectively secured according to the degree of related risk. Accompanying procedures are also necessary to ensure security controls are implemented according to management's objectives, and are applied consistently and effectively.

A comprehensive information security policy and accompanying procedures should be established and communicated to all employees. At a minimum, the policy should contain the overall approach to security and specific policies and procedures. In developing the policy, consider the following:

- Types and uses of all system resources and classification according to importance and sensitivity.
- Employee education and communication of the security policy.
- Assignment of responsibility for maintaining and enforcing security administrative procedures.
- Procedures for ensuring the confidentiality of sensitive information.
- Definition of user responsibilities for the information used and processed.
- Written management approval for granting access authorities.
- Limitations on special authorities based on defined business needs.
- Provisions for timely modification to employee access after termination or transfer.
- Password structure, format and usage guidelines.
- Periodic review of security violations.
- Security expectations for personal computer systems.

See agency response at page 19.

## **Notification of Terminated or Transferred Employees**

### **Department of Revenue**

During our review of security access rights at the Department of Revenue, we noted that there are no formal procedures in place for notifying the security administrator when a user terminates employment or transfers to another department or agency. The security administrator is either notified by phone that employees have terminated employment or transferred, or he learns that access must be modified when the users request access based on their new positions. As a result, unauthorized or inappropriate access could occur by transferred or terminated personnel.

Implement a procedure, which ensures that transferred or terminated employee access is removed in a timely manner. Consider the following:

- Generate a list of terminated and/or transferred employees from the Human Resources or Payroll system. Distribute the listing to all security administrators to ensure that access is removed or modified, accordingly.

Alternatively, forward a duplicate copy of the separation notification generated at the agency level for all terminated or transferred employees. Distribute this copy to all security administrators to ensure that access is removed or modified, accordingly.

- Generate a list of each employee's access by application system on a periodic basis (e.g. monthly). Distribute this listing for review to user management to ensure that all users with access to a particular application/transaction require such access based on his/her job responsibilities.

See agency response at page 20.

## **SUMMARY OF PRIOR YEAR FINDINGS**

The findings included in the prior year report on compliance and on internal control over financial reporting at the general purpose financial statement level issued by the joint audit team were reviewed to determine if the conditions still existed. Based on our audit procedures we determined that the finding related to the "Reconciliations – Department of Social Services" had not been corrected. Therefore, we have repeated the finding in the "Other Matters" section of this report on page 5.

**MANAGEMENTS' RESPONSES**

**SOUTH CAROLINA DEPARTMENT OF ARCHIVES & HISTORY**

December 29, 1998

Mr. Rich Gilbert, CPA  
Audit Manager  
Office of the State Auditor  
P.O. Box 11333  
Columbia, SC 29211

Dear Mr. Gilbert:

I am replying to your fax of December 22 regarding the GAPP closing package for the Department of Archives and History. Your findings indicated that we incorrectly listed our new building as construction in progress rather than buildings and improvements.

On June 30, 1998, the closing date on the GAPP information, the new Archives and History Center was not substantially complete. We did not receive a certificate of substantial completion until July 13, 1998. Therefore, utilizing the definition in the GAPP closing manual, we determined that on June 30 the building was not officially substantially complete and should be classified as construction in progress.

Sincerely,

Rodger E. Stroup  
Director

# SOUTH CAROLINA DEPARTMENT OF CORRECTIONS

January 8, 1999

Mr. Rich Gilbert  
Office of the State Auditor  
Suite 1200  
1401 Main Street  
Columbia, SC 29201

Dear Mr. Gilbert:

I have reviewed the GAAP Closing Package audit comment regarding Fixed Assets and offer the following response:

## **Audit Comment**

### **Fixed Assets**

The Department reported retainage payable of \$498,905 as an outstanding construction commitment. As a result, outstanding construction commitments were over stated by \$498,905.

### **Recommendation**

The auditor recommends that we implement procedures to ensure that employees responsible for completing and reviewing the closing packages are knowledgeable about GAAP and familiar with closing package instructions.

### **Response**

The Financial Accounting Branch of the South Carolina Department of Corrections will review the findings and the GAAP Closing Package Procedures Manual with the staff responsible for this error. In addition, we will establish training on the GAAP Closing Package Procedures Manual for all staff involved with the GAAP Closing Package process.

If you have any questions regarding this matter, please call me at (803) 896-1916.

Sincerely,

Bruce Burnett

**SOUTH CAROLINA DEPARTMENT OF HEALTH AND ENVIRONMENTAL CONTROL**

January 12, 1999

Mr. Rich Gilbert, CPA  
State Auditors Office  
1401 Main Street, Suite 1200  
Columbia, SC 29201

Dear Mr. Gilbert:

In response to the Management Letter Comment on the Fiscal Year 1998 Grants and Entitlement Closing Package, we offer the following:

We agree that the closing package, as originally submitted, did not include the additional WIC payables, which are estimated. However, we communicated that to the auditor in mid October and asked if we needed to submit an updated closing package or just have the corrections made per our conversation. The direction given to us was to just update our Agency copy and they would do the same. Therefore, while we feel that the closing package was not submitted accurately by the due date, the necessary amendments were communicated expeditiously and should not have resulted in a finding of omission.

If you have any questions, please feel free to call Mr. Tommy Watson at (803) 898-3425.

Sincerely,

R. Douglas Calvert  
Chief Operating Officer

**SOUTH CAROLINA DEPARTMENT OF HEALTH AND HUMAN SERVICES**

January 21, 1999

Mr. Rich M. Gilbert  
Director of State Audits  
State Auditor's Office  
1401 Main Street, Suite 1200  
Columbia, SC 29201

Dear Rich:

I have reviewed the attached reportable conditions associated with our agency's GAAP closing package and agree with your findings and recommendations. We have taken steps to ensure that closing packages are properly prepared and reviewed in accordance with Comptroller General procedures.

Sincerely,

Robert M. Kerr, CPA  
Chief, Bureau of Fiscal Affairs

G:\USERS\KERR\WP51\GAAP Audit.wpd

**SOUTH CAROLINA DEPARTMENT OF SOCIAL SERVICES**

January 7, 1999

Richard H. Gilbert  
Office of the State Auditor  
1401 Main Street, Suite 1200  
Columbia, SC 29211

Dear Mr. Gilbert:

This is the Department of Social Services response to the State of South Carolina statewide joint audit of the general purpose financial statements, relating to the FY 1997-98 GAAP financial packages submitted by the Department.

Reconciliation related finding: The Department does not reconcile its accounting records to the CSA467CM report for some of its federal programs.

Response: The Department has taken steps to implement procedures to timely prepare reconciliations for the twenty-seven (27) federal grants that the Department administered in FY 1997-98. This currently involves electronic spreadsheets which should be upgraded to an automated process in FY 1998-99.

Sincerely,

Morgan F. Denny  
Deputy State Director  
Fiscal and Administrative Management

MFD:wgk

fileWordPro\Letters\Gilbert1

**STATE OF SOUTH CAROLINA  
STATE BUDGET AND CONTROL BOARD**

January 19, 1999

Rich Gilbert  
Office of the State Auditor  
1401 Main Street, Suite 1200  
Columbia, SC 29201

Dear Mr. Gilbert:

Thank you for your comments from your Internal Controls review of the Budget and Control Board for the year ended June 30, 1998. We have enclosed our responses.

Yours truly,

Luther F. Carter  
Executive Director

Enclosure

## **DATA PROCESSING**

### **Access to System Resources - Office of Information Resources**

Response:

The observation stated a concern over the number of RACF userids which had SYSTEM SPECIAL and GROUP SPECIAL access.

- The 31 userids with SYSTEM SPECIAL are used by 16 individual technical support users. Most technical support personnel have multiple userids for accessing multiple systems simultaneously for system testing, troubleshooting problems, etc. Technical support staff do not share single userids so all access is accountable to an individual user. Technical support needs authority to reset passwords, to resolve problems when being on call and to back up other staff members.
- Of the 37 userids with GROUP SPECIAL, 31 userids are for other state agencies that administer their own RACF. They must have authority to reset passwords for their agency's users and perform other RACF functions as needed for their agency. The remaining 6 userids with GROUP SPECIAL consist of 2 userids for performing applications DBA functions with the remaining 4 userids for batch processing of financial applications.

The technical support staff daily monitors RACF functions performed and violations that occur. We will continue to periodically review our userids with SYSTEM SPECIAL and GROUP SPECIAL and remove the authority if it is no longer needed.

### **Access to System Resources - Financial Data Systems**

Response:

1. The technical support person for Financial Data Systems will begin to do periodic reviews with the user agencies to ensure they are aware of the individuals able to perform these functions. Department Managers in offices such as the Comptroller General and the State Treasurer will have to make decisions on who is allowed to perform their security administration functions.
2. This is again an area where we will institute regular reviews with the user to ensure the appropriate access level of individuals.
3. Financial Data Systems will begin discussions with the user agencies about this topic. We will need to determine an appropriate time frame to begin using password history function of RACF.
4. Some agencies in the past have not felt this was necessary in their environment, but

Financial Data Systems will offer this type of list to the user agencies. The agencies will need to help us specify what their key data and transactions are, so they have a workable list to use when reviewing.

### **Disaster Recovery/Business Continuity**

Response:

The Office of Information Resources (OIR) is currently involved in a Data Center Consolidation effort (9 agencies). The current (OIR) Data Center has UPS and emergency generator power capabilities. The new Data Center will also have a UPS system and emergency generator power with enough fuel to operate for five days. While in the process of creating the Disaster Recovery Plan for the Consolidated Data Center, OIR will consider your recommendations.

**STATE OF SOUTH CAROLINA  
OFFICE OF THE STATE TREASURER**

**Treasurer's Office**

**Information Security Policy**

**Management Response:**

The State Treasurer's Office does have in place several policies and procedures that address computer use by employees. We agree with your observation that there is not a dedicated formal information security policy. Accordingly, we agree with your recommendation to establish a comprehensive information security policy that is communicated to all new and current State Treasurer's Office employees.

We are in the process of drafting the initial policy, which will address the issues you suggested in your observation. In addition, any other concerns that come to our attention as we review information security will be added to this policy. Upon finalizing this policy, we will begin immediate communication to all current employees for them to review and sign. A copy of this document will be maintained in individual personnel files.

**STATE OF SOUTH CAROLINA  
DEPARTMENT OF REVENUE**

Thomas L. Wagner, Jr.  
Office of the State Auditor,  
1401 Main Street, Suite 1200  
Columbia, SC 29201  
January 20, 1999

Dear Mr. Wagner,

In response to the audit finding by Deloitte & Touche, regarding the lack of formal procedures for notifying the Security Administrator when a user terminates employment or transfers to another agency, the following procedure was implemented in the Department of Revenue on November 13, 1998.

The DOR Human Resources Office accesses the DOR Agency Termination Report on a daily basis and informs the Security Administrator, via E-mail, of all departed employees. The Security Administrator removes the departed employees' security accesses on a daily basis. To ensure no departed employee has been overlooked, Human Resources additionally accesses the DOR Agency Termination report at the end of each pay period and provides the names of all departed employees for that pay period to the Security Administrator, who verifies that all security accesses were appropriately terminated.

If you have any further questions regarding this matter, please contact Ken Clark, at (803) 898-5591.

Sincerely,

Ike A. Nooe, Administrator  
IRM Division

copy: Elizabeth A. Carpentier, Director  
E. Gregorie Frampton, Executive Administrator