• This report and any related follow-up correspondence are available to the public. Alternate formats may also be requested by contacting the Office of Legislative Audits as indicated at the bottom of the next page or through the Maryland Relay Service at 1-800-735-2258.

• Please address specific inquiries regarding this report to the Audit Manager listed on the inside back cover by telephone at (410) 946-5900.

• Electronic copies of our audit reports can be viewed or downloaded from the Internet via http://www.ola.state.md.us.

• The Department of Legislative Services – Office of the Executive Director, 90 State Circle, Annapolis, Maryland 21401 can also assist you in obtaining copies of our reports and related correspondence. The Department may be contacted by telephone at (410) 946-5400 or (301) 970-5400.
March 17, 2003

Delegate Van T. Mitchell, Co-Chair, Joint Audit Committee
Senator Nathaniel J. McFadden, Co-Chair, Joint Audit Committee
Members of Joint Audit Committee
Annapolis, Maryland

Ladies and Gentlemen:

We have audited the centralized operations of the Financial Management Information System (FMIS) as administered by the Department of Budget and Management’s Application Systems Management (ASM) Division and the Comptroller of the Treasury’s General Accounting Division for the period beginning January 1, 1998 and ending May 31, 2002. The System is used to support the State’s purchasing, accounting and payment functions. Expenditures recorded in FMIS for fiscal year 2002 totaled in excess of $24 billion.

Our audit disclosed that FMIS contained many essential internal controls that were functioning properly. However, our audit also disclosed certain weaknesses that reduced the effectiveness of the System’s internal controls. For example, we found that access to certain critical FMIS program files was not properly restricted or recorded. In addition, a number of State employees were assigned incompatible FMIS security duties.

Respectfully submitted,

Bruce A. Myers, CPA
Legislative Auditor
Table of Contents

Executive Summary 5

Background Information
   General Information 7
   Control Agencies’ Responsibilities 7
   FMIS Interfaces 8
   Current Status of Findings From Preceding Audit Report 8

Findings and Recommendations

FMIS Access Controls
   * Finding 1 – Modification Access to Program Files Supporting Online 9
     FMIS Processing Was Not Adequately Recorded or Restricted
   * Finding 2 – Reviews of FMIS Security Access Reports Were Not 10
     Performed by Independent Employees and Certain Other Security
     Reports Were Not Received or Reviewed

Assignment of Users’ Security Privileges
     FMIS Access Were Not Properly Segregated
   * Finding 4 – Central Security Officers Could Grant Themselves 12
     Unauthorized R*STARS Access

R*STARS
   * Finding 5 – R*STARS Control Profile Maintenance Procedures Were 13
     Not Adequate
   * Finding 6 – Unnecessary Modification Access to Critical R*STARS 13
     Control Profiles Was Provided

Ad-Hoc FMIS Database
   * Finding 7 – Assurance Was Lacking that the R*STARS Portion of the 14
     Separate Ad-Hoc Database Used by State Agencies for
     Supplemental Reporting Was Accurate

Audit Scope, Objectives, and Methodology 15

Auditees’ Responses  Appendix

* Denotes item repeated in full or part from preceding audit report.
Executive Summary

Legislative Audit Report on
Financial Management Information System Centralized Operations
March 2003

The Financial Management Information System (FMIS) is an integrated database system used to support the State’s purchasing, accounting and payment functions. The integration of procurement and accounting processing within FMIS results in the Department of Budget and Management and the Comptroller of the Treasury having responsibility for separate aspects of the System. Expenditures recorded in FMIS for fiscal year 2002 totaled in excess of $24 billion. Significant findings as a result of our audit are as follows:

- **Fifty-five individuals had unnecessary and unlogged modification access to the program files that supported FMIS online processing.**

  Modification access to critical program files should be limited to users whose job responsibilities require such access and such access should be recorded for security reporting purposes.

- **The security reports of changes to FMIS access rules were reviewed for propriety by the same individuals who initiated the changes, and reports of changes to userids were not received for review.**

  All FMIS security reports should be received and reviewed by independent personnel.

- **A number of State employees were assigned incompatible security duties.**

  A proper segregation of employee duties should be established.

- **Adequate controls were not established over the procedures for processing changes to control files containing critical accounting system software processing rules and business logic.**

  Change control procedures over these control files should be strengthened.
Background Information

General Information

The Financial Management Information System (FMIS) is an integrated database system with purchasing and accounting components. The System’s purchasing and accounting components are operational in virtually all Executive Branch agencies with the exception of the University System of Maryland. In addition, the Maryland Department of Transportation (MDOT) maintains its own version of FMIS, which is not included in the scope of this audit. The System runs on the Comptroller of the Treasury’s Annapolis Data Center’s computers and supports individual agency and statewide purchasing and accounting operations. Expenditures processed through and/or recorded in FMIS for fiscal year 2002 totaled in excess of $24 billion.

Control Agencies’ Responsibilities

The FMIS supports purchasing functions through the Advanced Purchasing and Inventory Control System (ADPICS) component and supports the accounting operations through the Relational Standard Accounting and Reporting System (R*STARS) component. The integration of procurement and accounting processing within FMIS results in two primary control agencies (that is, the Department of Budget and Management and the Comptroller of the Treasury) having responsibility for separate aspects of the System. These control agencies have statutory responsibility for oversight of the State’s purchasing and accounting related operations.

Specifically, the Application Systems Management (ASM) Division of the Department of Budget and Management’s Office of Information Technology is responsible for daily System administration, including maintenance, operation, security and back-up of related database records and the computer programs which perform on-line and overnight processing. The Comptroller of the Treasury’s General Accounting Division is primarily responsible for R*STARS operations, security and reporting.

The Department of Budget and Management (including the Office of Information Technology) and the Comptroller of the Treasury’s General Accounting Division are separately audited by the Office of Legislative Audits. Our most recent audits of these entities included a review of their agency-specific FMIS responsibilities. This audit of the centralized System operations included elements of FMIS operations relative to the State’s overall internal control structure not included in
the aforementioned agency audits (for example, database and security controls). For an expanded explanation of the nature and purpose of this audit, see the Audit Scope, Objectives and Methodology section of this report.

**FMIS Interfaces**

Because of unique requirements, certain State agencies process procurement, disbursement and financial information on in-house computer systems that interface certain financial information to FMIS for recordation, payment processing and reporting. The Judiciary and the University System of Maryland are the two largest entities operating internal systems that interface to FMIS. An additional interface entity is MDOT, which operates its own customized version of FMIS. With respect to interfaced data, our centralized audit included a review of the controls and processing of such data from the point of interface to FMIS through transaction processing and recordation.

**Current Status of Findings From Preceding Audit Report**

Our audit included a review to determine the current status of the fifteen fiscal/compliance findings included in our preceding audit report dated December 3, 1998. We determined that the Divisions satisfactorily addressed eight of these findings. The remaining seven findings are repeated in this report. In their responses to our preceding audit report, the Divisions generally agreed to implement the recommendations related to those findings.
Findings and Recommendations

FMIS Access Controls

Background
The significance of the data maintained in the FMIS database and the magnitude of the expenditures and revenues processed through FMIS necessitates that access to the data and related FMIS programs be adequately restricted. In addition, all unauthorized attempted accesses, changes to userid settings and to the rules governing system access, and certain allowed accesses should be recorded (that is, logged) for subsequent independent review. Critical FMIS data and program files on the Annapolis Data Center’s computer can be modified using different tools and by on-line transaction screens. FMIS file access control is provided by use of the Data Center’s security software product (ACF2) and its database management software (DB2), and FMIS application program controls.

Finding 1
Modification access to program files supporting online FMIS processing was not adequately recorded or restricted.

Analysis
Modification access to the program files supporting online FMIS processing was not properly controlled. Specifically, until we brought this to management’s attention during the audit, 55 individuals had unnecessary and unlogged modification access to these program files. As a result, erroneous or improper changes could be made to these files without detection by management. A similar condition was commented upon in our preceding audit report.

Recommendation 1
We again recommend that the ASM Division of the Department of Budget and Management monitor to ensure that modification access to critical program files is granted only to users whose job responsibilities require such access, and ensure that such access is recorded for security reporting purposes.
**Finding 2**

Reviews of FMIS security access reports were not performed by independent employees and certain other security reports were not received for review.

**Analysis**

The Annapolis Data Center’s security system’s (ACF2) reports of changes to FMIS access rules were reviewed for propriety by the same individuals who initiated the changes. Furthermore, until we brought this to management’s attention during the audit, ACF2 reports of changes to userid settings were not received by the ASM Division for review. As a result, erroneous or improper changes could be made to these access rules and userid settings, including the possibility of ASM security officers granting themselves improper access to FMIS information, without detection by management. A similar condition regarding the inadequate review of security reports was commented upon in our preceding audit report.

**Recommendation 2**

We again recommend that the ASM Division of the Department of Budget and Management receive all FMIS related ACF2 reports for review. Also, we again recommend that all such reports be reviewed by persons independent of the related transactions and that these reviews be documented.

**Assignment of Users’ Security Privileges**

**Background**

The purchasing and accounting segments of the FMIS include over 400 on-line screens for inquiry, entry or modification of data. Initial employee access and subsequent changes to access capabilities are obtained via request forms that are completed and approved by designated agency personnel who are responsible for FMIS coordination, security and access to the Annapolis Data Center. Statewide FMIS security officers in the ASM Division and the General Accounting Division evaluate agency FMIS access requests for general propriety and verify that the requests contain the required agency authorizations. FMIS access is established by the ASM Division and the General Accounting Division, and periodic reports of employee FMIS access are provided to State agencies for review and evaluation.
Finding 3
FMIS security designations, which granted agency personnel FMIS access, were not properly segregated.

Analysis
Eighteen employees in thirteen State agencies could render all of the approvals necessary to assign security privileges to employees of their respective agencies. Specifically, these individuals were responsible for coordinating their agency’s FMIS operations (referred to as the ASM Functional Coordinator), reviewing and requesting agency employee FMIS security settings (ASM Security officer), and creating mainframe userids and assigning overall mainframe access rights (Annapolis Data Center Security Officer). As a result, these 18 employees could either create fictitious users or amend their own security privileges to enable them to process unauthorized transactions through the System. In addition, these same employees were responsible for reviewing periodic reports to verify the propriety of the user privileges assigned by the ASM Division.

The ASM Internal Control and Security Policy and Procedures manual requires that the duties of the ASM Functional Coordinator and the ASM Security Officer be separated. However, no guidance had been provided to State agencies recommending that the aforementioned duties also be separate from that of the Annapolis Data Center Security Officer duties. Similar conditions were commented upon in our preceding audit report.

Recommendation 3
We again recommend that the ASM Division of the Department of Budget and Management, in conjunction with the aforementioned 13 agencies, ensure that an adequate segregation of FMIS and ACF2 duties is accomplished. We also again recommend that the ASM Internal Control and Security Policy and Procedures manual be amended to recommend that the duties of the ASM Functional Coordinator and the ASM Security Officer be separate from that of the Annapolis Data Center Security Officer to accomplish an adequate segregation of duties.
Finding 4
Central security officers could grant themselves unauthorized R*STARS access.

Analysis
Three General Accounting Division security officers could modify their own R*STARS access rights. Accordingly, these security officers could grant themselves improper security privileges and process unauthorized transactions, including disbursements through the System. The ADPICS software precluded ADPICS security officers from modifying their own userids and access rights. However, a similar restriction did not exist within the R*STARS software. In addition, one of these employees was responsible for reviewing periodic reports to verify the propriety of changes to R*STARS access rights. Similar conditions were commented upon in our preceding audit report.

Recommendation 4
We again recommend that the capabilities of the central R*STARS security officers be restricted to preclude them from being able to modify their own R*STARS access rights.

R*STARS

Background
The Relational Standard Accounting and Reporting System (R*STARS) is a comprehensive financial management information system designed to meet the accounting and reporting needs of all state agencies. State R*STARS processing rules and business logic are defined within separate control profiles (tables) to facilitate prompt online changes as the State’s financial and operational requirements change. These control profiles permit rapid adjustment of R*STARS via online screens. Access to these screens is controlled by users’ R*STARS security settings. R*STARS profiles control a wide range of critical processes related to budgetary control, security, error and vendor payment processing, reporting and overall system management. The General Accounting Division maintains most critical R*STARS profiles. We identified 29 critical R*STARS profiles which have significant internal control, reporting and system management considerations because they impact the reliability and integrity of critical System functions.
Finding 5
R*STARS control profile maintenance procedures were not adequate.

Analysis
The procedures for processing changes to the aforementioned 29 critical R*STARS control profiles were not adequate. Specifically, independent, documented verifications of changes made to the profiles to requested changes were not performed. Furthermore, some profile changes, prompted by user agencies, were not documented. The State’s R*STARS application vendor cites control of profile maintenance transactions as being critical for ensuring the integrity of the State’s accounting structure and the information produced by R*STARS. Similar conditions were commented upon in our preceding audit report.

Recommendation 5
We again recommend that the basis for any change to critical R*STARS control profiles be documented. We also again recommend that employees independent of the control profile maintenance process compare all changes made to these profiles to this documentation and retain evidence of these comparisons.

Finding 6
Unnecessary modification access to critical R*STARS control profiles was provided.

Analysis
Several General Accounting Division employees had unnecessary modification access to 12 of the aforementioned 29 critical R*STARS control profiles. For example, two employees could modify the R*STARS transaction code profile table, which defines all transaction posting rules even though these employees did not need this capability. Unauthorized changes to critical R*STARS control profiles could result in erroneous data and could compromise R*STARS System integrity. A similar condition was commented upon in our preceding audit report.

Recommendation 6
We again recommend that modification access to critical R*STARS control profiles be limited to individuals requiring such access and that this access be periodically reassessed relative to users' job responsibilities.
Ad-Hoc FMIS Database

Finding 7
Assurance was lacking that the R*STARS portion of the separate Ad-Hoc database used by State agencies for supplemental reporting was accurate.

Analysis
Assurance was lacking as to the accuracy of the R*STARS portion of the Ad-Hoc database used by State agencies to supplement the reporting capabilities of the FMIS standard reports. State agencies can generate FMIS reports using the Ad-Hoc database (which is a separate copy of selected items from the FMIS production database) in addition to the standard preformatted reports available from the FMIS production database. The ASM Division is responsible for statewide reconciliations of the FMIS production database to the Ad-Hoc database, to ensure the integrity of the Ad-Hoc database. However, our review of this reconciliation process disclosed that reconciliation reports of R*STARS data from the production database to the Ad-Hoc database were only generated for one State agency. A similar condition was commented upon in our preceding audit report.

Recommendation 7
We again recommend that complete reconciliations of the R*STARS production database to the related Ad-Hoc database be periodically performed (for example, weekly) for all State agencies. Until complete reconciliations are performed, the ASM Division of the Department of Budget and Management should advise State agencies of the risk associated in using the Ad-Hoc database.
Audit Scope, Objectives, and Methodology

We have audited the centralized operations of the Financial Management Information System (FMIS) for the period beginning January 1, 1998 and ending May 31, 2002. The audit was conducted in accordance with generally accepted government auditing standards.

The integration of procurement and accounting processing within FMIS results in two primary control agencies (that is, the Department of Budget and Management and the Comptroller of the Treasury) having responsibility for separate aspects of the System since these control agencies have statutory responsibility for oversight of the State’s purchasing and accounting operations. In addition, FMIS is a vital procurement and/or accounting application in virtually all State agencies. Therefore, internal control over FMIS is critical to the user agencies. Since we are responsible for auditing these agencies and evaluating their internal control structures, we periodically evaluate FMIS’s internal control structure.

As prescribed by the State Government Article, Section 2-1221 of the Annotated Code of Maryland, the objectives of this audit were to examine the elements of FMIS operations, relative to the State’s overall internal control structure (for example, database and security controls) and compliance with applicable State laws, rules and regulations not included in our individual audits of the aforementioned control agencies. We also determined the current status of the findings contained in our preceding audit report.

In planning and conducting our audit, we focused on the major financial related areas of operations based on assessments of materiality and risk. Our audit procedures included inquiries of appropriate personnel, inspection of documents and records, and observation of FMIS operations. We also tested transactions and performed other auditing procedures that we considered necessary to achieve our objectives.

The Maryland Department of Transportation maintains its own version of FMIS, which is not included in the scope of this audit. In addition, certain State agencies, including the Judiciary, University System of Maryland and the Maryland Department of Transportation process procurement, disbursement and financial information on in-house computer systems that interface certain financial information to centralized FMIS for recordation, payment processing and reporting. With respect to interfaced data, our centralized audit included a review of the controls and processing of such data from the point of interface to FMIS through transaction processing and recordation.
The aforementioned two control agencies are responsible for establishing and maintaining overall FMIS effective internal control. Internal control is a process designed to provide reasonable assurance that objectives pertaining to the reliability of financial records, effectiveness and efficiency of operations including safeguarding of assets, and compliance with applicable laws, rules and regulations are achieved.

Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. In addition, projections of any evaluation of internal control to future periods are subject to the risk that conditions may change or compliance with policies and procedures may deteriorate.

Our reports are designed to assist the Maryland General Assembly in exercising its legislative oversight function and to provide constructive recommendations for improving State operations. As a result, our reports generally do not address activities we reviewed that are functioning properly.

This report includes findings relating to conditions that we consider to be significant deficiencies in the design or operation of internal control that could adversely affect the State’s ability to maintain reliable financial records, operate effectively and efficiently and/or comply with applicable laws, rules and regulations. Our audit did not disclose any significant instances of noncompliance with applicable laws, rules or regulations.

The Department of Budget and Management’s and the Comptroller of the Treasury’s responses to our findings and recommendations are included as an appendix to this report. As prescribed in the State Government Article, Section 2-1224 of the Annotated Code of Maryland, we will advise the Department and the Comptroller regarding the results of our review of their responses.
March 13, 2003

Mr. Bruce A. Myers, CPA
Legislative Auditor
Department of Legislative Services
Office of Legislative Audits
301 West Preston Street, Room 1202
Baltimore, MD 21201

Dear Mr. Myers:

The Department of Budget and Management has reviewed your draft audit report on the Financial Management Information Systems (FMIS) Centralized Operations. We appreciate the opportunity to provide responses and information pertaining to the findings noted during your audit. As requested, our responses to findings 1, 2, 3 and 7 in the report, which pertain to the Department’s FMIS Centralized Operations, are attached.

The Department would like to acknowledge the value the legislative auditor’s review of this area has been. It has provided confirmation of activities that are functioning properly, and guidance in identifying weaknesses in the FMIS operations and prioritizing actions to be taken to address these areas of risk.

If you have any questions or need additional information, you may contact the Assistant Director of the Application Systems Management Division, Robert Campbell at 410-260-7084 or me at 410-260-7041.

Sincerely,

James C. DiPaola
Secretary

cc: Mr. Thomas K. Lee, Deputy Secretary
    Mr. Robert Campbell, Assistant Director, Applications Systems Management
Response to Audit Report of
Financial Management Information System
Centralized Operations
March 2003

FMIS – Access Controls

Finding 1
Modification access to program files supporting online FMIS processing was not adequately recorded or restricted

**DBM Response:** We concur with the audit finding, with the following noted. Due to audit fieldwork conducted, ASM became aware of this situation and corrected the problem, as recommended by the auditor, as of March 28, 2002. ASM believes that this finding has been adequately corrected. ASM will continue to monitor access to critical program files to ensure continued compliance of this audit finding.

Finding 2
Reviews of FMIS security access reports were not performed by independent employees and certain other security reports were not received for review

**DBM Response:** We concur with the audit finding, with the following noted. Due to audit fieldwork conducted, ASM requested, via a memorandum dated 2/8/02 to ADC, the Logonid Modification Report be included in our daily run of ACF2 reports. Effective 2/9/02 ASM began receiving the Logon Modification Report. Beginning in early October 2002, a member of the ASM Security group, independent of the ACF2 Security Officer, began reviewing, signing and filing the ACF2 security reports daily. The same individual who is reviewing changes made (i.e., the security reports) is not also the same individual who has made changes. ASM believes that, currently, this finding has been adequately corrected. In addition, as requested by OLA, the Daily Reports will be reviewed reasonableness of changes made (i.e., changes made as noted on the report will be reviewed for who processed the change). This review will be documented and maintained.
Assignment of Users Security Privileges

Finding 3

*FMIS security designations, which granted agency personnel FMIS access, were not properly segregated.*

We concur with the audit finding with the following noted. The situation noted in the Analysis section of the finding was accurate when tested by the auditors prior to April 2002. Based on audit fieldwork conducted, DBM distributed a memorandum dated 2/27/02 to all agencies that had the same individual listed as the Functional Coordinator, and ASM Security Officer. We informed them we would no longer accept signatures on security forms until separation of duties was identified. As of April 1, 2002 all agencies were in compliance.

We are now in the process of getting access to the ACF2 Security Officers listing (controlled by ADC). Once we have this access we will notify agencies that do not have 3 separate individuals serving in the roles of ASM Security Officer, ASM Functional Officer and ACF2 Security Officer that it is recommended that for all 3 functions to be separated. In some situations where there is limited staffing this may be difficult. Thus, we feel that with maintaining that one person cannot function as both the ASM Security Officer and the ASM Functional Officer and with ASM requiring the signatures of both these individuals on access forms, there is no segregation problem.

ASM believe that this finding has been adequately corrected.

Ad-Hoc FMIS Database

Finding 7

*Assurance was lacking the separate Ad-Hoc database used by State agencies for supplemental reporting was accurate*

Development of a reconciliation process of the RSTARS Ad-Hoc tables to production RSTARS is in process. This process will mimic what is currently being done for the reconciliation of the ADPICS Ad-Hoc tables to production ADPICS. The Ad-Hoc to RSTARS reconciliation will consist of 5 processes.

- PCHADAE1 – Ad-Hoc ADT1 to RSTARS AE Reconciliation (Accounting Event)
- PCHADDC1 – Ad-Hoc ADD1 to RSTARS DF Reconciliation (Document Financial)
- PCHADGL1 – Ad-Hoc ADG1 to RSTARS GL Reconciliation (General Ledger)
- PCHADGL2 – Ad-Hoc ADG1 to RSTARS SGL Reconciliation (Summary General Ledger)
PCHADSU2 – Summary of the above listed reports

Selected fields are totaled from each system by last processing date and compared. Record counts are also generated and compared. Any discrepancy between the two systems is printed in detail on the individual table report, with an out of balance entry written on the summary report. A remedy ticket will be created for each out of balance condition, documenting the procedures used to fix the out of balance condition. The summary report along with the remedy ticket will be filed until the next audit period. These reports will be processed during the nightly batch cycle and reviewed on a daily basis. Remedy tickets will serve as documentation of any necessary ‘fixes’ made to the system as a result of this review. This documentation will be maintained for audit verification. The estimated completion date for the R*STARS to R*STARS Ad-Hoc reconciliation is July 2003.

Correspondence will also be sent to the Ad-Hoc group, the Financial Applications Committee, along with a BBS message indicating the R*STARS Ad-Hoc database is not being reconciled to the R*STARS production database.
March 5, 2003

Mr. Bruce A. Myers, CPA
Legislative Auditor
Department of Legislative Services
Office of Legislative Audits
Maryland General Assembly
301 West Preston Street, Room 1202
Baltimore, Maryland 21201

Dear Mr. Myers:

Thank you for the opportunity to respond to the audit report on the Financial Management Information System (FMIS) Centralized Operations. As requested, our response specifically addresses findings 4, 5, and 6.

Finding number 4 requests that R*STARS security officers be restricted from modifying their own R*STARS access rights. The General Accounting Division (GAD) concurs with the recommendation and a modification has been made to the R*STARS security system software to prevent employees from changing their own security profile records.

Finding number 5 recommends that the basis for any change to critical R*STARS control profiles be documented and independently compared with the actual changes, and that the evidence of this comparison be retained. We concur with the Auditor’s recommendation. It is the General Accounting Division’s procedure to require all changes to the statewide profiles be documented and approved. An independent employee is assigned to monitor all activity recorded on the Profile Maintenance Log Report (DAFR9900) and to track all changes and related documentation. In most cases, a formal written request is required to authorize any change to a statewide profile. Certain changes that occur frequently and are not critical to the Comptroller’s control, such as a request to reopen a closed fiscal month on the 25 profile or a change to an effective end date on the 20 profile, are processed based on a verbal request from the agency. For these less significant changes GAD has agreed with the Auditor to obtain agency documentation or to document the agency’s verbal request by providing a written explanation and name of the requestor on the screen print of the changed profile.

Finding number 6 recommends that modification access to critical R*STARS control profiles be limited to individuals requiring such access and that this access be periodically
reassessed relative to users' job responsibilities. We concur with the Auditor's recommendation. We will review all requests by GAD personnel for access to critical control profiles in R*STARS in order to limit access to the degree required by the individual's job responsibilities. Additionally, we will reassess such access when individuals' job duties are reassigned.

Sincerely,

[Signature]

Stephen M. Cordi
Deputy Comptroller

[Signature]

John D. Kenney
Director, General Accounting Division

SMC/JDK:ja
AUDIT TEAM

Stephen P. Jersey, CPA, CISA
Information Systems Audit Manager

Richard L. Carter, CISA
Edwin L. Paul, CPA
Information Systems Senior Auditors

Albert E. Schmidt, CPA
Information Systems Staff Auditor

Brian D. Schenck
Staff Auditor