AUDITOR GENERAL

DAVID W. MARTIN, CPA

DEPARTMENT OF FINANCIAL SERVICES

SELECTED DIVISION OF TREASURY SYSTEMS

Information Technology Audit

SUMMARY

The Chief Financial Officer (CFO) serves as the chief fiscal officer of the State and is responsible to settle and approve accounts against the State and keep all State funds and securities. The CFO heads the Department of Financial Services (Department) that has a wide range of constitutional and statutory responsibilities. Within the Department, the Division of Treasury performs functions generally associated with private financial institutions, such as deposit security, funds management, and deferred compensation. To perform the Division of Treasury's functions, the Department maintains approximately 22 individual Division of Treasury information technology (IT) systems (Treasury systems).

Our audit focused on evaluating selected IT controls applicable to the following Treasury systems: Bank Accounts, Investment Accounting, Chargebacks, Receipts, and Verifies during the period January 2008 through March 2008.

The results of our audit are summarized below:

Finding No. 1: Program change controls for the Treasury systems needed improvement.

Finding No. 2: Some excessive and inappropriate system access privileges existed. Additionally, terminated and reassigned employees' access privileges were not removed in a timely manner.

Finding No. 3: Aspects of the Department's practices for managing access privileges needed improvement.

Finding No. 4: In addition to the matters discussed in Finding Nos. 2 and 3, certain Department security and application controls needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising the Department's data and IT resources.

BACKGROUND

The CFO has various statutory responsibilities for State funds that include paying warrants and other orders for the disbursement of State funds, accounting for all State funds and securities, and depositing and investing funds. The Division of Treasury is responsible for ensuring that State moneys, employee deferred compensation contributions, State and local governments' public funds on deposit in Florida banks and savings associations, and cash and other assets held for safekeeping by the CFO are adequately accounted for, invested, and protected.

Within the Division of Treasury, the Bureau of Funds Management (Bureau) is responsible for posting State receipts and disbursements, performing cash management services, and investing available funds. To perform these duties, several Treasury systems have been developed and maintained by the Division of Information Systems (DIS), Bureau of Financial Applications, Treasury programming staff. The primary systems used by the Bureau for cash management were developed in Microsoft Access or Java and run on IBM AS400 servers.

FINDINGS AND RECOMMENDATIONS

To maintain data integrity and compensate for a lack of automated functionality and integration of the Treasury systems, the Department implemented various manual processes and reconciliations. While the manual processes provided the Department additional assurance of data integrity, some of the processes were duplicative, manually intensive, and an inefficient use of resources.

To provide more integration and efficiency in its business processes, the Department has pursued the replacement of the Treasury systems. Most of the systems were scheduled for replacement as part of Project Aspire, the anticipated replacement for the State's existing accounting and cash management systems. However, in May 2007, Project Aspire was suspended and the Department, as of May 2008, was in the process of researching alternate solutions for replacing the Treasury systems.

As discussed in the following findings and recommendations, our audit disclosed controls and practices applicable to the Treasury systems that need improvement through either a replacement system or enhancements to the current systems.

Finding No. 1:
Program Change Controls

Effective controls over program changes are intended to ensure that only authorized programs changes are implemented. It is also good business practice for program changes to be documented, reviewed, and approved. The likelihood of program change controls being followed on a consistent basis as intended by management is increased when management's expectations are clearly communicated to IT personnel in the form of written policies, procedures, and other guidelines. Additionally, to ensure an appropriate separation of duties, a group or persons independent of the programmers should control the movement of programs into production.

Our audit disclosed the following aspects of the Department's program change controls applicable to the Treasury systems that needed improvement. Specifically:

- ➢ The Department had developed Change Management and Control Policy No. 4-17 and DIS Operating Procedure No. DIS-015, defining change management policies and procedures to be followed for production environment changes to enterprise information resources. However, in response to audit inquiry, Department management indicated that Treasury programming staff did not follow these established policies and procedures but were working to better align their internal practices with Department and DIS policies and procedures. When established change management policies and procedures are not followed, the risk is increased that programming staff will not consistently perform their duties as expected by management.
- ➢ Program change requests were manually logged by the Department, but there was no mechanism in place to automatically detect and log Treasury systems program changes being moved into the production environment. The absence of an automatic system-generated log increases the risk that unauthorized and unrecorded program changes will be moved into the production environment and not be timely detected.
- ➢ Five program change requests for the Bank Accounts, Investment Accounting, Chargebacks, Receipts, and Verifies systems were shown in Department records as having been completed during the period January 1, 2008, through February 12, 2008. Information recorded in the change requests was incomplete, limiting the Department's ability to manage the program change process. Specifically:
  - One change request lacked documentation identifying the programmer assigned to work on the program change.
  - All five change requests lacked a record identifying who tested the program changes and who moved the changes into the production environment.

- All five change requests lacked documentation of user acceptance of the program changes.

- We were informed by Department management that all five of the program change requests mentioned above were programmed, tested, and moved to production by the same programmer, contrary to an appropriate separation of incompatible duties. Under these conditions, the risk is increased that unauthorized or erroneous program changes will be implemented without timely detection.

Recommendation: The Department should follow and adequately document compliance with established program change control procedures to ensure that all program changes are properly authorized, designed, tested, and implemented in a manner consistent with management's intent. Procedures should be implemented to ensure that all program changes within the production environment can be tracked to authorized change requests. Additionally, the Department should separate work responsibilities such that one employee does not control all critical stages of the program change process.

Finding No. 2: Appropriateness of Access Privileges

An important aspect of IT security management is the establishment of system access privileges that restrict end users to only those system functions necessary to perform their assigned duties. Properly configured access privileges help enforce an appropriate separation of incompatible duties and minimize the risk of unauthorized system actions. Examples of functions that are separated and generally assigned to individual employees or groups are application programming, systems programming, library change management, production control and scheduling, and data administration. Additionally, system end users, rather than IT staff, should be responsible for transaction origination and correction of production data.

Our review of the Department's end-user application level access listings for the Bank Accounts, Investment Accounting, Chargebacks, and Verifies systems as of January 17, 2008, and the Receipts system as of February 6, 2008, disclosed instances of inappropriate update access privileges in the systems' production environments. Specifically:

- Four Treasury programmers had update access privileges in three or more of the Treasury systems, contrary to an appropriate separation of incompatible duties.
- Five Division of Treasury employees had unnecessary update access privileges in one or more of the Treasury systems. Two of the five employees previously had been reassigned within the Division and did not require access as a part of their new duties.

Under these conditions, the Department's risk is increased that the access privileges could be misused.

In response to audit inquiry, Department management stated that the Treasury systems were not designed to allow only inquiry or reporting application-level access privileges separate from update privileges. This limited the Department's ability to restrict staff access privileges to only what was necessary for their job duties. Specifically, employees were granted update access privileges even when read-only or reporting access privileges were required to perform their job duties.

Our review of the Department's system level access listings associated with the Treasury systems, showing employees and others who had access to production programs and data (outside of the application controls of the systems) as of February 29, 2008, and employees who had access to the production job scheduler as of February 22, 2008, disclosed instances of inappropriate access privileges to production programs, data, and the job scheduler. Specifically:

- All five Treasury programmers had update access capabilities to the Bank Accounts, Investment Accounting, Chargebacks, Receipts, and Verifies systems' production program code and data. Additionally, the five Treasury programmers had update access capabilities to the related production job scheduler.
- Three database administrators had update access capabilities to production program code for the Investment Accounting, Chargebacks, Receipts, and Verifies systems.
- A systems programming administrator and an IT business consultant manager with programming responsibilities had update access capabilities to the production program code for the Bank Accounts system.
- A user group with 11 end-user profiles had update access capabilities to production program code for the Investment Accounting, Chargebacks, and Verifies systems.
- Another user group with 91 end-user and system profiles had inappropriate update access capabilities to production program code for the Investment Accounting, Chargebacks, Receipts, and Verifies systems. In response to audit inquiry, Department management indicated that the user group has now been modified to have read-only access and was reduced to include only 24 internal user profiles.
- Access capabilities to the Chargebacks and Verifies systems' production data had not been deleted for two former employees, with termination dates of November 11, 2002, and November 30, 2002, respectively. One of the former employee's access privileges was being used by Treasury programming staff to run batch programs. Subsequent to audit inquiry, Department management indicated that both of the former employees' access privileges had been disabled on April 1, 2008.
- Access capabilities to the Chargebacks and Verifies systems' production data that were no longer required had not been deleted for two reassigned employees who transferred to another area within the Department on October 26, 2005, and May 1, 2007, respectively. Subsequent to audit inquiry, Department management indicated that both of the reassigned employees' access privileges had been disabled on April 1, 2008.

Inappropriate or unneeded access privileges increase the risk of unauthorized disclosure, modification, or destruction of data and IT resources.

Recommendation: The Department should continue to modify or remove the system access privileges of current and former employees and others, to the extent practicable, to remove unnecessary capabilities and promote a separation of incompatible duties. Additionally, in future Treasury system development projects, the Department should ensure that all new systems include the ability to grant inquiry and reporting capabilities separate from update capabilities.

Finding No. 3: Management of Access Privileges

Effective management of system access privileges includes the use of standard access authorization forms, approved by senior managers and maintained on file, to document the approval of user access privileges. The periodic review of access authorization listings by system owners and management helps ensure that privileges remain commensurate with employee job duties. According to DIS Operating Procedure No. DIS-011, access requests were to be approved by the functional owners and submitted, usually via e-mail, by the Treasury IT resource liaison to the DIS Help Desk which would ensure that the correct security administrator was notified of the request.

Our audit disclosed instances where the Department was lacking documentation to support application level access privileges in the Bank Accounts, Investment Accounting, Chargebacks, and Verifies systems as of January 17, 2008, and the Receipts system as of February 6, 2008. Specifically:

- The original access authorization requests from the functional owners for 13 of the 18 active Treasury systems end users could not be provided upon audit request. Additionally, the DIS Help Desk access request forms to support the existing access privileges could not be provided for 12 of these end users.

- No authorization forms or other written authorizations from the functional owners existed for the Treasury systems access privileges of the four programmers discussed previously in Finding No. 2 who had update access privileges in three or more of the systems.

In response to audit inquiry, Department management indicated that, when the Treasury systems were developed, all end users from the previous systems were added to the newly developed systems and no documentation or authorization was obtained from the functional owners. Department management further indicated that, since January 2004, the Treasury IT resource liaison has retained the DIS Help Desk access request forms and related e-mails; however, the original access authorization requests approved by the functional owners were not retained.

In addition, the Department's Enterprise Security Policy No. 4-03, effective September 1, 2006, required a formal process for the periodic review and confirmation of user accounts, access controls, and privileges. The Policy also stated that the periodic review would include, but not be limited to, a review of the rights, restrictions, and password removals as it applied to active employees and third parties. Although the Department performed a review of the Treasury systems' access privileges in August 2007, Department management indicated that such a review is not being performed on a periodic basis.

The lack of documentation of access authorizations limits management's ability to ensure that access privileges are appropriate and increases the risk that inappropriate access privileges will not be detected. Additionally, without periodic reviews of access privileges, the risk is increased that inappropriate or unnecessary access privileges will not be timely detected and corrected.

Recommendation: The Department should ensure that authorization of all access privileges associated with the Treasury systems is documented to facilitate effective security administration. In addition, periodic reviews of Treasury system access privileges should be performed to ensure that privileges remain necessary and commensurate with employees' job duties.

Finding No. 4: Other Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of data, IT resources, and sensitive information. During our audit, we identified certain Department security and application controls, in addition to the matters discussed in Finding Nos. 2 and 3, that needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising Department data and IT resources. However, appropriate Department staff have been notified of these issues. Without adequate security and application controls, the integrity, confidentiality, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, destruction, or modification.

Recommendation: The Department should implement the appropriate security and application controls to ensure the continued integrity, confidentiality, and availability of Department data and IT resources.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application controls related to the Treasury Bank Accounts, Investment Accounting, Chargebacks, Receipts, and Verifies systems.

The scope of our audit focused on evaluating selected IT controls applicable to the Treasury Bank Accounts, Investment Accounting, Chargebacks, Receipts, and Verifies systems during the period January 2008 through March 2008. In conducting our audit, we interviewed appropriate Department personnel, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to the Treasury systems.

We conducted this IT audit in accordance with applicable generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT audit.

David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated July 11, 2008, the Chief Financial Officer provided responses to our preliminary and tentative findings. This letter is included at the end of this report as APPENDIX A.

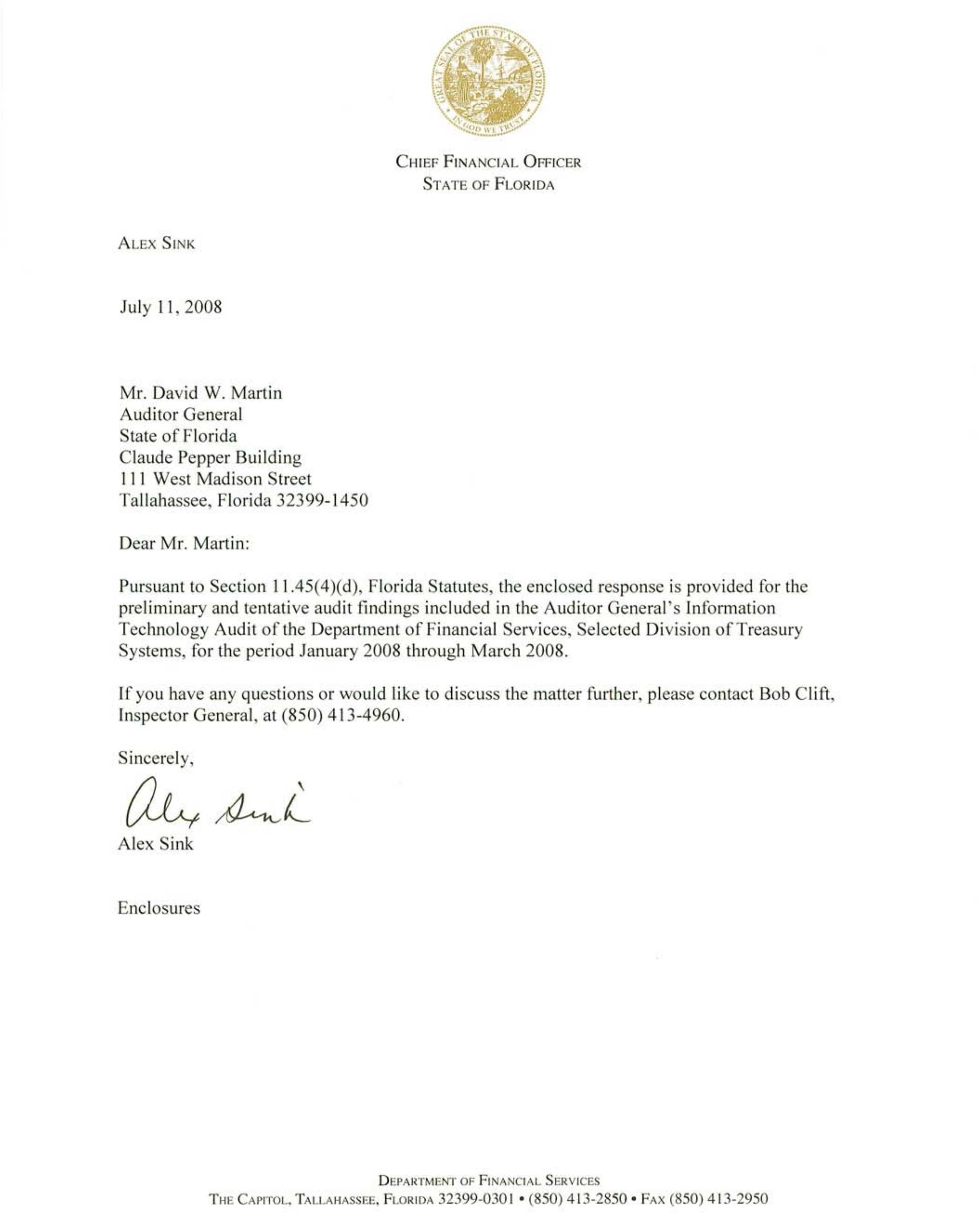
This audit was conducted by Cathy Jones, CISA, and supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.myflorida.com/audgen/); by telephone (850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

MANAGEMENT RESPONSE



CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

ALEX SINK

July 11, 2008

Mr. David W. Martin
Auditor General
State of Florida
Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's Information Technology Audit of the Department of Financial Services, Selected Division of Treasury Systems, for the period January 2008 through March 2008.

If you have any questions or would like to discuss the matter further, please contact Bob Clift, Inspector General, at (850) 413-4960.

Sincerely,

Alex Sink

Alex Sink

Enclosures

Florida Department of Financial Services

Audit Response
Selected Division of Treasury Systems
Information Technology Audit
For the Period January 2008 through March 2008

Finding No. 1: Program change controls for the Treasury systems needed improvement.

Recommendation: The Department should follow and adequately document compliance with established program change control procedures to ensure that all program changes are properly authorized, designed, tested, and implemented in a manner consistent with management's intent. Procedures should be implemented to ensure that all program changes within the production environment can be tracked to authorized change requests. Additionally, the Department should separate work responsibilities such that one employee does not control all critical stages of the program change process.

Response: The Department concurs. Effective August 1, 2008, the Division of Treasury will be incorporated into the DIS Application Service Request (ASR) system. The ASR system provides the ability to track requests for changes, document the separation of duties including the identification of the resources assigned for programming, testing, and moving changes into the production environment, and document user acceptance testing. A Request for Change (RFC) will be created within the Remedy Change Management System per DFS AP&P 4-17 Change Management and Control Policy and DIS-015 Change Management Operating Procedures, and the ASR number(s) will be listed in the RFC to provide a cross-reference to the authorized change requests.

System maintenance and deployment responsibilities will be segregated on older platforms by assigning the code development and code promotion to different Bureau of Financial Applications (BFA) staff starting August 1, 2008, and tracked using the ASR system.

All new development since August 2007 using the .NET development and SQL server platforms ensures separation of duties. Programmers do not have access to the production environment on the .Net server or the SQL database server and deployments will be implemented by staff in those sections.

AP&P No. 4-17 Change Management and Control Policy, and DIS-015 Change Management Operating Procedures will be followed for production deployments and database structure changes will follow the DIS-010 Procedures for Database Change Requests for new and old environments

Finding No. 2: Some excessive and inappropriate system access privileges existed. Additionally, terminated and reassigned employees' access privileges were not removed in a timely manner.

Recommendation: The Department should continue to modify or remove the system access privileges of current and former employees and others, to the extent practicable, to remove unnecessary capabilities and promote a separation of incompatible duties. Additionally, in future Treasury system development projects, the Department should ensure that all new systems include the ability to grant inquiry and reporting capabilities separate from update capabilities.

Response: The Department concurs. To control system access privileges, effective July 10, 2008, the Bureau of Financial Applications will complete modifications to all end user profiles and groups on the Treasury AS400 to remove individual user access to production code and data.

As of August 2007, new system design incorporates role based security for the system users that includes separation of inquiry, update, and reporting capabilities.

Finding No. 3: Aspects of the Department's practices for managing access privileges needed improvement.

Recommendation: The Department should ensure that authorization of all access privileges associated with the Treasury systems is documented to facilitate effective security administration. In addition, periodic reviews of Treasury system access privileges should be performed to ensure that privileges remain necessary and commensurate with employees' job duties.

Response: The Department concurs. The Division of Treasury will follow the access process specified by DFS AP&P 4-05 Application Access Control. Additionally, effective July 1, 2008, a new monthly audit procedure has been implemented by the Division of Treasury to review user access privileges. Final documentation for this procedure is pending completion by August 1, 2008.

Finding No. 4: In addition to the matters discussed in Finding Nos. 2 and 3, certain Department security and application controls needed improvement. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising the Department's data and IT resources.

Recommendation: The Department should implement the appropriate security and application controls to ensure the continued integrity, confidentiality, and availability of Department data and IT resources.

Response: The Department concurs with the recommendation and will implement appropriate security controls.

THIS PAGE INTENTIONALLY LEFT BLANK