AUDITOR GENERAL

DAVID W. MARTIN, CPA

DEPARTMENT OF TRANSPORTATION TRNS*PORT SYSTEM SITEMANAGER MODULE, LABORATORY INFORMATION MANAGEMENT SYSTEM, AND CONSULTANT INVOICE TRANSMITTAL SYSTEM

Information Technology Audit

SUMMARY

The Department of Transportation (Department) is responsible for the development and maintenance of Florida's transportation system. Among the application systems used by the Department for project and financial management purposes are the SiteManager module of the TRNS*PORT System (SiteManager), the Laboratory Information Management System (LIMS), and the Consultant Invoice Transmittal System (CITS). The Department uses these systems as follows:

- **SiteManager – to generate and approve payments for construction and maintenance projects.**
- **LIMS – to record and report construction material sampling results to ensure that materials used met contract specifications.**
- **CITS – to approve related payments for consultants who submitted invoices via the Internet.**

Our audit focused on evaluating selected information technology (IT) controls applicable to SiteManager, LIMS, and CITS during the period April 2008 through June 2008 and selected actions through August 1, 2008. Specifically, the audit included selected application IT controls and selected general IT controls over systems modification and logical access to programs and data.

The results of our audit are summarized below:

Finding No. 1: **The LIMS program change controls were deficient and did not follow the Department's information systems development methodology (ISDM).**

Finding No. 2: **Certain security controls related to SiteManager, LIMS, and CITS and the supporting computer environment at the Central Office, Turnpike Enterprise, and Districts needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources.**

Finding No. 3: **The Department's Electronic Security for Public Records Exemptions Policy was outdated.**

BACKGROUND

The Department is a decentralized agency with a Central Office, a Turnpike Enterprise, and seven Districts. The Central Office is responsible for establishing and monitoring the implementation of Department policies, rules, procedures, and standards to ensure uniform compliance and quality performance by the Central Office units and Districts that implement transportation programs.

To assist in the implementation and management of the transportation programs, the Department uses SiteManager, LIMS, and CITS, among many other systems. The core programming code for SiteManager and LIMS was developed and is maintained by software vendors. CITS was developed and is maintained by the Department. The Department also develops and maintains SiteManager, LIMS, and CITS interfaces with other Department application systems. The Office of Information Systems within the Department's Central Office coordinates program maintenance for SiteManager and CITS, while the Department's State Materials Office is responsible for LIMS program maintenance.

Finding No. 1: Maintenance of LIMS

The Department's information systems development methodology (ISDM) establishes standards for information systems developed for the Department by the Office of Information Systems, provided that the systems meet the following criteria:

- The system is used by more than one Department office.
- The system creates or modifies data or data structures that are used by more than one Department office.
- The system has corporate or strategic value to the Department.

The ISDM specifies, among other things, the program change control process to be followed when maintaining applicable systems, including required approvals and documentation.

LIMS and its data were used by all Department Districts and the Turnpike Enterprise. LIMS was used by the Department to ensure that the materials and workmanship incorporated into each construction project met contract terms, plans, and specifications. As such, LIMS has strategic value to the Department. Nevertheless, LIMS maintenance was overseen by the Department's State Materials Office rather than the Office of Information Systems and the LIMS program change process did not follow the Department's ISDM.

Our audit disclosed that the program change controls associated with LIMS were deficient. Specifically, the Department did not document all LIMS changes and was unable to provide, upon audit request, the population of LIMS program changes that occurred during the audit period. Additionally, existing program change documentation did not always include change requests, authorizations to initiate changes, evidence of program change testing, and approvals to implement LIMS program changes. Absent appropriate program change documentation, the Department has limited assurance that changes made to LIMS were appropriately authorized, tested, and approved for implementation.

Recommendation: The Department should document all LIMS program changes to provide management the ability to identify all changes made to the system and ensure that changes are properly authorized, tested, and approved for implementation in a manner consistent with its ISDM. The Department should also consider assigning the Office of Information Systems the responsibility for maintaining LIMS because of the system's Departmentwide significance.

Finding No. 2: Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to SiteManager, LIMS, and CITS and the supporting computing environment operated by the Central Office, Turnpike Enterprise, and the Districts that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls, the confidentiality, integrity, 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, modification, or destruction.

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

Finding No. 3: Department Security Policies

Effective security management includes periodically reviewing and updating written security policies to ensure that the policies remain relevant and address current information risks. The Department's Electronic Security for Public Records Exemptions Policy, which establishes a process and standards for providing security for the Department's electronic records that are exempt from public disclosure, was outdated. The Policy, dated November 29, 1993, cited administrative rules that no longer exist and included several inaccurate references to Florida Statutes. Under these conditions, the risk is increased that management's expectations for protecting information will not be effectively communicated, understood, or consistently met.

Recommendation: The Department should periodically review and update its security policies as necessary to ensure that management's expectations for protecting Department information are clearly and accurately communicated to employees.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application controls relating to SiteManager, LIMS, and CITS.

The scope of our audit focused on evaluating selected IT controls applicable to the systems during the period April 2008 through June 2008 and selected actions through August 1, 2008.

In conducting our audit, we :

- Interviewed Department personnel.
- Obtained an understanding of the Department's systems modification procedures, application and user controls, and security controls as they related to SiteManager, LIMS, and CITS.
- Observed, documented, tested, and evaluated key processes and procedures related to the Department's systems modification activities, transaction logging, security administration function, and program and data security controls for SiteManager, LIMS, and CITS.

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 October 3, 2008, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as APPENDIX A.

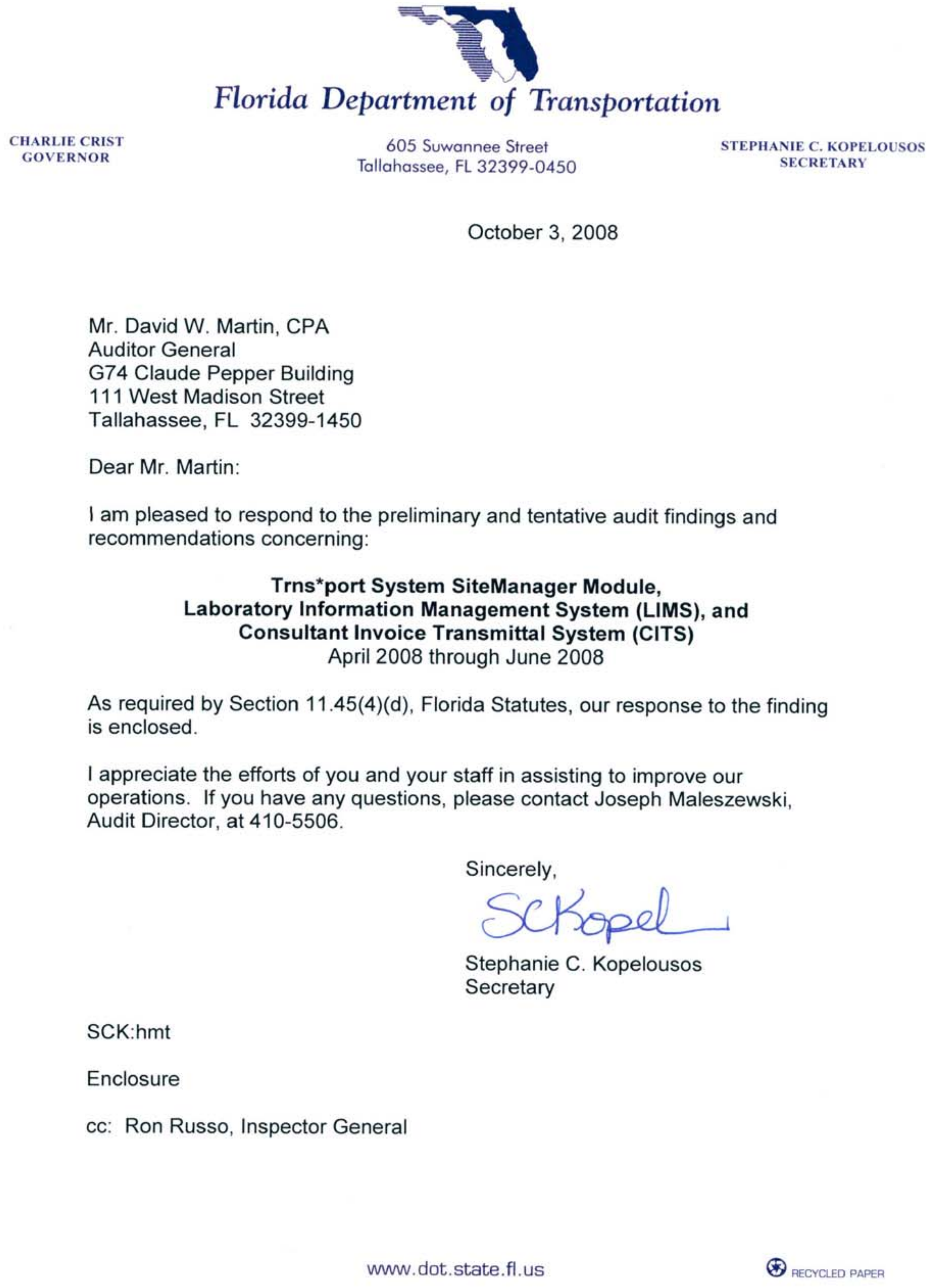
This audit was conducted by Art Wahl, CPA, CISA, and supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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



Florida Department of Transportation

CHARLIE CRIST
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

STEPHANIE C. KOPELOUSOS
SECRETARY

October 3, 2008

Mr. David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Martin:

I am pleased to respond to the preliminary and tentative audit findings and recommendations concerning:

Trns*port System SiteManager Module,
Laboratory Information Management System (LIMS), and
Consultant Invoice Transmittal System (CITS)
April 2008 through June 2008

As required by Section 11.45(4)(d), Florida Statutes, our response to the finding is enclosed.

I appreciate the efforts of you and your staff in assisting to improve our operations. If you have any questions, please contact Joseph Maleszewski, Audit Director, at 410-5506.

Sincerely,

SCKopel

Stephanie C. Kopelousos
Secretary

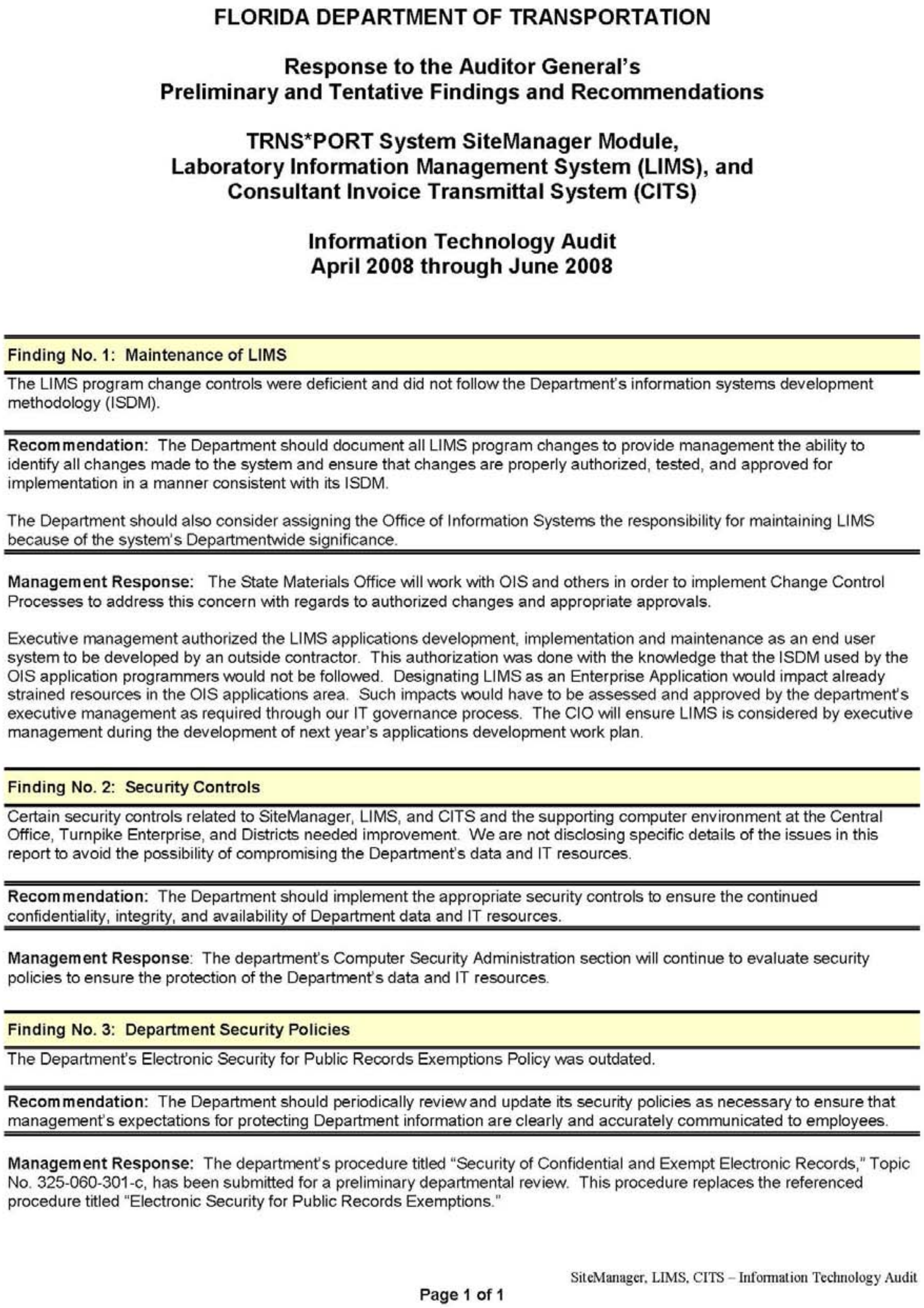
SCK:hmt

Enclosure

cc: Ron Russo, Inspector General

www.dot.state.fl.us

RECYCLED PAPER



FLORIDA DEPARTMENT OF TRANSPORTATION

Response to the Auditor General's Preliminary and Tentative Findings and Recommendations

TRNS*PORT System SiteManager Module, Laboratory Information Management System (LIMS), and Consultant Invoice Transmittal System (CITS)

Information Technology Audit April 2008 through June 2008

Finding No. 1: Maintenance of LIMS

The LIMS program change controls were deficient and did not follow the Department's information systems development methodology (ISDM).

Recommendation: The Department should document all LIMS program changes to provide management the ability to identify all changes made to the system and ensure that changes are properly authorized, tested, and approved for implementation in a manner consistent with its ISDM.

The Department should also consider assigning the Office of Information Systems the responsibility for maintaining LIMS because of the system's Departmentwide significance.

Management Response: The State Materials Office will work with OIS and others in order to implement Change Control Processes to address this concern with regards to authorized changes and appropriate approvals.

Executive management authorized the LIMS applications development, implementation and maintenance as an end user system to be developed by an outside contractor. This authorization was done with the knowledge that the ISDM used by the OIS application programmers would not be followed. Designating LIMS as an Enterprise Application would impact already strained resources in the OIS applications area. Such impacts would have to be assessed and approved by the department's executive management as required through our IT governance process. The CIO will ensure LIMS is considered by executive management during the development of next year's applications development work plan.

Finding No. 2: Security Controls

Certain security controls related to SiteManager, LIMS, and CITS and the supporting computer environment at the Central Office, Turnpike Enterprise, and Districts needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising the Department's data and IT resources.

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

Management Response: The department's Computer Security Administration section will continue to evaluate security policies to ensure the protection of the Department's data and IT resources.

Finding No. 3: Department Security Policies

The Department's Electronic Security for Public Records Exemptions Policy was outdated.

Recommendation: The Department should periodically review and update its security policies as necessary to ensure that management's expectations for protecting Department information are clearly and accurately communicated to employees.

Management Response: The department's procedure titled "Security of Confidential and Exempt Electronic Records," Topic No. 325-060-301-c, has been submitted for a preliminary departmental review. This procedure replaces the referenced procedure titled "Electronic Security for Public Records Exemptions."

THIS PAGE INTENTIONALLY LEFT BLANK