AUDITOR GENERAL
WILLIAM O. MONROE, CPA

DEPARTMENT OF COMMUNITY AFFAIRS
EMTRAKER SYSTEM
SELECTED GENERAL CONTROLS
Information Technology Audit

SUMMARY

The Division of Emergency Management (Division) within the Department of Community Affairs (Department) is responsible for maintaining a comprehensive Statewide program of emergency management, and provides programs and services to assist communities in preparing for and responding to natural and man-made disasters. The Division uses the EMTraker System to assist in managing emergency situations. The EMTraker System provides a database and a communications link between local governments and emergency responders at the State Emergency Management Center (EOC).

Our audit focused on evaluating the effectiveness of selected general controls related to the EMTraker System and its information technology (IT) environment for the period June 2005 through September 2005. The results of our audit are summarized below:

Finding No. 1: **Improvements were needed in the Department's entitywide security program.**

Finding No. 2: **Deficiencies were noted in certain security controls protecting the EMTraker System.**

Finding No. 3: **Environmental control improvements were needed at the Department's data center housing various operational systems, such as EMTraker.**

Finding No. 4: **Improvements were needed in the Department's Information Systems Development Methodology (ISDM).**

BACKGROUND

The Department focuses its time and resources on three primary program areas; community planning, emergency management, and housing and community development. The Division of Emergency Management addresses all aspects of emergency management for man-made and natural disasters in Florida. The Division depends on a complex network of responders, communications, and technologies to determine resource logistics and availability for disaster response as well as recovery operations. Among these is the EMTraker System, which is used to assist in managing emergency situations. The EMTraker System is a standalone database that is both internal client-based, used by emergency responders at the EOC, and web-based for access by local counties. The system provides a link between local authorities and State emergency responders, giving local communities the communications tool necessary to request resources during an emergency.

Finding No. 1:
Security Program

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program establishes a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Principles that help ensure that information security policies address current risks include implementing appropriate security policies and controls to mitigate identified risks, designating positions of special trust, and promoting security awareness.

We noted aspects of the overall Department security program that needed improvement, as follows:

- The Department's security policies and procedures had not been formally approved. According to State Technology Office (STO) information resource security policies and standards[1], each agency is to develop an information resource security program that includes a documented and maintained current internal information resource security plan approved by the agency Chief Information Office, and maintained by the agency's Information Security Manager[2]. The agency security program and plan are to include, among other things, written internal policies and procedures for protection of information resources, and are to be signed by the agency head. The Department provided us with a Security Posture and Policy document which defined IT security and operational procedures. This document was represented as being a draft document that had not been officially approved as of the conclusion of our audit field work. Without approved security policies and procedures, management cannot be assured that the Department's security will be administered as intended.
- The Department had not designated key IT employees, such as, but not limited to, security administrators, developers, programmers, and database administrators, as occupying positions of special trust and had not ensured that appropriate background checks of these individuals, including fingerprinting, had been completed as required by Florida law.[3] Neither had the Department established written procedures describing the measures necessary for the oversight of those positions. By not designating positions of special trust for positions with high access levels, or documenting detailed review procedures of the actions taken by the individuals occupying those positions, the risk is increased that inappropriate access or modification to data and information technology resources may occur without detection.
- The Department had not developed a comprehensive security awareness and ongoing training program. The purpose of the security awareness program, which can include training and publications, is to inform personnel of the importance of the information they handle and the legal and business reasons for maintaining its integrity, confidentiality, and availability. Employees should receive documentation describing security policies, procedures, and individual responsibilities. The lack of a comprehensive security awareness and training program increases the risk to, and the vulnerability of, the Department's information technology resources by limiting management's assurance that Department staff understand the importance of IT security and are sufficiently prepared to safeguard data and IT resources.

The above-listed security management issues increase the risk that controls may be inadequate and inconsistently applied and responsibilities may be unclear, misunderstood, and improperly implemented. This could lead to inadequate protection of sensitive or critical resources.

Recommendation: The Department should enhance its information resource security program by formally approving and implementing appropriate policies, procedures, and controls, including the designation of positions of special trust and the associated background checks. Furthermore, management should promote ongoing security awareness through adequate training programs.

[1] Chapter 60DD-2.001(5)(b), Florida Administrative Code

[2] Effective July 1, 2005, the responsibilities of the STO were assimilated by DMS. Prior to this date, Section 282.102(2), Florida Statutes, provided the STO with certain rulemaking authority with regard to the State's IT resources, and as of the completion of our audit, rulemaking authority statutorily remained with the STO.

[3] Section 110.1127(1), Florida Statutes

Finding No. 2: Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of information systems data and resources. During our audit, we identified deficiencies in aspects of the Department's IT network security controls. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising the Department's network security. However, the appropriate Department personnel have been notified of the deficiencies.

Recommendation: The Department should implement appropriate action to correct the network security control features to enhance the safeguarding of Department IT resources.

Finding No. 3: Environmental Controls

STO information resource security policies and standards[4] provide that one of the major causes of computer downtime is the failure to maintain proper controls over temperature, humidity, air movement, cleanliness, and power. Information resources are to be protected from environmental hazards, and environmental controls must also provide for the safety of personnel.

We noted that the Department's data center that housed various systems, such as the EMTraker System, did not have adequate controls in place to protect it from environmental hazards. Specifically, the data center was not equipped with adequate air conditioning, electrically non-conductive fire suppression, raised flooring with water drainage, or emergency power shut-off switches. According to the Department, it was in the process of making arrangements to relocate its computer equipment to a facility with more comprehensive environmental controls.

Without adequate controls in place to safeguard computer equipment from environmental hazards, the Department's risk is increased of equipment failure and damage in the event of an emergency situation.

Recommendation: The Department should proceed with efforts to establish a data center environment that contains the proper environmental controls to ensure the safety of its computer equipment.

Finding No. 4: Information Systems Development Methodology (ISDM)

STO information technology life cycle policies and standards[5] establish, among other things, a common ISDM outlining procedures, practices, and guidelines governing the initiation, concept development, planning, requirements analysis, design, development, integration and test, implementation, operations, maintenance and disposition of information technology.

We noted that improvements were needed in the Department's ISDM. The Department's ISDM did not address the following elements prescribed in the STO IT life cycle policies and standards:

- Preparing a cost-benefit analysis which identifies cost or benefit information for analyzing and evaluating alternative solutions to a problem and for making decisions about initiating, and continuing, the development of IT systems.
- Performing a security certification and assessment certifying that the system security plan, security risk assessment, configuration management plan, and contingency plan have been updated, tested, reviewed, and approved.
- Performing a user satisfaction review to determine if systems are accurate and reliable.
- Preparing a disposition plan for IT hardware, software and data disposal, including provisions for, prior to disposal, archiving software and erasing all confidential and exempt information contained in all electronic memory components within IT equipment.

[4] Chapter 60DD-2.003(3)(a), Florida Administrative Code

[5] Chapter 60DD-7, Florida Administrative Code

Without a complete and effective ISDM, the Department's risk is increased of overlooking crucial design elements needed in a system that could result in project failure or reduced project management efficiency.

Recommendation: The Department's current ISDM should be expanded to include all applicable aspects of recommended practices within the STO rules, to ensure that a proper IT life cycle process is established.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to evaluate the effectiveness of selected general IT controls in the achieving management's objectives of compliance with controlling laws, administrative rules, and other guidelines; the reliability, integrity, and availability of data; the economic, efficient, and effective operation of IT; and the safeguarding and confidentiality of information resources. The scope of this audit focused on controls over logical access to programs and data, systems maintenance controls, and other selected general controls related to the Department's EMTraker System and its IT environment during the period June 2005 through September 2005. In conducting our audit, we interviewed appropriate Department personnel, observed Department processes and procedures, and performed various other audit procedures to test selected IT controls.

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 information technology audit.

William O. Monroe

William O. Monroe, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated March 1, 2006, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as Appendix A.

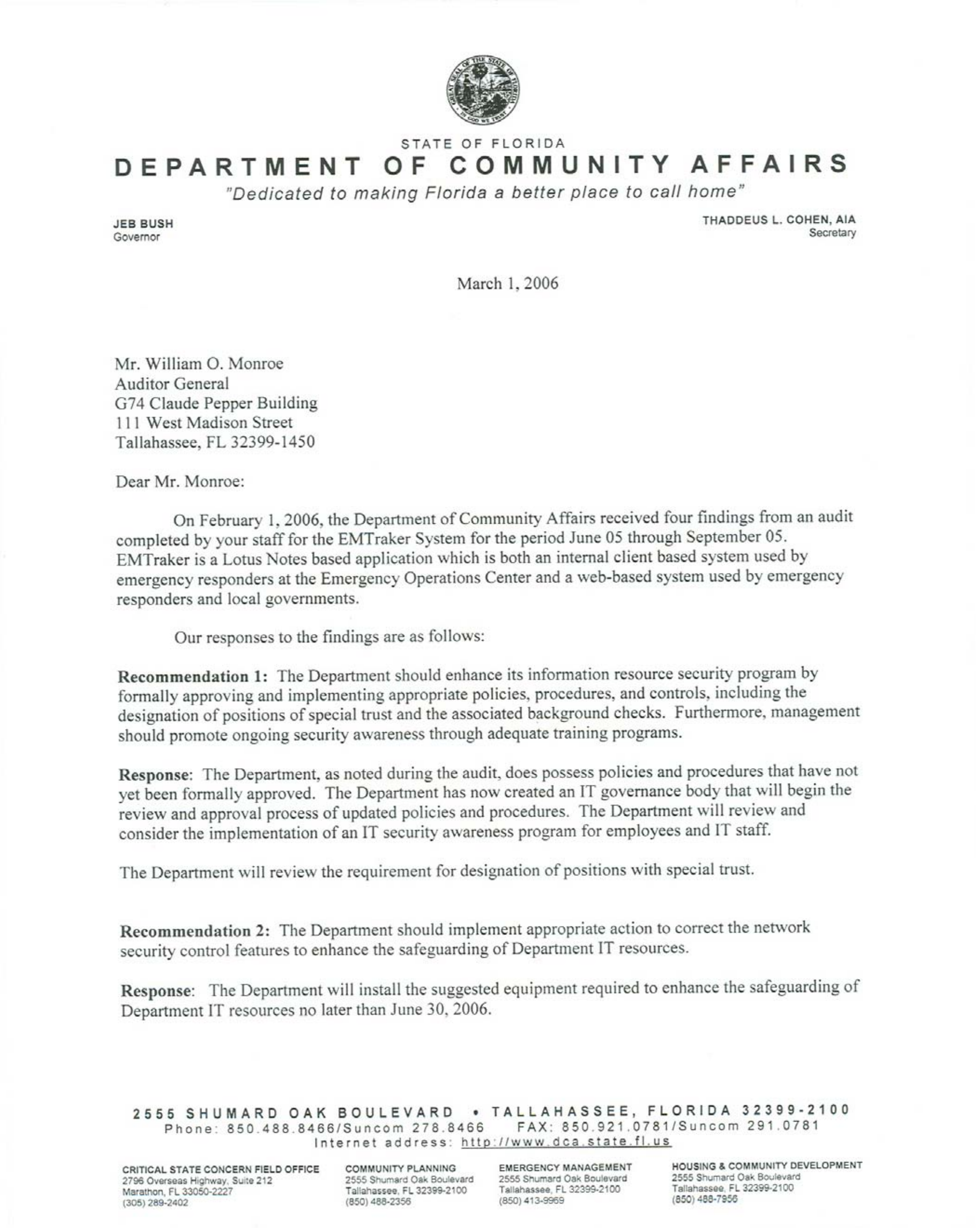
To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in ***Government Auditing Standards*** issued by the Comptroller General of the United States. This audit was conducted by William Tuck, 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.state.fl.us/audgen); by telephone (850 487-9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.

APPENDIX A

MANAGEMENT RESPONSE



STATE OF FLORIDA

DEPARTMENT OF COMMUNITY AFFAIRS

"Dedicated to making Florida a better place to call home"

JEB BUSH
Governor

THADDEUS L. COHEN, AIA
Secretary

March 1, 2006

Mr. William O. Monroe
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Monroe:

On February 1, 2006, the Department of Community Affairs received four findings from an audit completed by your staff for the EMTraker System for the period June 05 through September 05. EMTraker is a Lotus Notes based application which is both an internal client based system used by emergency responders at the Emergency Operations Center and a web-based system used by emergency responders and local governments.

Our responses to the findings are as follows:

Recommendation 1: The Department should enhance its information resource security program by formally approving and implementing appropriate policies, procedures, and controls, including the designation of positions of special trust and the associated background checks. Furthermore, management should promote ongoing security awareness through adequate training programs.

Response: The Department, as noted during the audit, does possess policies and procedures that have not yet been formally approved. The Department has now created an IT governance body that will begin the review and approval process of updated policies and procedures. The Department will review and consider the implementation of an IT security awareness program for employees and IT staff.

The Department will review the requirement for designation of positions with special trust.

Recommendation 2: The Department should implement appropriate action to correct the network security control features to enhance the safeguarding of Department IT resources.

Response: The Department will install the suggested equipment required to enhance the safeguarding of Department IT resources no later than June 30, 2006.

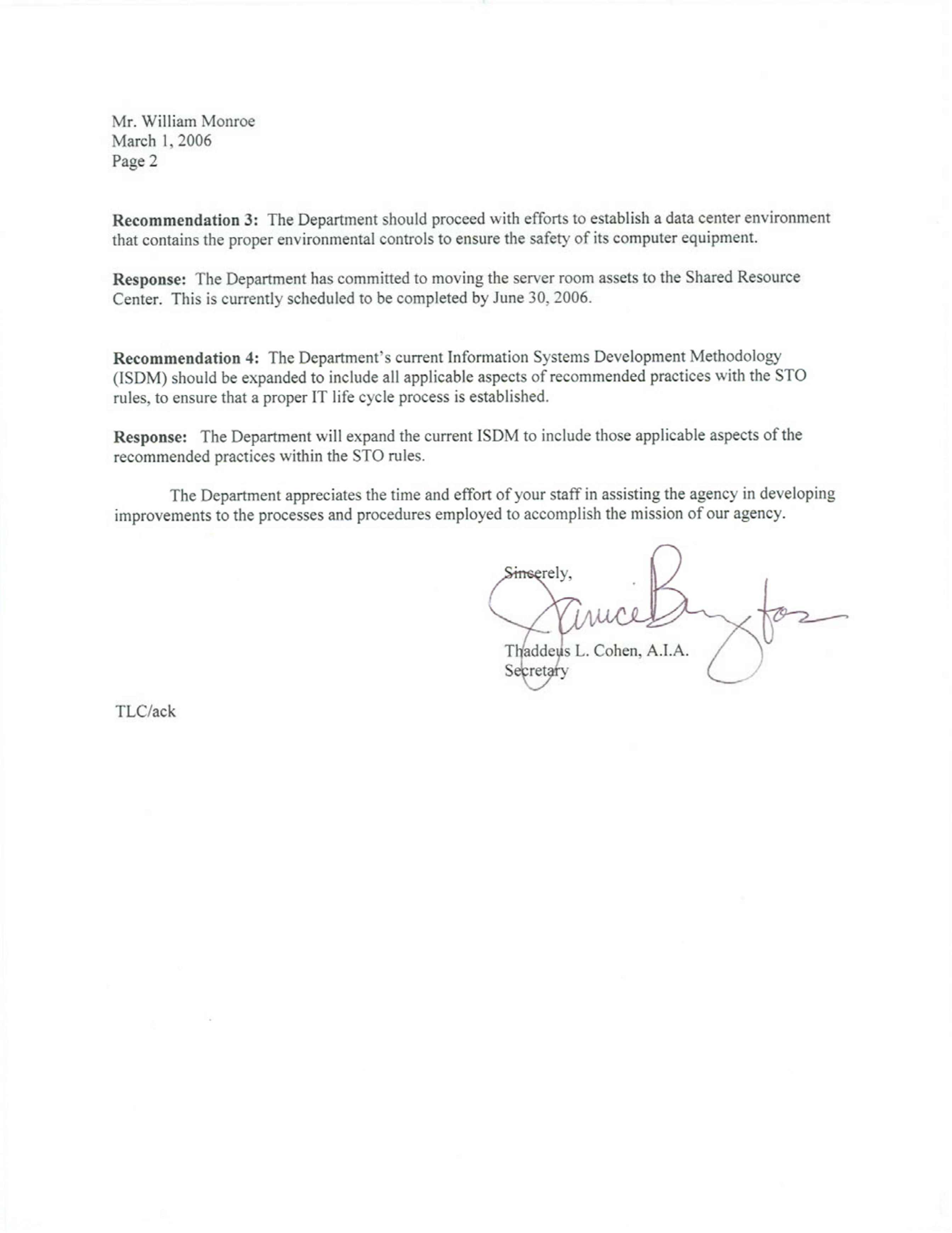
2555 SHUMARD OAK BOULEVARD • TALLAHASSEE, FLORIDA 32399-2100
Phone: 850.488.8466/Suncom 278.8466 FAX: 850.921.0781/Suncom 291.0781
Internet address: http://www.dca.state.fl.us

CRITICAL STATE CONCERN FIELD OFFICE
2796 Overseas Highway, Suite 212
Marathon, FL 33050-2227
(305) 289-2402

COMMUNITY PLANNING
2555 Shumard Oak Boulevard
Tallahassee, FL 32399-2100
(850) 488-2356

EMERGENCY MANAGEMENT
2555 Shumard Oak Boulevard
Tallahassee, FL 32399-2100
(850) 413-9969

HOUSING & COMMUNITY DEVELOPMENT
2555 Shumard Oak Boulevard
Tallahassee, FL 32399-2100
(850) 488-7956



Mr. William Monroe
March 1, 2006
Page 2

Recommendation 3: The Department should proceed with efforts to establish a data center environment that contains the proper environmental controls to ensure the safety of its computer equipment.

Response: The Department has committed to moving the server room assets to the Shared Resource Center. This is currently scheduled to be completed by June 30, 2006.

Recommendation 4: The Department's current Information Systems Development Methodology (ISDM) should be expanded to include all applicable aspects of recommended practices with the STO rules, to ensure that a proper IT life cycle process is established.

Response: The Department will expand the current ISDM to include those applicable aspects of the recommended practices within the STO rules.

The Department appreciates the time and effort of your staff in assisting the agency in developing improvements to the processes and procedures employed to accomplish the mission of our agency.

Sincerely,

Thaddeus L. Cohen, A.I.A.
Secretary

TLC/ack

THIS PAGE INTENTIONALLY LEFT BLANK