



Auditor General

William O. Monroe, CPA



**FLORIDA DEPARTMENT OF STATE
SELECTED INFORMATION SYSTEMS FUNCTIONS
INFORMATION TECHNOLOGY REVIEW
For the Period July 18, 2000, Through September 22, 2000**

Introduction

The Division of Corporations (Division) within the Florida Department of State (Department) serves as the State's central repository for a variety of business entity filings and annual reports, Uniform Commercial Code financing statements, trade and service mark registrations, fictitious name registrations, and tax lien recordings. The strategic issue of the Division is to maintain a single central commercial repository for recording and retrieving all commercial information and related documentation with convenient public access and use in support of Florida's economic and commercial growth.

We reviewed selected information systems functions applicable to the Division, in part, to evaluate the extent of progress the Department has made in correcting information systems control deficiencies we previously noted in paragraphs 22 through 60 of Report No. 13177, dated March 25, 1998. As discussed in the following report sections, the deficiencies continued to exist at the Department during the period July 18, 2000 through September 22, 2000.

As part of this evaluation, we noted that the Department recently contracted with Science Applications International Corporation (SAIC) to conduct an in-depth review related to access controls and vulnerabilities. SAIC described the results of its review in a Security Services Vulnerability Report (SSVR), dated June 28, 2000. In its report, SAIC noted certain access control deficiencies similar to those found in our review. As part of the Department's agreement with SAIC, the company also conducted a vulnerability assessment of the Department of Management

Services. Both assessments were paid for using funds from the Department's Division of Licensing Trust Fund. Sufficient justification was not provided by the Department to demonstrate the benefit to the Division's licensing activities of the Department of Management Services' assessment. This matter is discussed further in Finding No. 3.

Finding No. 1:

The Department should enhance the effectiveness of systems development and maintenance controls.*

The effective use of a systems development methodology is the key to developing and maintaining information systems that meet the constantly changing needs of the organization. Procedures, including standards for all work products and the review and approvals for these work products, tools, and techniques are used to create, refine, and control the work products that are produced at each stage of the systems development life cycle. An organization's systems development methodology should be formalized and documented to provide consistent guidance to all staff at all levels of skill and experience. Management should maintain control of changes to ensure that all changes are authorized and properly tested, and a separation between the preparation of the change and the implementation of the change in the production environment is maintained.

The Department's Information Systems Development Methodology (ISDM) addresses such issues as project

* Denotes Prior Audit Report Comment, Auditor General Report No. 13177, Dated March 25, 1998

planning and management, system design, system development, and implementation of the Department's computer environment. However, we noted that the Department's ISDM did not require the following elements: the testing of modifications by staff other than the individual who coded the program; supervisory approval for program moves into the production environment; or, the supervisory review of program move activity. In addition, we noted that the ISDM did not include a requirement for the updating of design and functional specifications to reflect modifications performed. Not only have these issues been omitted from written policy; we noted that these controls are not performed on a regular basis.

The absence of the above controls increases the risk that erroneous or incomplete programs could be moved into operation without timely detection by management, and could hinder the efforts of systems and user staff to maintain, operate, and use the Division's application systems.

Recommendation:

The Department should develop and enforce policies and procedures to ensure that modifications are tested by staff independent of the individuals who code changes; supervisory approval is obtained for moving programs into the production environment; and that program move activity is reviewed on a regular basis.

Agency Response:

"We concur with the recommendation. The current Information Systems Development Methodology (ISDM) document does not require the elements enumerated in the audit findings (testing of modifications by staff other than the individual who coded the program; supervisory approval for program moves into production; supervisory review of program move activity; updating of design and functional specifications to reflect modifications performed). However, it should be noted that although application development does not follow formal standards, the Division of Corporations does document changes, upgrades, and move activity associated with program modifications. User groups also perform internal testing before any application is moved into production.

"The Department is in the process of revising the current ISDM and plan to have a completed document approved and published prior to June 30, 2001.

"This revised document will incorporate the elements contained in the audit findings."

Finding No. 2:

The Department had not implemented or utilized sufficient access controls to adequately protect programs and data files from improper disclosure and modification or appropriately monitor security/access activities. *

The establishment of access control policies and procedures helps to ensure that management objectives for the protection of information resources will be achieved. Proper access controls are intended, among other things, to prevent or detect unnecessary and/or unauthorized disclosure or modification to programs and data files.

During our review, we identified deficiencies in the access controls implemented by the Department. Specific details of these deficiencies are not disclosed in this report to avoid any possibility of compromising Department information. However, the appropriate Department personnel have been notified of the deficiencies.

Without adequate access controls in place, the risk exists that the Department's information resources may be subject to improper disclosure and/or modification. In addition, unauthorized system actions, should they occur, may not be timely detected.

Recommendation:

The Department should implement the appropriate access controls to enhance the security of data and programs.

Agency Response:

"We concur with the recommendation. The Department has developed an Information Technology Security program, which was approved and implemented on 12 January 2001. Departmental operating procedures governing the various aspects of information technology security have been developed and are currently being implemented. These documents are attached for information and review."¹

* Denotes Prior Audit Report Comment, Auditor General Report No. 13177, Dated March 25, 1998

¹ The documents referenced are confidential information pursuant to Section 282.318(2)(a)3., Florida Statutes, and are not included in this report.

Finding No. 3:

The Department paid for a vulnerability assessment for the Department of Management Services using funds from the Division of Licensing Trust Fund without providing sufficient justification for the use of the Trust Fund moneys for the assessment.

Chapter 493, "Private Investigative, Private Security, and Repossession Services", Florida Statutes, requires regulation of licensed and unlicensed persons and businesses engaged in private security, investigative, and recovery industries. Pursuant to Chapter 493.6117, Florida Statutes, there is created within the Division of Licensing of the Department, a Division of Licensing Trust Fund. According to statutory guidance, the Legislature shall appropriate from the Division of Licensing Trust Fund such amounts as it deems necessary for the purpose of administering the provisions of Chapter 493. Chapter 215.32, Florida Statutes, states that the state agency or branch of state government receiving or collecting trust fund moneys shall be responsible for their proper expenditure as provided by law.

On May 3, 2000, a purchase order was issued in the amount of \$495,231 from the Division of Licensing Trust Fund for the purpose of obtaining a vulnerability assessment from SAIC of the Department of State's corporate and licensing databases. This purchase order also covered a vulnerability assessment for the Department of Management Services. The purchase order amount was within amounts available from the Division of Licensing Trust Fund; however, the authority to spend the money required a budget amendment. Accordingly, a budget amendment was prepared by the Department of State's Director of Administrative Services, and included the vulnerability assessments request for both Departments. The Department of Management Services' central role in State technology was the justification given in the budget amendment for the vulnerability assessment at that Department. The amendment was approved by the Executive Office of the Governor, Office of Policy and Budget. SAIC conducted the assessments and was paid \$495,231.

According to the proposal submitted by SAIC, the assessments for both the Department and the Department of Management Services would be conducted as two independent efforts, although no cost breakdown between the two agencies was provided.

The justification given in the budget amendment request for the Department of Management Services' vulnerability assessment did not sufficiently demonstrate how the assessment benefited the Division's regulatory activities. The Department did not provide further documentation demonstrating the assessment's benefit to the Division. Consequently, we question whether the expenditure was consistent with the intent of the Division of Licensing Trust Fund as set forth in Section 493.6117, Florida Statutes.

Recommendation:

The Department should clearly establish its justification for expenditures to ensure that trust fund moneys are used for their intended purpose.

Agency Response:

"The Department followed established procedures in obtaining spending authority to fund the vulnerability assessment for the Department of State and Department of Management Services. Approval for this action was requested and received from the Office of Policy and Budget within the Executive Office of the Governor on 5/2/2000. The Division of Licensing has seven (7) Regional Offices which utilize the statewide data network that is administered and maintained by the Department of Management Services. These offices transmit confidential information and images on a routine basis; therefore, potential breaches of security of the statewide system is a legitimate concern of the Division, its licensees and clients."

* Denotes Prior Audit Report Comment, Auditor General Report No. 13177, Dated March 25, 1998

Scope, Objectives and Methodology:

The scope and objectives of this review included:

- Evaluating selected information systems functions applicable to the Division of Corporations during the period July 18, 2000 through September 22, 2000.
- Determining the effectiveness of selected general controls.
- Evaluating the extent to which the Department corrected, or is in the process of correcting, Information Systems and Systems Development and Access Control deficiencies disclosed in the prior audit (report No. 13177).

We conducted our audit in accordance with applicable standards contained in *Government Auditing Standards* issued by the Comptroller General of the United States. To meet the audit objectives described above, we:

- Reviewed the prior audit report and working papers;
- Interviewed appropriate Department personnel;
- Reviewed Department written policies and procedures;
- Reviewed applicable Florida Statutes;
- Obtained an understanding of the Department's internal control procedures;
- Reviewed the SSVR, dated June 28, 2000, issued by SAIC for issues related to the Information Systems and Systems Development and Access Control deficiencies disclosed in the prior audit (report No. 13177). The Department contracted with SAIC to perform a vulnerability assessment of information technology and security programs to determine weaknesses and vulnerabilities in existing infrastructure.

Respectfully submitted,



William O. Monroe, CPA

Audit Supervised by:

Tina Greene, CPA*, CISA

Audit Team Leader:

Jennifer Barineau, CPA*, CISA

This report and other Auditor General reports can be obtained on our web site (www.state.fl.us/audgen); by telephone at (850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

Please contact Jon Ingram, CPA. CISA, Audit Manager, with any questions regarding this report. He may be reached via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.*