REPORT NO. 2011-192
JUNE 2011

DEPARTMENT OF REVENUE

SYSTEM FOR UNIFIED TAXATION (SUNTAX)
AND
IMAGING MANAGEMENT SYSTEM (IMS)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

EXECUTIVE DIRECTOR OF THE DEPARTMENT OF REVENUE

Pursuant to Section 20.21(1), Florida Statutes, the head of the Department of Revenue is the Governor and Cabinet, which consists of the Governor, Attorney General, Chief Financial Officer, and Commissioner of Agriculture. Pursuant to Section 20.05(1)(g), Florida Statutes, the Governor and Cabinet is responsible for appointing the Executive Director of the Department of Revenue. Lisa Vickers served as the Executive Director during the period of our audit.

The audit team leader was Daniel Pearce, CISA, and the audit was supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF REVENUE

System for Unified Taxation (SUNTAX)
and
Imaging Management System (IMS)

SUMMARY

Section 20.21(2)(g), Florida Statutes, provides that the Department of Revenue (Department) is responsible for tax processing, including receipts processing, tax returns processing, license registration, and taxpayer registration. Among the systems used by the Department for tax processing are the System for Unified Taxation (SUNTAX) and the Imaging Management System (IMS).

The Department integrated the administration of all taxes into SUNTAX, a single, unified tax system. IMS is used by the Department as a front-end system to initiate the process of tax collection and tax return processing.

Our audit focused on evaluating selected information technology (IT) controls applicable to SUNTAX and IMS. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2009-199. The results of our audit are summarized below:

Finding No. 1: The Department did not timely disable the SUNTAX, IMS operating system, and network access privileges of some former employees and contractors. Additionally, the Department did not conduct periodic reviews of former employee and contractor access privileges in the IMS operating system or the IMS database. Some of these issues were also noted in prior audits of the Department, most recently our report No. 2009-199.

Finding No. 2: Some inappropriate SUNTAX and IMS access privileges existed.

Finding No. 3: Certain Department logical access controls, security logging and monitoring practices, and data transmission controls were deficient or needed improvement. Some of the issues were also noted in prior audits of the Department, most recently our report No. 2009-199.

Finding No. 4: As similarly noted in prior audits of the Department, most recently our report No. 2009-199, program change controls over SUNTAX and IMS needed improvement.

Finding No. 5: Some of the Department's written IT policies and procedures were outdated and contained inaccuracies. The Department also lacked written procedures for some important IMS program change controls.

Finding No. 6: As similarly noted in our report No. 2009-199, some Department employees were granted unnecessary physical access privileges to the rooms that housed the Department's IMS servers.

Finding No. 7: Contrary to the requirements of the State of Florida, *General Records Schedule* for the retention of access control records, the Department did not retain some IMS operating system access control records.

BACKGROUND

SUNTAX is based on Systems, Applications, and Products in Data Processing (SAP), a commercial off-the-shelf enterprise resource planning software package that uses a common framework across all tax types. SUNTAX provides functions such as:

- One-stop registration to establish a taxpayer's account for all taxes in a single system.
- Processing of all financial tax returns, payments, and related correspondence, including electronic filings.

- Posting of financial transactions to the general ledger and taxpayer account records to maintain accurate accounts receivable and payable across tax types, resulting in accurate distribution of collected funds to the proper taxing authority.
- Maintaining a taxpayer account including multiple addresses, status for taxes, and a summary of delinquent tax returns and financial obligations.
- Supporting the collection of delinquent taxes, identifying new taxpayers, and improving compliance of existing taxpayers.

IMS, an in-house developed front-end system, is used to process incoming tax returns and accompanying checks, including the depositing of checks. IMS is also used to scan documents, capture nondepository data, and archive scanned document images.

General Tax Administration (GTA) is the primary user of SUNTAX and IMS. GTA is responsible for the administration of tax collection, tax enforcement, tax processing, taxpayer registration, and fund distribution, as well as providing taxpayer assistance and resolving taxpayer complaints. The Department's Information Services Program (ISP) functions include developing, maintaining, and managing systems for tax return processing and taxpayer registration activities, including SUNTAX and IMS.

There are three components within SUNTAX: R/3 allows the entry of financial accounting transactions, Customer Relationship Management allows the development and management of cases including leads for potential tax recovery and bankruptcy, and Business Warehouse allows the storing of data to run queries.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Timely Disabling of Access Privileges

Effective management of system access privileges includes provisions to timely remove or adjust employee and contractor access privileges when employment or contractual terminations occur. Prompt action is necessary to ensure that access privileges are not misused by the former employee or others. Department policy required user accounts to be inactivated (disabled) promptly upon the departure of personnel.

The Department did not disable the SUNTAX, IMS, and network access privileges of some former employees and contractors in a timely manner, as described in the following paragraphs. The existence of the former employee and contractor access privileges indicated a need for improved Department review of access privileges and increased the risk that access privileges could be misused by former employees or others.

Upon audit request, the Department provided us a list of 275 Department employees and GTA contractors who terminated from employment or contractual services with the Department during the period July 1, 2010, through December 31, 2010. Our comparison of this list to the user access privileges within SUNTAX and IMS disclosed that some access privileges were not timely disabled. Specifically:

- The SUNTAX application access privileges of one former employee and one former contractor were shown as active in a Department access listing dated January 5, 2011, 48 and 158 days after the termination dates of the employee and contractor, respectively. A similar issue was noted in prior audits of the Department, most recently our report No. 2009-199.
- The SUNTAX application access privileges of an additional nine former employees were disabled as of the date of our test but had remained active from 2 to 130 days after the dates the employees terminated. A similar issue was noted in our report No. 2009-199.

- The IMS operating system access privileges of a former employee remained active as of January 13, 2011, 117 days after the date the employee terminated.

For the network, upon audit request, the Department provided us a list of 100 former GTA and ISP employees and GTA contractors. Our review of the network access privileges of a sample of 18 of the 100 former employees and contractors disclosed that the access privileges of 2 employees remained active for 4 and 12 days, respectively, after their dates of termination, after which the access privileges were detected and disabled by Department access control administrators. A similar issue was noted in our report No. 2009-199.

Department access control administrators used monthly reports of terminated employees to verify that access privileges of the terminated employees were appropriately disabled in the SUNTAX application, IMS application, and the Department's network. However, in response to audit inquiry, Department staff indicated that the access control administrator responsible for disabling IMS operating system and database access privileges did not receive the report and, therefore, did not conduct a monthly review to ensure that the access privileges of former employees were appropriately removed.

Recommendation: The Department should ensure that SUNTAX, IMS operating system, and network access privileges of former employees and contractors are disabled in a timely manner. The Department should perform periodic reviews of former employee access privileges within the IMS operating system and the IMS database to ensure that access privileges are appropriately disabled.

Finding No. 2: Appropriateness of Access Privileges

Effective management of employee and contractor access privileges promotes an appropriate separation of duties by ensuring that user access privileges are limited to only what is needed to perform assigned job duties and that employees and contractors are restricted from performing incompatible functions. For example, an appropriate separation of IT duties typically includes restricting programmers from updating production data.

We noted instances where SUNTAX and IMS access privileges were inappropriate. Specifically:

- Of 58 ISP employees and contractors associated with SUNTAX application development, 1 employee and 2 contractors had update access privileges to production data in the SUNTAX production environment, contrary to an appropriate separation of duties.
- Of 14 user accounts with IMS database access privileges, 3 user accounts not assigned to individuals or necessary for system processing existed, and 1 employee had access privileges that exceeded what was necessary to perform his job functions.

The existence of the inappropriate access privileges indicated a need for improved Department review of SUNTAX and IMS access privileges. Without appropriate restriction of access privileges, the risk of unauthorized disclosure, modification, or destruction of data and IT resources was increased.

Recommendation: The Department should limit access privileges to only what is needed in the performance of employee and contractor job functions and implement additional review procedures to ensure that access privileges remain appropriate.

Finding No. 3: Other 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 in the areas of logical access controls, security logging and

monitoring practices, and data transmission controls that were deficient or 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. Some of the issues were also included in prior audits of the Department, most recently our report No. 2009-199. Without adequate security controls in the areas of logical access controls, security logging and monitoring practices, and data transmission 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 appropriate security controls in the areas of logical access controls, security logging and monitoring practices, and data transmission controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Finding No. 4: Program Change Controls

Effective controls over changes to programs are intended to ensure that only approved and properly functioning changes are implemented. Department standards set forth requirements for the documentation of program changes. The Department used automated software to manage and control changes to SUNTAX and IMS.

Rev-Trac was the automated change control software used by the Department to manage and control program changes in SUNTAX and provide centrally managed documentation of program changes. Our audit test disclosed that, for 6 of 30 SUNTAX Rev-Trac change requests completed between July 1, 2010, and December 31, 2010, the maintenance logs (program change history) within the source code of the SUNTAX programs associated with the requests had not been updated, contrary to Department standards. A similar issue was noted in prior audits of the Department, most recently our report No. 2009-199.

The Production Version Control System (PVCS) was the software used by the Department for program version control and revision management for changes to IMS. Sign-offs for each phase of the program change process and post-implementation approvals were controlled and documented utilizing manual approvals and a *PVCS IMS Application Design and Support, Application Signoff Document*. Our review of 30 IMS program changes moved into the production environment between July 1, 2010, and December 31, 2010, disclosed instances where program change documentation was missing. Specifically, upon audit request, Department staff could not provide documentation to support that 24 program changes were approved prior to being moved into the production environment. Additionally, 3 IMS program changes lacked documentation of post-implementation approval. Under these conditions, the risk was increased that unapproved or erroneous IMS program changes could be moved into the production environment without timely detection. A similar issue was noted in prior audits of the Department, most recently our report No. 2009-199.

Recommendation: The Department should follow and adequately document compliance with established program change control procedures to ensure that all program changes are properly approved, documented, and implemented.

Finding No. 5: IT Policies and Procedures

Sound IT management includes the establishment of policies and procedures that describe management's expectations for controlling the Department's IT operations. Written policies and procedures help ensure that management directives are clearly communicated, understood, accepted, and followed by all staff.

Our audit disclosed the following:

- *SUNTAX Security Policies and Procedures* were stored on the Department's internal network for employee reference but were out of date and contained inaccuracies, such as obsolete methods for requesting user access and incorrect password length requirements.
- The Department lacked written procedures for the detailed steps required to move IMS program changes into production.
- The Department lacked written procedures on the use of PVCS for IMS program version control and revision management.
- The procedures for completing the *PVCS IMS Application Design and Support, Application Signoff Document* did not reflect the Department's current practices of approving program changes to be moved into the production environment via e-mail and signing the *Application Signoff Document* after the program change is moved into the production environment.

The above-described inaccuracies in policies and procedures and the absence of written procedures increase the risk that management's expectations will not be properly or consistently communicated, understood, or carried out.

Recommendation: The Department should update and correct inaccuracies in existing policies and procedures and establish written procedures for moving IMS program changes into the production environment and for using PVCS to manage and control IMS changes.

Finding No. 6: Physical Access

Effective IT security includes controls that limit physical access to computer resources. Upon audit request, the Department provided us a listing of employees with physical access privileges to the rooms that house the IMS servers (IMS server rooms). Our audit disclosed that, of the 41 employees with physical access privileges to the IMS server rooms as of January 18, 2011, 3 employees had no apparent business reason for the access privileges. In addition, Department staff could not provide documentation that the appropriateness of physical access privileges to the IMS server rooms had been periodically reviewed.

Under these conditions, the risk was increased that unauthorized employees may misuse or damage the IMS servers, jeopardizing the operation of IMS and the confidentiality, integrity, and availability of IMS data and IT resources. On February 17, 2011, in response to audit inquiry, Department staff removed the IMS server room access privileges of the three employees in question. A similar issue was noted in our report No. 2009-199.

Recommendation: The Department should periodically review the appropriateness of physical access privileges to the IMS server rooms to ensure that access is limited to only those employees who need access to perform their job duties.

Finding No. 7: Access Control Records Retention

The State of Florida, *General Records Schedule GS1-SL for State and Local Government Agencies* (*General Records Schedule*), revised by the Department of State effective August 2010, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment. Contrary to the *General Records Schedule* requirements, the Department did not retain the dates that IMS operating system access privileges were disabled. Without the adequate retention of access control records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of security incidents, should they occur. Additionally, the Department is not in compliance with the State's record retention requirements.

Recommendation: The Department should ensure that access control records are retained as required by the *General Records Schedule*.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2009-199.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit from November 2010 through March 2011 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.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to SUNTAX and IMS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations; and whether the Department had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2009-199.

The scope of this audit focused on evaluating selected IT controls applicable to SUNTAX and IMS, including selected general IT controls over systems development and modification; logical access to operating systems, database, programs, and data; and computer operations. The audit also included selected application controls and selected user controls applicable to SUNTAX and IMS.

In conducting our audit, we:

- Interviewed Department personnel.
- Inspected Department IT policies and procedures.
- Observed and evaluated the effectiveness of selected input, processing, and output controls, as well as exception reporting and manual follow-up procedures, for SUNTAX and IMS. As part of the evaluation, we

tested the appropriateness of user transaction thresholds for compromises and corrections, the appropriateness of the Department's follow-up on 37 SUNTAX and IMS errors related to failed file loads, the appropriateness of the Department's follow-up on 36 IMS errors related to remittance processing, and the accuracy of 52 remittance transactions processed by IMS.

- Evaluated the effectiveness of selected controls for promoting data accuracy and the proper administration of taxes.
- Observed and evaluated the effectiveness of selected logical access controls in ensuring that access privileges to SUNTAX, IMS, operating systems, and databases were appropriate.
- Evaluated the appropriateness of access privileges to the IMS application, SUNTAX and IMS operating systems, and SUNTAX and IMS databases. Evaluated the appropriateness of access privileges to selected SUNTAX application functions. Evaluated whether selected access privileges to the IMS application were appropriately authorized.
- Evaluated the effectiveness of controls for timely disabling the access privileges of former employees and contractors. Specifically, we reviewed a list of 275 employees and GTA contractors who terminated from employment or contractual services with the Department during the period July 1, 2010, through December 31, 2010, to determine if access privileges to the network and the SUNTAX and IMS applications, operating systems, and databases were disabled. Where adequate documentation was available, we determined if access privileges were timely disabled in relation to their termination dates. Additionally, we selected a sample of 18 individuals from a list of 100 former ISP and GTA employees and GTA contractors to determine if network access privileges had been timely disabled in relation to their termination dates.
- Tested the effectiveness of selected controls over the authorization, testing, approval, and documentation of 30 SUNTAX Rev-Trac change requests and 30 IMS program changes between July 1, 2010, and December 31, 2010.
- Evaluated the adequacy of security controls over selected internal and external connections to SUNTAX and IMS.
- Evaluated the adequacy of physical security controls to IMS IT resources located within the Department's facilities.

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 operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated June 20, 2011, the Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT A.

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT A
MANAGEMENT'S RESPONSE

FLORIDA
DEPARTMENT OF REVENUE

Executive Director
Lisa Vickers

Child Support Enforcement
Ann Coffin
Director

General Tax Administration
Jim Evers
Director

Property Tax Oversight
James McAdams
Director

Information Services
Tony Powell
Director

June 20, 2011

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

Dear Mr. Martin:

As required by section 11.45(4)(d), Florida Statutes, enclosed is the Department's response to the preliminary and tentative findings and recommendations of your audit of the Department of Revenue System for Unified Taxation (SUNTAX) and Imaging Management System (IMS).

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact Teresa Wood, Director of Auditing, at 717-7598.

Sincerely,

Lisa Vickers

LV/tw

Enclosure

cc: Sharon Doredant, Inspector General
Teresa Wood, Director of Auditing

Tallahassee, Florida
32399-0100
www.myflorida.com/dor

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Revenue
Auditor General SUNTAX and IMS Information Technology Audit
Preliminary and Tentative Response

Finding 1: The Department did not timely disable the SUNTAX, IMS operating system, and network access privileges of some former employees and contractors. Additionally, the Department did not conduct periodic reviews of former employee and contractor access privileges in the IMS operating system or the IMS database. Some of these issues were also noted in prior audits of the Department, most recently our report No. 2009-199.

Recommendation: The Department should ensure that SUNTAX, IMS operating system, and network access privileges of former employees and contractors are disabled in a timely manner. The Department should perform periodic reviews of former employee access privileges within the IMS operating system and the IMS database to ensure that access privileges are appropriately disabled.

Response: The Department has implemented an automated process, via our internal phonebook and if utilized in a diligent manner by supervisors, informs SUNTAX security administrators of the termination of employees. This is also the case if contractors are listed in the department phonebook. However, if they are not, it is then incumbent upon the supervisor of the contractor to notify SUNTAX security. The Department is in the process of adding all contractors to the internal phonebook. In the case of periodic reviews, a follow-up monthly termination report is provided from the Executive Program that contains a listing of all employees that have separated from the department. These notifications are reviewed as received to ensure access to SUNTAX, IMS has been removed. A yearly review of all access to SUNTAX, IMS is performed by the security administrator to ensure that employees that transfer or leave the department no longer have access.

Finding 2: Some inappropriate SUNTAX and IMS access privileges existed.

Recommendation: The Department should limit access privileges to only what is needed in the performance of employee and contractor job functions and implement additional review procedures to ensure that access privileges remain appropriate.

Response: The Department will review the current process for creating, maintaining and periodically reviewing employee and contractor access privileges. The result will be to determine where controls can be implemented and/or strengthened to adequately manage the appropriateness of access privileges.

Finding 3: Certain Department logical access controls, security logging and monitoring practices, and data transmission controls were deficient or needed improvement. Some of the issues were also noted in prior audits of the Department, most recently our report No. 2009-199.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Revenue
Preliminary & Tentative Findings – Response
AG SUNTAX/IMS IT Audit

Recommendation: The Department should implement appropriate security controls in the areas of logical access controls, security logging and monitoring practices, and data transmission controls to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

Response: The Department will, based on available system functionality, funding, and human resources implement appropriate security controls in the areas of logical access controls, security logging and monitoring practices, and data transmission controls.

Finding 4: As similarly noted in prior audits of the Department, most recently our report No. 2009-199, program change controls over SUNTAX and IMS 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 approved, documented, and implemented.

Response: In July of 2011, the Information Services Program will fully implement their Release and Deployment Process. With the rollout of this process, controls will be implemented and existing ones strengthened. This will help to ensure greater compliance with program change control procedures and adequately ensure that all program changes are properly approved, documented, and implemented.

Finding 5: Some of the Department's written IT policies and procedures were outdated and contained inaccuracies. The Department also lacked written procedures for some important IMS program change controls.

Recommendation: The Department should update and correct inaccuracies in existing policies and procedures and establish written procedures for moving IMS program changes into the production environment and for using PVCS to manage and control IMS changes.

Response: We have opened an internal service ticket to update and correct the inaccuracies in existing policies and procedures. The due date is 6/30/11. In July of 2011, the Information Services Program will fully implement their Release and Deployment Process. This process will implement stronger control procedures for the release of changes. It will also serve as a catalyst to review, update and correct inaccuracies in existing policies and procedures and establish written procedures for moving IMS program changes into the production environment and for using PVCS to manage and control IMS changes.

Finding 6: As similarly noted in our report No. 2009-199, some Department employees were granted unnecessary physical access privileges to the rooms that housed the Department's IMS servers.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Revenue
Preliminary & Tentative Findings – Response
AG SUNTAX/IMS IT Audit

Recommendation: The Department should periodically review the appropriateness of physical access privileges to the IMS server rooms to ensure that access is limited to only those employees who need access to perform their job duties.

Response: The General Tax Administration has reviewed, and are currently reviewing, employee physical access privileges to the IMS server rooms for business needs. Controls will be implemented and strengthened as appropriate.

Finding 7: Contrary to the requirements of the State of Florida, General Records Schedule for the retention of access control records, the Department did not retain some IMS operating system access control records.

Recommendation: The Department should ensure that access control records are retained as required by the General Records Schedule.

Response: We will determine the logistics (available funds, storage infrastructure and resources) involved in adequately ensuring that access controls records are kept according to the standards provided by *General Records Schedule*.