REPORT NO. 2015-006
AUGUST 2014

DEPARTMENT OF REVENUE

SYSTEM FOR UNIFIED TAXATION (SUNTAX)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

HEAD OF THE DEPARTMENT OF REVENUE AND THE EXECUTIVE DIRECTOR

Pursuant to Section 20.21(1), Florida Statutes, the head of the Department of Revenue is the Governor and Cabinet, which includes the 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 employing an Executive Director of the Department of Revenue. Marshall Stranburg served as the Executive Director during the audit period.

The audit team leader was Wayne Revell, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF REVENUE

System for Unified Taxation (SUNTAX)

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 is the System for Unified Taxation (SUNTAX). The Department integrated the administration of all taxes into SUNTAX, a single, unified tax system.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to SUNTAX. We also determined the status of corrective actions regarding selected audit findings included in our report No. 2011-192. Corrective actions were not taken for three of the five prior audit findings included in prior audit reports, most recently report No. 2011-192. In addition, one prior audit finding was only partially corrected.

Our audit disclosed areas in which enhancements in SUNTAX IT controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: Some inappropriate SUNTAX access privileges existed. In addition, the Department did not timely deactivate the SUNTAX application access privileges of some former employees.

Finding No. 2: The Department had not established a review schedule to ensure that reviews of user access privileges to SUNTAX were conducted on a periodic basis.

Finding No. 3: Certain Department security management, logical access, monitoring and logging, and data transmission controls needed improvement.

Finding No. 4: The Department's documentation of program change requests needed improvement.

Finding No. 5: The Department had not performed a comprehensive risk assessment for SUNTAX.

Finding No. 6: The Department had not tested its SUNTAX disaster recovery plan since 2012.

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.

General Tax Administration (GTA) is the primary user of SUNTAX. 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.

There are four components within SUNTAX: Enterprise Core Component 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, Business Warehouse allows the storage of data to run queries, and SAP NetWeaver Enterprise Portal allows internal and external users to view reports and Florida counties to file and pay clerk fees.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: 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 job duties typically includes restricting programmers from updating production data. Effective management of access privileges also includes provisions to timely remove employee access privileges when employment terminations occur. Prompt action is necessary to ensure that access privileges are not misused by the former employee. We noted instances where SUNTAX access privileges were inappropriate. Specifically:

- Of 52 Department employees and contractors with SUNTAX development keys (roles) as of March 17, 2014, 21 employees and 9 contractors also had update access privileges to SUNTAX as a user allowing them to update production data, contrary to an appropriate separation of duties. A similar issue was noted in our report No. 2011-192.
- Of 73 SUNTAX operating system and database active users as of March 28, 2014, access was not appropriate for 26 of these users. Specifically, the 26 users were granted access in excess of what was needed for their current job duties.
- The SUNTAX application access privileges of two former employees were shown as active in a Department access listing dated March 17, 2014, or 224 and 247 days after the employment termination dates of the employees. Furthermore, the SUNTAX application access privileges of an additional six former employees were deactivated as of the date of our test but had remained active from 3 to 8 days after the dates the employees terminated employment. The access privileges of the former employees had not been used subsequent to their employment termination dates. A similar issue was noted in prior audits of the Department, most recently our report No. 2011-192.

The existence of the inappropriate access privileges indicated a need for improved Department review of SUNTAX access privileges as also discussed below in Finding No. 2. Without appropriate restriction and timely deactivation of access privileges, the risk that unauthorized disclosure, modification, or destruction of data and IT resources may occur is increased.

Recommendation: The Department should limit access privileges to only what is needed in the performance of employee and contractor job duties. Additionally, the Department should ensure that the access privileges of former employees are deactivated in a timely manner upon termination.

Finding No. 2: Periodic Review of User Access Privileges

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic reviews of user access privileges help ensure that access provided to each user remains appropriate.

The Department had performed a review of user access privileges in 2013 but had not established a review schedule to ensure that reviews are conducted on a periodic basis. As indicated by the excessive access privileges noted in Finding No. 1 above, the lack of scheduled periodic reviews of access privileges to SUNTAX increases the risk that inappropriate access privileges may not be timely detected and may result in unauthorized or inappropriate changes to SUNTAX data and programs.

Recommendation: The Department should establish a review schedule to ensure that reviews of user access privileges to SUNTAX are conducted on a periodic basis.

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 security management, logical access, monitoring and logging, and data transmission 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. Some of the issues were also communicated to Department management in connection with prior audits of the Department, most recently our report No. 2011-192. Without adequate security controls in the areas of security management, logical access, monitoring and logging, and data transmission, the risk is increased that the confidentiality, integrity, and availability of data and IT resources may be compromised.

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

Finding No. 4: Documentation of Program Change Requests

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. 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 4 of 36 SUNTAX Rev-Trac change requests requiring maintenance logs (program change history) completed between July 1, 2013, and March 17, 2014, the maintenance logs within the source code of the SUNTAX programs associated with the requests had not been updated, contrary to Department standards. A

[1] Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code; and existing contracts of the AEIT to the AST.

similar issue was noted in prior audits of the Department, most recently our report No. 2011-192. The lack of program change documentation may limit the Department's ability to identify the changes made to the program code.

Recommendation: The Department should follow and comply with established standards for the documentation of all program changes.

Finding No. 5: Risk Assessment

AEIT Rule 71A-1.020(2), Florida Administrative Code, provides that agencies shall implement a documented risk management program, including risk analysis for high-impact information resources. One component of a risk management program is a comprehensive risk assessment. A risk assessment is the process of identifying, prioritizing, and estimating information security risks.

The Department had completed an AEIT – Office of Information Security *2011 Florida Enterprise Information Security Risk Assessment Survey*. However, we noted that the Department had not performed a comprehensive risk assessment for SUNTAX. Under these conditions, the risk was increased that unmitigated risks or vulnerabilities may result that could impact the operations of the Department and the confidentiality, integrity, and availability of Department data and IT resources.

Recommendation: The Department should, pursuant to AEIT Rules, perform a comprehensive risk assessment for SUNTAX.

Finding No. 6: Disaster Recovery Plan Testing

AEIT Rule 71A-1.012(5), Florida Administrative Code, provides that Information Technology Disaster Recovery Plans shall be tested at least annually and the results of the annual exercise shall document those plan procedures that were successful and modifications required to correct the plan. Furthermore, the Department's *Information Technology Service Management Continuity Management Procedures* provides that service continuity tests be conducted, at least annually, in accordance with the Department's Service Continuity Plan.

Department staff indicated that the Disaster Recovery Plan for SUNTAX was last tested on December 19, 2012. Without timely testing of the SUNTAX Disaster Recovery Plan, the Department's ability to efficiently and effectively continue operations with minimal loss in the event of a processing disruption may be limited.

Recommendation: The Department should conduct annual testing of its SUNTAX Disaster Recovery Plan to validate the plan and determine the areas in the plan that need to be modified.

PRIOR AUDIT FOLLOW-UP

The Department had taken corrective actions for one of the five findings included in our report No. 2011-192 that were applicable to the scope of this audit. Corrective actions were not taken for three of the five prior audit findings as described in the findings above. In addition, one prior audit finding was only partially corrected. Two prior audit findings included in our report No. 2011-192 were not in the scope of this audit.

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 in March and April 2014 in accordance with 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 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; and the safeguarding of IT resources. An additional objective was to determine the extent to which the Department had corrected, or was in the process of correcting, deficiencies disclosed in audit report No. 2011-192 that were within the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to SUNTAX during the period July 2013 through April 2014. The audit included selected business process application controls over transaction data input, processing, and output applicable to SUNTAX and selected application-level general controls related to security management, application access, configuration management, and contingency planning.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls and IT controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective IT operational policies, procedures, or practices. The focus of this IT operational audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of the audit, the audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the purpose or goals involving compliance requirements for SUNTAX.
- Obtained an understanding of the data and business process flows for SUNTAX.
- Obtained an understanding of the IT computing platforms for SUNTAX.
- Obtained an understanding of the information security program, including procedures for security administration for SUNTAX.
- Obtained an understanding of SUNTAX configuration management processes.
- Documented any significant changes which had occurred in SUNTAX, including policies, procedures, hardware, software, organizational structure, and personnel related to SUNTAX.
- Observed and evaluated transaction data input, processing, and output controls that ensure the completeness, accuracy, validity, and confidentiality of SUNTAX data.
- Evaluated application security management controls related to SUNTAX.
- Evaluated the effectiveness of selected SUNTAX access controls, including controls over user authentication, logical access, sensitive and confidential data, and logging.
- Evaluated application configuration management controls related to SUNTAX.
- Evaluated contingency planning controls related to SUNTAX.
- Evaluated the effectiveness of the SUNTAX program change management process. Specifically, we reviewed 40 of 1,008 completed program changes from July 1, 2013, through March 17, 2014, to determine whether program changes were authorized, tested, approved, and appropriately moved to production.
- Evaluated the appropriateness of administrator access privileges granted to the SUNTAX operating system and database.
- Evaluated the appropriateness of developer access privileges granted to the SUNTAX production application environment.
- Evaluated the effectiveness of the Department's controls regarding the removal of access privileges to the SUNTAX application for terminated users.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe those matters requiring corrective action.

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 August 7, 2014, the Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

FLORIDA
DEPARTMENT OF REVENUE

Executive Director
Marshall Stranburg

Child Support Enforcement
Ann Coffin
Director

General Tax Administration
Maria Johnson
Director

Property Tax Oversight
James McAdams
Director

Information Services
Damu Kuttikrishnan
Director

Tallahassee, Florida 32399-0100

August 7, 2014

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, attached is the Department's response to the preliminary and tentative findings and recommendations included in your report for the audit of the Department of Revenue System for Unified Taxation (SUNTAX).

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact Marie Walker, Director of Auditing, at 717-7598 or walkem@dor.state.fl.us.

Sincerely,

Marshall Stranburg

MS/mw

Attachment

cc: Arthur Hart, Audit Manager
T. Wayne Revell, Audit Coordinator
Andrea Moreland, Deputy Executive Director
Maria Johnson, General Tax Administration Program Director
Damu Kuttikrishnan, Information Services Program Director
Sharon Doredant, Inspector General
Marie Walker, Director of Auditing

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Revenue
Auditor General SUNTAX Audit
Preliminary and Tentative Response

Finding 1: Some inappropriate SUNTAX access privileges existed. In addition, the Department did not timely deactivate the SUNTAX application access privileges of some former employees.

Recommendation: The Department should limit access privileges to only what is needed in the performance of employee and contractor job duties. Additionally, the Department should ensure that the access privileges of former employees are deactivated in a timely manner upon termination.

Response: We agree with your findings and recommendations, and are planning more in-depth reviews of both user privileges and role content.

Finding 2: The Department had not established a review schedule to ensure that reviews of user access privileges to SUNTAX were conducted on a periodic basis.

Recommendation: The Department should establish a review schedule to ensure that reviews of user access privileges to SUNTAX are conducted on a periodic basis.

Response: We agree with the finding and recommendation. We plan to comply with the process which requires annual reviews of SUNTAX user access privileges. An annual review was initiated July 2014.

Finding 3: Certain Department security management, logical access, monitoring and logging, and data transmission controls needed improvement.

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

Response: We agree with the finding and recommendation. We will work to implement improvements and increase security controls, and should have these in place by October 1, 2014.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Revenue
Auditor General SUNTAX Audit
Preliminary and Tentative Response

Finding 4: The Department's documentation of program change requests needed improvement.

Recommendation: The Department should follow and comply with established standards for the documentation of all program changes.

Response: Controls are in place to ensure the logs are maintained. We have improved oversight to comply with the standards. We consider this finding complete.

Finding 5: The Department had not performed a comprehensive risk assessment for SUNTAX.

Recommendation: The Department should, pursuant to AEIT Rules, perform a comprehensive risk assessment for SUNTAX.

Response: A comprehensive risk assessment of SUNTAX was completed on July 25, 2014. Risks have been identified and ranked for prioritization based on impact and probability. We consider this finding complete.

Finding 6: The Department had not tested its SUNTAX disaster recovery plan since 2012.

Recommendation: The Department should conduct annual testing of its SUNTAX Disaster Recovery Plan to validate the plan and determine the areas in the plan that need to be modified.

Response: We agree with the finding and recommendation. A test of the SUNTAX Disaster Recovery Plan is scheduled for October 2014.