REPORT NO. 2009-199
APRIL 2009

DEPARTMENT OF REVENUE

SYSTEM FOR UNIFIED TAXATION (SUNTAX)

AND

IMAGING MANAGEMENT SYSTEM (IMS)

Information Technology Operational Audit

October 2008 Through January 2009
and Selected Actions Through February 5, 2009

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 Echeverri served as the Executive Director during the audit period.

The audit team leader was Suzanne Varick, CPA, 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 audit reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; 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, including related interfaces with other systems during the period October 2008 through January 2009 and selected actions through February 5, 2009. We also determined the status of corrective actions regarding prior audit findings disclosed in our report No. 2008-097. The results of our audit are summarized below:

Finding No. 1: **Contrary to Section 119.071(5)(a)2.a., Florida Statutes, the Department used employee social security numbers (SSNs) without specific authorization in law or without having established the imperative need to use the SSN for the performance of its duties and responsibilities as prescribed by law.**

Finding No. 2: **As similarly noted in our report No. 2008-097, former employee and contractor access privileges in SUNTAX and the network had not been removed in a timely manner.**

Finding No. 3: **We noted an instance where a user had inappropriate access privileges to SUNTAX. In addition, as similarly noted in our report No. 2008-097, controls related to the authorization of IMS user access needed improvement.**

Finding No. 4: **Certain user identifications (IDs) and passwords were being shared by Department employees.**

Finding No. 5: **In addition to the matters discussed in Finding Nos. 1 through 4 and 10, certain Department security controls were deficient. Some of the issues were also included in our report No. 2008-097.**

Finding No. 6: **As similarly noted in our report No. 2008-097, program change controls over SUNTAX and IMS needed improvement.**

Finding No. 7: **The Department lacked effective procedures for addressing data errors generated during the load process of data into SUNTAX.**

Finding No. 8: **A programming error existed within the approval process for compromise waivers.**

Finding No. 9: **Off-site backup procedures needed improvement.**

Finding No. 10: **The Department's written IT procedures needed improvement.**

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.

SUNTAX was implemented in phases. The last major tax to be brought into SUNTAX, Unemployment Compensation, was implemented in March 2008.

IMS, an in-house developed front-end system, is used to process incoming tax returns and accompanying checks, including the mailing of receipts and 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 (CRM) allows the development and management of cases including leads for potential tax recovery and bankruptcy, and Business Warehouse (BW) allows the storing of data to run queries.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Use of SSNs

Section 119.071(4)(a)1., Florida Statutes, provides that all employee SSNs held by an agency are confidential and exempt from public inspection. Pursuant to Section 119.071(5)(a)2.a., Florida Statutes, an agency may not collect an individual's SSN unless the agency has stated in writing the purpose for its collection and unless the agency is specifically authorized by law to do so or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law.

The Department collected and used employee SSNs in the network operating system and the Learning Management System (LMS), as well as on various documents and reports. Although the Department stated in writing the purpose for its collection of SSNs, no specific authorization existed in law for the Department to collect the SSNs of network and LMS users and the Department had not established the imperative need to use the SSN, rather than another number. The use of the SSN is contrary to State law and increases the risk of improper disclosure of SSNs.

Recommendation: The Department should comply with State law by clearly establishing why the use of employee SSNs is imperative for the Department to perform its duties and responsibilities or alternatively establish another number to be used rather than the SSN for these purposes. Additionally, the Department should review its practice of placing the SSN on various documents and reports and discontinue the practice whenever practicable to minimize the risk of exposing the SSN to employees or others who have no business need to view the number.

Finding No. 2: Former Employee and Contractor Access Privileges

Effective management of system access privileges includes provisions to timely remove or adjust employee and contractor access privileges when employment or contract terminations occur. Prompt action is necessary to ensure that access privileges are not misused by the former employee or others.

Department procedures state that SUNTAX user accounts are to be inactivated (disabled) on the effective date of employment or contract termination. Department procedures further state that network user accounts are to be disabled upon termination. Our review of access privileges for the three components of SUNTAX and the network disclosed instances where the access privileges of Department employees and contractors who terminated employment or whose contract expired during the period July 1, 2008, through November 18, 2008, had not been timely removed.

Specifically, for SUNTAX, upon audit request, the Department provided us a list of 91 GTA and ISP former employees and contractors. We noted instances where, as similarly noted in our report No. 2008-097, the SUNTAX access privileges to one or more of the R/3, CRM, and BW components had not been timely inactivated, increasing the risk that the access privileges could be misused by the former employees, contractors, or others. Specifically, from a sample of 15 of the 91 former GTA and ISP employees and contractors, the access privileges of 3 employees were not timely inactivated. Through the Department's internal monthly review, the access privileges for these 3 employees were inactivated 34 days after termination of employment with the exception of 1 employee's access to the SUNTAX CRM component which was inactivated 140 days after termination of employment based on our audit inquiry. Our review indicated that the access privileges of these 3 employees had not been used subsequent to the employees' termination of employment.

Through additional audit procedures, we noted another former contractor whose SUNTAX R/3 and CRM component access privileges remained active for 342 days after the end of the contract. In response to audit inquiry, the Department inactivated the accounts on January 15, 2009, and determined that the access privileges had not been used after the contract expiration date.

For the network, upon audit request, the Department provided us a list of 314 former employees and contractors. From a sample of 30 of the 314 former employees and contractors, we noted that 1 contractor's access privileges remained active for 182 days after the end of the contract, increasing the risk that the access privileges could be misused by the former contractor or others. In response to audit inquiry, Department staff disabled the account and determined that the account had not been used after the contract expiration date.

For 12 of the 30 network accounts, the Department could not demonstrate, of record, whether the access privileges had been disabled timely. Specifically:

- Nine network accounts, though disabled at the time of our testing, had no expiration date or time set. It was the Department's stated practice to set an expiration date and time on network accounts at the time a termination form was received. The network access privileges of the nine former employees had not been used after the employees' terminations.

- The network accounts of two former employees and one contractor did not exist at the time of our testing, having been inadvertently deleted by the Department. The State of Florida, General Records Schedule for State and Local Government Agencies, Schedule GS1-GL, revised by the Department of State effective September 2007, provides that access control records must be retained for one anniversary year after superseded or after the employee separates from employment.

Recommendation: The Department should ensure that SUNTAX and network access privileges of former employees and contractors are removed in a timely manner and that access control records are retained as provided in the General Records Schedule.

Finding No. 3: Management of User Access Privileges

An important aspect of IT security management is the establishment of system access privileges that restrict end users to only those system functions necessary to perform their assigned duties. Effective access controls include the use of access authorizations on standard forms that are maintained on file and approved by senior management. Additionally, properly configured access privileges help enforce an appropriate separation of incompatible duties and minimize the risk of unauthorized system actions. The periodic review of access authorization listings by system owners and management helps ensure that privileges remain commensurate with employee job duties. Appropriate access controls also include provisions for user access rights to data to be in line with defined business needs and job functions.

For SUNTAX, the following aspects of user access controls needed improvement:

- Of the 17 employees with access privileges to unemployment tax functions within SUNTAX as of January 5, 2009, and selected for testing, 1 employee had update access privileges that were not necessary for his job functions. Under these conditions, the risk was increased of unauthorized disclosure, modification, or destruction of data and IT resources.
- The Department did not perform periodic reviews of SUNTAX access privileges, including SUNTAX access privileges granted to Department employees and contractors through the unemployment tax Enterprise Portal (ePortal). Without a periodic review of user access privileges, the risk is increased that inappropriate and unauthorized access may not be timely detected.

For IMS, as similarly noted in our report No. 2008-097, the following aspects of user access controls needed improvement:

- For 2 of the 15 IMS user accounts sampled, the employees had access privileges to IMS functions that exceeded the privileges requested on their IMS User Access Request forms. Failure to document access authorizations increases the risk of inappropriate access and unauthorized use, disclosure, or modification of data and programs. In response to audit inquiry, the Department corrected the IMS User Access Request forms for these two employees to match the access privileges that existed in the system.
- Both of the employees noted above also had access to IMS that exceeded what was necessary for their job functions and was contrary to an appropriate separation of duties. One of the employees was also noted in two previous audits as having excessive access. Although these two employees functioned as system administrators, their access privileges included operational functions in IMS. Absent system access privileges that enforce an appropriate separation of duties, the risk is increased that erroneous or fraudulent transactions could be processed. In response to audit inquiry, the Department adjusted the IMS access privileges of the two employees to be consistent with their job functions.

Recommendation: The Department should implement appropriate controls to ensure that access privileges granted correspond to the access privileges requested by the employees' supervisors. The Department should also perform periodic reviews of access privileges to ensure that access privileges are appropriate and commensurate with users' job functions.

Finding No. 4: User Identification and Authentication

Effective access controls include a process for the unique identification and authentication of system users. The unique identification of system users allows management to affix responsibility for system activity to an individual person.

Our review of the Oracle databases containing SUNTAX information disclosed instances where Department employees shared user IDs and passwords for authentication. Specifically, one primary administrator and three backup administrators within the BASIS Systems Support Group administer the Oracle databases by sharing the delivered Oracle SYS and SYSTEM user IDs and corresponding passwords. The sharing of user IDs and passwords may limit the Department's ability to assign responsibility for system activities.

Recommendation: The Department should cease the practice of allowing users to share user IDs and passwords. Each system user should be assigned a unique user ID with a corresponding password.

Finding No. 5: 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 related to the network, SUNTAX, IMS, and Oracle databases that were deficient, in addition to the matters discussed in Finding Nos. 1 through 4 and 10. 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 our report No. 2008-097. 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. 6: Program Change Controls

Effective controls over changes to programs are intended to ensure that only authorized and properly functioning changes are implemented. Rev-Trac was the automated change control tool used by the Department to manage and control program changes in SUNTAX and provide centrally managed documentation of program changes.

Our review of 30 SUNTAX program changes disclosed instances where, as similarly noted in our report No. 2008-097, one or more of the forms of program change documentation required by Department procedures and standards were missing. Specifically:

- Eight program changes lacked a Rev-Trac History Log that would have provided the requestor name, description of the program change, batch job or transaction code, testing method, and the date the program change was needed in production;

- Eight program changes lacked new or updated program change specifications that should have been attached to the Rev-Trac requests; and
- Ten program changes lacked a maintenance log (program change history) within the source code of the program.

The Production Version Control System (PVCS) was used for program version control and revision management for changes to IMS. Approvals and signoffs for each phase of the program change process were controlled and documented utilizing manual approvals and a PVCS IMS Application Design and Support, Application Signoff Document (PVCS form).

Our review of the IMS program change process for 30 IMS changes disclosed the following deficiencies, as similarly noted in our report No. 2008-097:

- Twenty program changes lacked evidence of authorization.
- Twenty program changes did not have the required Intranet Project Management System number or Helpdesk Expert Automation Tool (HEAT) ticket number properly documented in the program change history.
- Two program changes lacked a PVCS form and, as a result, the Department could not demonstrate that the changes were tested by someone independent of the programmer, appropriately approved for production, or appropriately implemented.
- For the remaining 28 program changes where a PVCS form was provided:
  - Four program changes lacked evidence that the change was tested by someone independent of the programmer.
  - One program change lacked evidence that the change was appropriately approved for production.
  - Two program changes lacked certain required signatures on the PVCS form evidencing that the change was appropriately implemented.

Without adequate program change controls, the risk is increased that unauthorized or erroneous programs could be moved into the production environment without timely detection.

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

Finding No. 7: SUNTAX Data Error Follow-Up

Effective exception reporting procedures allow erroneous transactions to be identified without disruption of other transactions. The periodic review of exception reports and prompt follow-up on exceptions increase management's assurance that erroneous actions taken through a computer system, should they occur, will be timely detected and corrected.

During the SUNTAX file load process, file transfer protocol (FTP) input files containing data such as tax returns, payments, or returned checks were edited by SUNTAX. FTP input files containing errors were rejected and saved into a failed file directory. Exception reports were generated online and electronically mailed (e-mailed) to Department staff at the time the file was rejected. The exception reports were automatically deleted after 30 days if not addressed by Department staff. An employee was assigned responsibility for researching, correcting, and resubmitting the file to be reloaded into SUNTAX at which time the failed file was manually deleted from the failed file directory. However, there was nothing that would prevent a failed file from being deleted before the file was reloaded by the assigned employee or other authorized staff. Since the failed files were not archived, there were no

logs of the errors maintained. In addition, effective procedures for the review of the corrections of errors on the failed file did not exist to ensure that the errors were followed up on. Without effective procedures for the review of data errors, there is an increased risk that SUNTAX data, such as tax returns, payments, and returned checks, will not be recorded in SUNTAX in a timely manner.

Recommendation: The Department should implement controls to ensure that all failed files are timely reviewed, corrected, and reloaded into SUNTAX. Additionally, the Department should maintain a history log of failed file exceptions to provide increased assurance that failed files are being corrected and reloaded into SUNTAX in a timely manner.

Finding No. 8: Compromise Waivers

IT controls are intended to ensure that, among other things, all data expected for processing are received and processed completely, accurately and in a timely manner and all output is delivered in accordance with business requirements. Our audit disclosed a programming error within the approval process for compromise waivers.

When the Department agrees to compromise a taxpayer's interest, penalties, or taxes, a compromise waiver transaction is performed. Threshold limits, as set forth in Department of Revenue Rule 12-13.004, Florida Administrative Code, are built into SUNTAX that limit the amounts of interest, penalties, or taxes a specific employee position can waive. When initiating employees create compromise waivers that are above established thresholds, the waivers are routed to approving employees with the appropriate threshold limits to authorize the waivers. Our review of ten compromise waivers between July 2008 and November 2008 disclosed that the approving employees of two compromise waivers were not restricted by their threshold limits established in SUNTAX and set forth in Department of Revenue Rule 12-13.004, Florida Administrative Code, and were able to approve compromise waivers above their thresholds. In response to audit inquiry, Department staff determined that a programming error existed in the way SUNTAX classified the type of waiver that was to be compromised and utilized the wrong waiver type in determining the user's threshold limits. Department staff indicated that a program change was implemented on February 5, 2009, to correct the issue.

Recommendation: The Department should review the appropriateness of compromise waiver approvals that occurred in excess of approval authority set forth in Department rule.

Finding No. 9: Backup Procedures

There are a number of steps that an agency can take to prevent or minimize the damage to automated operations that may occur from unexpected events. One example is routinely backing up data files and programs and securely storing them at an off-site location. Such actions maintain the agency's ability to restore data files, which otherwise may be impossible to recreate if lost.

The Department uses VERITAS NetBackup to create full data and program backups (off-line and root backup images) of its SUNTAX production servers for the three components of SUNTAX: R/3, CRM, and BW. The backup images are copied to tape once a week and cycled off-site. Should the Department need to recover lost data by using the off-site backup tapes, the backup data could be up to approximately nine days old. The Department had not created a formal plan addressing the issue of how a potentially significant data loss from SUNTAX would be restored. The risk is increased that, should an event occur causing a loss of production data and on-site backups, the Department's ability to timely and completely restore the lost information could be hindered.

Recommendation: The Department should review the frequency with which it cycles backups of SUNTAX files to the off-site location and consider a more frequent off-site rotation to further minimize the impact of a system loss.

Finding No. 10: IT Procedures

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

Our audit disclosed the following:

- Although a process existed for the backup, recovery, and tape rotation of SUNTAX data and programs, no written procedures existed for this process.
- No written procedures existed for the security monitoring activities of the SUNTAX security administrator.

The absence of written procedures for data and program backup and security administrator monitoring activities increases the risk that management's expectations will not be properly or consistently communicated, understood, or carried out.

Recommendation: The Department should establish written procedures for the backup of SUNTAX data and programs and security administrator monitoring activities.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for findings included in our report No. 2008-097.

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 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 related 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 to determine whether the Department had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2008-097.

The scope of this audit focused on evaluating selected IT controls applicable to SUNTAX and IMS during the period October 2008 through January 2009 and selected actions through February 5, 2009.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of the Department's program change control procedures, SUNTAX and IMS access and security controls, and SUNTAX and IMS application controls.
- Evaluated the adequacy of security over selected external connections to SUNTAX.
- Observed, documented, and tested the effectiveness of selected logical access controls in ensuring that access to the network, SUNTAX data files, and database was appropriately restricted.
- Observed, documented, and tested the effectiveness of selected IMS application access controls.
- Observed, documented, and tested the effectiveness of selected controls over the authorization, testing, approval, and documentation of SUNTAX and IMS application program modifications.
- Observed, documented, and tested the appropriateness of selected controls surrounding the backup of SUNTAX programs and data.
- Observed, documented, and tested the effectiveness of selected input, processing, and output controls for SUNTAX.
- Evaluated the effectiveness of selected controls for promoting accuracy and proper application of the employer's annual unemployment tax rate.

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 April 28, 2009, 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
Lisa Echeverri

Child Support Enforcement
Ann Coffin
Director

General Tax Administration
Jim Evers
Director

Property Tax Oversight
James McAdams
Director

Administrative Services
Nancy Kelley
Director

Information Services
Tony Powell
Director

April 28, 2009

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, and in response to your letter of March 30, 2009, enclosed is the Department's response to the preliminary and tentative findings and recommendations of your Information Technology Audit of the Department of Revenue, SUNTAX and IMS Systems.

We appreciate the professionalism displayed by your audit staff. If further information is needed, please contact Bob Bliss, Director of Auditing, at 487-0701.

Sincerely,

Lisa Echeverri

LE/RB/bso

Enclosure

cc: Sharon Doredant
Bob Bliss

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

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Revenue
System for Unified Taxation (SUNTAX)
and
Imaging Management Systems (IMS)
Information Technology Operational Audit
Response to Preliminary and Tentative Audit Findings

Finding No. 1: Contrary to section 119.071(5)(a)2.a., Florida Statutes, the Department used employee social security numbers (SSNs) without specific authorization in law or without having established the imperative need to use the SSN for the performance of its duties and responsibilities as prescribed by law.

Recommendation: The Department should comply with State law by clearly establishing why the use of employee SSNs is imperative for the Department to perform its duties and responsibilities or alternatively establish another number to be used rather than the SSN for these purposes. Additionally, the Department should review its practice of placing the SSN on various documents and reports and discontinue the practice whenever practicable to minimize the risk of exposing the SSN to employees or others who have no business need to view the number.

Response: Finding No. 1 states Revenue's use of the SSN is contrary to State law and increases the risk of improper disclosure of SSNs. Furthermore, the finding details Revenue's use of SSNs in three areas: (1) in our Learning Management System (LMS); (2) in establishing network and application accounts; and (3) when e-mailing the Selection Approval E-mail Notification Form to Revenue employees who may or may not be authorized to have such information. Revenue agrees with the findings and has put together a SSN Elimination Team to address these findings. This team has developed a plan to eliminate the unnecessary use of SSNs throughout Revenue. Currently, the SSN Elimination Team is implementing the removal of SSNs from LMS, network and application accounts, and in the Selection Approval E-mail Notification Form.

Learning Management System

Revenue has begun implementing its plan to remove SSNs as the unique identifier in LMS. Revenue has created a unique identifier to be used in lieu of the SSN thus eliminating the need to use the SSN in LMS. The unique identifier has already been integrated into LMS. Next, the SSN will be removed from the LMS programming code.

Network Accounts

Upon removal of the SSN in LMS, Revenue will remove the SSN from network and application accounts.

Selection Approval E-mail Notification Form

Revenue has already identified both authorized and non-authorized persons who receive the e-mail form. Non-authorized persons will be removed from the e-mail group that receives the form, and any other access and rights shall be revoked. Encrypted e-mail will continue to be the means by which authorized persons shall receive the Selection Approval E-mail Notification Form.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

In conclusion we take our responsibility to maintain the confidentiality of personal information very seriously and do everything we can to ensure that we protect social security numbers and other confidential information.

Finding No. 2: As similarly noted in our report No. 2008-097, former employee and contractor access privileges in SUNTAX and the network had not been removed in a timely manner.

Recommendation: The Department should ensure that SUNTAX and network access privileges of former employees and contractors are removed in a timely manner and that access control records are retained as provided in the General Records Schedule.

Response: We concur. A new process has been implemented to help ensure supervisors of terminating employees notify Security Administrators in a timely fashion. A new process was implemented on April 10, 2009, for supervisors and contract managers to initiate the employee and contractor separation process through the DOR phone book on the DORweb.

This process automatically inactivates the LDAP account on the effective date of the employee's termination and notifies the appropriate security groups and helps ensure that security access is removed in a timely manner for employees leaving the agency. We have also updated the required forms and created a comprehensive separation process checklist.

Terminating employees have their network account disabled on their termination date. This date is captured in the Novell account record as well in hard copy form. Electronic and hard copy records are retained for at least one year in accordance with the General Records Schedule for State and Local Government Agencies.

Instructions on this new process were distributed to all supervisors on 4/10/2009 and the comprehensive web page outlining the steps in the process is available at all times to supervisors. Additional information regarding the process for contract managers for the management of contract resources will be developed and included in the Purchasing and Contract Management Manual by June 30, 2009. This update to the Purchasing and Contract Management Manual will include instructions to contract managers on how to request the removal of systems access for terminating contracted employees. A bulletin to all contract managers will also be issued by June 30, 2009, notifying contract managers of the manual update. This bulletin will outline the contract manager's responsibility when contracted employees leave the agency.

The Information Services Program and the Administrative Services Program will continue to work together to improve and simplify this process.

Finding No. 3: We noted an instance where a user had inappropriate access privileges to SUNTAX. In addition, as similarly noted in our report No. 2008-097, controls related to the authorization of IMS user access needed improvement.

Recommendation: The Department should implement appropriate controls to ensure that access privileges granted correspond to the access privileges requested by the employees'

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

supervisors. The Department should also perform periodic reviews of access privileges to ensure that access privileges are appropriate and commensurate with the users' job functions.

Response for SUNTAX: We concur. The Department is looking at some of the SUNTAX security roles and considering splitting them into multiple roles with fewer capabilities.

Reports of the Department's employee personnel actions are sent monthly to the agency's security administrators. SUNTAX security administrators review the monthly reports. Employees who are assigned to a new position are reviewed and access is changed or removed if no longer needed. SUNTAX security administrators plan to start an annual review of SUNTAX user access to managers to confirm that their employees have the appropriate access.

A report of users and their roles will be generated for each central office or service center. The employee's manager or equivalent will verify each employee's security role. This will be implemented by the end of the first quarter of FY 2009/10.

The Department has established an inactivity threshold for the SUNTAX application at 181 days. If no activity occurs on an account within SUNTAX, the account will be inactivated by locking the account.

Response for IMS: We concur. In reference to IMS user access controls, Returns and Revenue Processing (RRP) has revised procedures to require an annual review and reauthorization of access privileges. The Standard Operating Procedure (SOP) has been updated to reflect this requirement. In addition, the request form has been revised and contains greater detail to help ensure the authorization requested is consistent with the position's responsibilities. RRP will work closely with ISP to ensure that user administration for IMS is consistent on an enterprise basis.

With regard to the second part of this IMS finding, the positions cited as having authorization exceeding the requirements of their job functions have been relocated to ISP and no longer have operational access to IMS.

Finding No. 4: Certain user identifications (IDs) and passwords were being shared by department employees.

Recommendation: The Department should cease the practice of allowing users to share user IDs and passwords. Each system user should be assigned a unique user ID with a corresponding password.

Response: We concur. Department policy states that users should not share user IDs and passwords. System delivered user IDs for access to the operating system (e.g., SysAcct) are not established by BASIS but come with the Oracle system. Only one password can be assigned to this ID and it is necessary that more than one BASIS employee be aware of and use this ID/password when required to log into the operating system. We will evaluate the possibility of logging in with individual unique ID/passwords and then SU (Switch User) to the system account to log into the operating system thereby establishing an audit trail of access.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 5: In addition to the matters discussed in Finding Nos. 1 through 4 and 10, certain department security controls were deficient. Some of the issues were also included in our report No. 2008-097.

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

Response: The Department will address additional confidentiality, integrity, availability and security control issues on the SUNTAX and IMS servers/applications/use language based on what is addressed in the confidential findings.

Finding No. 6: As similarly noted in our report No. 2008-097, 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 authorized, designed, tested, and implemented.

Response: Information Services will work with the operating programs, General Tax specifically, on the Release Management and Change Management processes for the SUNTAX and Image Management Systems. The SUNTAX system currently has the release process in place and we will review the policies for any compliance issues. Work on this issue is planned to resume after the end of the 2008/09 fiscal year.

Finding No. 7: The Department lacked effective procedures for addressing data errors generated during the load process of data into SUNTAX.

Recommendation: The Department should implement controls to ensure that all failed files are timely reviewed, corrected, and reloaded into SUNTAX. Additionally, the Department should maintain a history log of failed file exceptions to provide increased assurance that failed files are being corrected and reloaded into SUNTAX in a timely manner.

Response: We concur. While we do maintain control logs monitoring the transmission and successful load of files, the notification process is e-mail based and subject to the Department's e-mail archiving rules (30 days). As such, notification of failed files must be reviewed in that thirty (30) day time frame or risk the move to archive. As a resolution, we will be adding a standardized address to the broadcast list for the failed file notification. This address will further have rules set to roll all notifications to an accessible archive file before the (30) days.

In addition, RRP will be completing a procedure document outlining proper steps, time frames and responsibilities for the review and correction of failed files.

Finding No. 8: A programming error existed within the approval process for compromise waivers.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation: The Department should review the appropriateness of compromise waiver approvals that occurred in excess of approval authority set forth in department rule.

Response: We concur. Upon notification by the Auditor General staff, a review of a SUNTAX database table found an error where the cells for penalty and interest compromise thresholds were reversed. This allowed some users to approve the compromise of interest at the penalty threshold amounts. Once discovered, a correction was made to the production system that same evening. The error has been resolved.

As a precautionary measure, SUNTAX has begun analysis for generation of a periodic (period to be determined) report that will compare all compromises against their respective thresholds. This report will be performed in the Business Intelligence environment and list any user exceeding allowable thresholds. The report will be forwarded to the Process Owner for Receivables Management.

Finding No. 9: Off-site backup procedures needed improvement.

Recommendation: The Department should review the frequency with which it cycles backups of SUNTAX files to the off-site location and consider a more frequent off-site rotation to further minimize the impact of a system loss.

Response: The current backup process will be improved by June 30, 2009. We will develop written procedures to support the new process by September 30, 2009.

This improvement will replicate the production and development data between the hosting two data centers (SSRC and NWRDC), reduce the dependency on tapes, and have a Recovery Point Objective (RPO) of two hours for both the CAMS and SUNTAX SAP instances.

Finding No. 10: The Department's written IT procedures needed improvement.

Recommendation: The Department should establish written procedures for the backup of SUNTAX data and programs and security administrator monitoring activities.

Response: The following procedures have been developed:

1. SUNTAX Backup Policy
2. SUNTAX Backup & Recovery Procedures

Security administrator monitoring procedures will be developed by the end of first quarter of FY 2009/10.