FLORIDA
DEPARTMENT OF REVENUE
Executive Director
Lisa Echeverri

October 30, 2009

Ms. Kathy DuBose, Staff Director
Joint Legislative Auditing Committee
404 South Monroe Street
876 Pepper Building
Tallahassee, Florida 32399-1100

Dear Ms. DuBose:

In accordance with section 20.055(5)(g), Florida Statutes, the Department of Revenue is submitting a written explanation of the status of the recommendations in Auditor General Report No. 2009-199, dated May 1, 2009.

The Department is in the process of reviewing and/or implementing the auditor's recommendations. If further information is needed, please contact me at 488-4328.

Sincerely,

Sharon Doredant
Inspector General

SD/dm

Attachment

CORRECTIVE ACTION PLAN

Rev. 11/04

Status Date	Report No.	Report Title	
October 2009	AG2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person	Program/Process		Phone No.
Brunetta Pfaender	ISP/Information Security		921-4271

Activity	Accountability		Schedule	
	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
n/a	n/a	n/a	no	varied (see below)

Finding No.	1
Date	4/28/09

Finding

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 SSN's 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.

Original Response

Finding No. 1 states Revenue's use of the SSN is contrary to State law and increases the risk of improper disclosure of SSN's. Furthermore, the finding details Revenue's use of SSN's 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 SSN's throughout Revenue. Currently, the SSN Elimination Team is implementing the removal of SSN's 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 SSN's 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.

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.

Program's Status

10/02/2009
1) We are in the process of eliminating the use of SSN's as a unique identifier in LMS.
a.) We have removed the SSN field from LMS and no longer use it as a unique identifier for active and future employees of the Department.
b.) We will hold a meeting on 10/16 to remove SSN's in LMS that are used for a small group of PTO External users. This removal will be completed by 10/21/09.
c.) We will meet on 10/5 to identify a unique identifier to use in place of the SSN's for former employees. This removal will also be completed by 10/21/09.

2) The Novell Directory contains SSN's because HR and IT applications use it as a unique identifier, and authenticate to it. If SSN's are removed from the Novell Directory then these other HR and IT systems

	will not cease to function ceasing payroll and other vital agency functions. As a result, the HR and IT applications will need to use a different unique identifier before SSN's can be removed from the Network Directory. We are meeting on 10/5 to determine any HR and IT applications that can use a unique identifier other than the SSN. 3) Information Security staff will need to restrict the distribution of the Selection Approval E-mail Notification Form to only those Revenue employees who have a need to know. This may be more involved than simply not sending the form to certain persons.
Status per OIG ☒ **Open** ☐ **Management assumes risk** ☐ **Partially complete** ☐ **Complete**	We reviewed the above statements provided by the ISP Information Security Manager's office and have determined that the corrective action is open.

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title
October 2009	AG2009-199	DOR and IMS Information Technology Operational Audit

Contact Person	Program/Process	Phone No.
Traci Jones Brunetta Pfaender	EXEC/Workforce Management ISP/Information Security	922-4131 921-4271

Activity	Accountability		Schedule	
	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
n/a	n/a	n/a	no	n/a

Finding	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.
No. 2	
Date 4/28/2009	
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.
Original 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.
Program's Status	10/19/09 Employee Separation policy as implemented effective May 12, 2009 and can be found at: http://dorweb01/library/ASP/Payroll/EmplyeSprtn.pdf Security staff procedures for removing terminated employees from the network are as follows: (J:ISP Procedures\Removal of System Users.doc)
Status per OIG ☐ Open ☐ Management assumes risk ☒ Partially complete ☐ Complete	We reviewed the Employee Separation Policy and the security staff procedures as stated above. We also observed the change to the DOR phone book on the DORweb that initiates the employee and contractor separation process. However, we were unable to receive sufficient information to confirm that SUNTAX accounts of all former employees were removed. Therefore, the finding is noted as partially complete.

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title	
October 2009	AG2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person	**Program/Process**		**Phone No.**
Brunetta Pfaender/ISP Donna Kornatowski/GTA	ISP/Security Administration & GTA/Returns and Reconciliation		921-4271 488-5545

Activity	Accountability		Schedule	
	Responsible Unit	**Coordinating Unit**	**Repeat Finding**	**Anticipated Completion Date**
n/a	n/a	n/a	no	n/a

Finding No. 3 **Date** 4/28/2009	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' 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.
Original Response	**(ISP) 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. **(GTA) 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.
Program's Status	10/19/09 **(ISP) Response for SUNTAX** Service Center Managers, Regional Managers and other senior GTA executives have access to SUNTAX transaction ZSEC01. This transactions reports each SUNTAX users Role and last login date for the employees under their responsibility. This transaction may be used by managers to verify their direct report's security role. 10/19/09 **(GTA) Response for IMS** (1) The IMS Standard Operating Procedure (SOP) has been updated to reflect revised procedures requiring an annual review and reauthorization of IMS access privileges. (2) 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.
Status per OIG ☐Open ☐Management assumes risk ☒Partially complete ☐Complete	We verified the above assertions from GTA by reviewing documentation provided by the Program. This included the IMS Standard Operating Procedure (SOP) and screenshots showing the removal of the positions. The information submitted by GTA is sufficient to consider their part of the corrective action plan complete. However, the information provided by ISP is insufficient to consider the corrective action plan complete; therefore, the finding is noted as partially complete.

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title	
October 2009	AG2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person	**Program/Process**		**Phone No.**
Paul Forrester	**ISP/BASIS System Support**		**414-8407**

Activity	Accountability		Schedule	
	Responsible Unit	**Coordinating Unit**	**Repeat Finding**	**Anticipated Completion Date**
n/a	n/a	n/a	no	n/a

Finding No. 4 / **Date** 4/28/2009	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.
Original 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.
Program's Status	10/19/09 The SUNTAX Oracle system was replaced by SQL Server 2008 in July 2009. BASIS users now have the ability to login in individually, and no longer have a need to share passwords.
Status per OIG ☐ Open ☐ Management assumes risk ☐ Partially complete ☒ Complete	We verified the above statement through information provided by the BASIS administrator. The corrective action plan is complete.

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title	
October 2009	AG2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person	**Program/Process**		**Phone No.**
Brunetta Pfaender	**ISP/Information Security**		921-4271

Activity	Accountability		Schedule	
	Responsible Unit	**Coordinating Unit**	**Repeat Finding**	**Anticipated Completion Date**
n/a	n/a	n/a	no	TBD

Finding No.	5
Date	4/28/2009
Finding	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.
Original 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.
Program's Status	The Department continues its plans to address the noted confidentiality, integrity, availability and security issues.
Status per OIG ☒ **Open** ☐ **Management assumes risk** ☐ **Partially complete** ☐ **Complete**	Specific details related to corrective actions are confidential

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title	
October 2009	AG2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person	**Program/Process**		**Phone No.**
Chris Ajhar	ISP/Application Management		922-4243

Activity	Accountability		Schedule	
	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
n/a	n/a	n/a	yes	June 2010 and TBD

Finding No. 6, Date 4/28/2009	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.
Original 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.
Program's Status	10/14/2009 We will have a release process in place by June 30, 2010. The Change process is partly in place for application development.
Status per OIG ☐ Open ☐ Management assumes risk ☒ Partially complete ☐ Complete	The Office of the Inspector General is currently reviewing the Change Management process and has verified the assertions made by the program. The corrective action plan is partially complete.

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title	
October 2009	AG2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person	**Program/Process**		**Phone No.**
Donna Kornatowski	**General Tax Administration**		**850-488-5545**

Activity	Accountability		Schedule	
	Responsible Unit	**Coordinating Unit**	**Repeat Finding**	**Anticipated Completion Date**
n/a	Jim Cook	n/a	no	n/a

Finding No. 7 **Date** 4/28/2009	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.
Original 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.
Program's Status	10/19/09 1) We have created written procedures documenting the process of failed file error notification via email. 2) We have created written procedures documenting the process to correct the failed file error upon receipt of the email. 3) Old failed file directories have been reconfigured, creating "an archive of everything that has ever failed, through the 5/31/08 validations, since SAP was brought up." 4) A procedure document has been developed, outlining proper steps, time frames and responsibilities for the review and correction of failed files.
Status per OIG ☐ **Open** ☐ **Management assumes risk** ☐ **Partially complete** ☒ **Complete**	We have reviewed the documentation provided by GTA verifying each of the four assertions. The information provided to the OIG is sufficient to consider the corrective action plan complete.

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title	
October 2009	2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person	**Program/Process**		**Phone No.**
James Evers	General Tax Administration/Program Directors Office		(850) 488-5163
Activity	**Accountability**		**Schedule**
n/a	**Responsible Unit**	**Coordinating Unit**	**Repeat Finding** / **Anticipated Completion Date**
	n/a	n/a	no / n/a

Finding No. 8 / **Date** 4/28/2009	A programming error existed within the approval process for compromise waivers.
Recommendation	The Department should review the appropriateness of compromise waiver approvals that occurred in excess of approval authority set forth in department rule.
Original 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.
Program's Status	The issue in Finding 8 has been resolved.
Status per OIG ☒ **Open** ☐ **Management assumes risk** ☐ **Partially complete** ☐ **Complete**	Although GTA management has asserted the necessary correction was made to resolve the error, as of this date we have not received sufficient evidence to independently conclude that the deficiency was corrected. Thus, we will consider this CAP open until sufficient evidence of the corrective action is provided by the Program.

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title	
October 2009	AG2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person:	Program/Process		Phone No.
Mark Montenieri	ISP/Storage Manager		921-0764

Activity	Accountability		Schedule	
	Responsible Unit	Coordinating Unit	Repeat Finding	Anticipated Completion Date
n/a	Mark Montenieri	n/a	no	Early 2010

Finding No.	9
Finding Date	4/28/2009
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.
Original 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 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.
Program's Status	10/19/2009 As of June 2009, our backups use a data domain storage unit (disk, instead of tape), located in each data center. The data then replicates itself to another data domain unit, which will be located in Atlanta later this year, but currently resides in Tallahassee. A full backup policy document, step-by-step recovery guide, and continuity plan will be available early next year.
Status per OIG ☐ Open ☐ Management assumes risk ☒ Partially complete ☐ Complete	There has been limited activity directed to implement the recommendation. The corrective action is partially complete.

CORRECTIVE ACTION PLAN

Status Date	Report No.	Report Title	
October 209	2009-199	DOR and IMS Information Technology Operational Audit	
Contact Person	**Program/Process**		**Phone No.**
Mark Monteneri	**ISP/Storage Manager**		**921-0764**

Activity	Accountability		Schedule	
	Responsible Unit	**Coordinating Unit**	**Repeat Finding**	**Anticipated Completion Date**
n/a	n/a	n/a	no	Early 2010

Finding	
No. 10	The Department's written IT procedures needed improvement.
Date 4/28/2009	
Recommendation	The Department should establish written procedures for the backup of SUNTAX data and programs and security administrator monitoring activities.
Original 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.
Program's Status	The documents reference above are located at http://sdrmosd1/sa/SA Library/Forms/AllItems.aspx which is a secure network directory. We are currently working towards creating a disaster recovery site in Atlanta near the first of the year 2010, and the procedures will be modified accordingly.
Status per OIG ☐ **Open** ☐ **Management assumes risk** ☒ **Partially complete** ☐ **Complete**	We verified that the SUNTAX Backup Policy and SUNTAX Backup & Recovery Procedures have been developed. We could not confirm the existence of security administrator monitoring procedures. Therefore, the corrective action plan as partially complete.