October 3, 2011

The Honorable Jeff Atwater  
Chief Financial Officer  
The Capitol, PL-11  
Tallahassee, Florida 32399-0301

Dear Mr. Atwater:

As required by Section 20.055, Florida Statutes, I have enclosed the Department’s six-month status updates regarding corrective actions taken in response to Auditor General Report Number 2011-173, Selected Division of Treasury Applications Information Technology Operational Audit.

If you have any questions, please do not hesitate to contact me.

Sincerely,

Ned Luczynski

cc: Robert Kneip, Chief of Staff  
Paul Whitfield, Deputy Chief Financial Officer  
Kathy DuBose, Coordinator, Joint Legislative Auditing Committee
Department of Financial Services  
Office of Inspector General  

SIX-MONTH FOLLOW-UP REPORT  
STATUS OF CORRECTIVE ACTION

<table>
<thead>
<tr>
<th>Reviewing Entity</th>
<th>Report No.</th>
<th>Report Title</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor General</td>
<td>AG 2011-173</td>
<td>Selected Division of Treasury Applications Information Technology Operational Audit</td>
<td>April 6, 2011</td>
</tr>
</tbody>
</table>

**Finding No. 1**  
Some password controls surrounding the Treasury applications needed improvement. One issue relating to password expiration intervals was also disclosed in our report No. 2009-004.

**Recommendation**  
The Department should ensure that adequate password controls are maintained in accordance with established policy to reduce the risk of compromise to passwords and unauthorized disclosure, modification, or destruction of data and IT resources.

**Original Response**  
The Department concurs. In response to the audit inquiry related to the override of two user profiles, Department staff disabled the user profiles and adjusted the expiration interval on the identified user profiles so that the passwords would expire in accordance with Department policy.

In response to the audit inquiry related to password length parameters, DIS will remove Treasury's ability for that control to be changed to less than the Department standard.

In response to the audit inquiry related to the "change password screen," all applications will be reviewed and modified to ensure that closing the Change Password screen will quit the application if a user tries to circumvent the requirement to change their password.

---

**Six-month Follow-up: October 6, 2011**

**Responsible Division(s)**  
Division of Information Systems  
Division of Treasury

**Reported Status**  
The Compliance Officer reviewed password change intervals for all profiles (users and services) as of September 7, 2011. No user profiles had been set to override the system parameters.

The selected Treasury applications now use Active Directory for authentication. As a result, network password controls cannot be circumvented by application users. This modification was moved into production on 5/27/2011.

**OIG Assessment**  
CLOSED. It appears that management has taken appropriate corrective action.
Department of Financial Services  
Office of Inspector General  

SIX-MONTH FOLLOW-UP REPORT  
STATUS OF CORRECTIVE ACTION

<table>
<thead>
<tr>
<th>Reviewing Entity</th>
<th>Report No.</th>
<th>Report Title</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor General</td>
<td>AG 2011-173</td>
<td>Selected Division of Treasury Applications Information Technology Operational Audit</td>
<td>April 6, 2011</td>
</tr>
</tbody>
</table>

Finding No. 2  
The access privileges of some Department staff with regard to production programs and data were not appropriate for their job duties. Similar issues were disclosed in our report No. 2009-004.

Recommendation  
The Department should ensure that update access permissions continue to remain commensurate with assigned job duties.

Original Response  
The Department concurs. In response to the audit inquiry, Department staff removed the test profile from the two server groups on November 5, 2010. The Department will ensure that access permissions are commensurate with assigned job duties. The Department will explore refining the Personnel Action Request (PAR) process to include the Information Technology Application Access and Resource Request Form (Form 1820).

Six-month Follow-up: October 6, 2011  
Responsible Division(s)  
Division of Information Systems  
Division of Treasury

Reported Status  
The Department has taken steps to ensure that update access permissions remain commensurate with assigned job duties. As of September 7, 2011, the Compliance Officer reviewed server group memberships to ensure that access permissions remained commensurate with assigned job duties.

OIG Assessment  
Management has taken appropriate action to ensure that update access permissions are commensurate with assigned job duties. However, we will continue to monitor this recommendation until such time as management establishes and implements policies and procedures to provide for such review and assurance on an on-going basis.
## SIX-MONTH FOLLOW-UP REPORT
### STATUS OF CORRECTIVE ACTION

<table>
<thead>
<tr>
<th>Reviewing Entity</th>
<th>Report No.</th>
<th>Report Title</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor General</td>
<td>AG 2011-173</td>
<td>Selected Division of Treasury Applications Information Technology Operational Audit</td>
<td>April 6, 2011</td>
</tr>
</tbody>
</table>

**Finding No. 3**
Program change controls needed improvement in the areas of monitoring program changes in the production environment and the movement of source programs into the production environment. One issue relating to monitoring program changes in the production environment was also disclosed in our report No. 2009-004.

**Recommendation**
The Department should provide for an automatic system-generated log of changes to production Treasury application programs. Until a logging mechanism can be acquired, the Department should implement alternative monitoring and review processes over program changes in the Treasury production environment to ensure that unauthorized or erroneous modifications, should they occur, are timely detected. In addition, the Department should implement procedures to ensure the integrity of the Treasury source programs by having an independent group or person move the source programs to a separately controlled production library.

**Original Response**
The Department concurs. In the absence of an automated monitoring tool, procedures will be developed to have an independent party move source programs to a controlled production library. Comparisons will be made between production libraries and the controlled production source code libraries to ensure that erroneous production changes will be detected in a timely manner.

---

**Six-month Follow-up: October 6, 2011**

**Responsible Division(s)**
Division of Information Systems  
Division of Treasury

**Reported Status**
An independent party now moves source programs to a separately controlled production library; programmers are precluded from update capability to this library. In addition, an extensive development project for the selected Treasury applications is in process. New system capabilities will address an appropriate separation of duties and adequate logging.

**OIG Assessment**
It appears that management has taken appropriate corrective action concerning movement of source programs. However, we will continue to monitor the finding until such time as system capabilities regarding separation of duties and adequate logging are implemented.
Department of Financial Services  
Office of Inspector General  

SIX-MONTH FOLLOW-UP REPORT  
STATUS OF CORRECTIVE ACTION

<table>
<thead>
<tr>
<th>Reviewing Entity</th>
<th>Report No.</th>
<th>Report Title</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor General</td>
<td>AG 2011-173</td>
<td>Selected Division of Treasury Applications Information Technology Operational Audit</td>
<td>April 6, 2011</td>
</tr>
</tbody>
</table>

**Finding No. 4**  
The Department did not have written procedures for some Treasury application security administration functions.

**Recommendation**  
The Department should enhance its procedures to provide written guidance on all security administration functions of the Authorized System.

**Original Response**  
The Department concurs. Written procedures will be developed to address all security administration functions of the Authorization System.

**Six-month Follow-up: October 6, 2011**

**Responsible Division(s)**  
Division of Information Systems  
Division of Treasury

**Reported Status**  
The Department implemented a Single Sign-On system effective May 27, 2011. Treasury has developed written procedures to address the security administration functions of the Single Sign-On system.

**OIG Assessment**  
CLOSED. It appears that management has taken appropriate corrective action.
<table>
<thead>
<tr>
<th>Reviewing Entity</th>
<th>Report No.</th>
<th>Report Title</th>
<th>Date Published</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditor General</td>
<td>AG 2011-173</td>
<td>Selected Division of Treasury Applications Information Technology Operational Audit</td>
<td>April 6, 2011</td>
</tr>
</tbody>
</table>

**Finding No. 5**
Some Department security controls in the areas of user authentication and system logging needed improvement. Similar issues regarding system logging were also disclosed in our report No. 2009-004.

**Recommendation**
The Department should improve security controls related to user authentication and system logging to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.

**Original Response**
The Department concurs with the recommendation and will pursue security control remediation.

**Six-month Follow-up: October 6, 2011**

<table>
<thead>
<tr>
<th>Responsible Division(s)</th>
<th>Reported Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Division of Information Systems Division of Treasury</td>
<td>The Department has corrected security controls related to user authentication and continues to address security controls related to system logging to ensure the continued confidentiality, integrity, and availability of Department data and IT resources.</td>
</tr>
</tbody>
</table>

**OIG Assessment**
Management has taken corrective action in some areas; however, we will continue to monitor management’s efforts to improve security controls.