June 13, 2018

Erin Rock, Secretary
Florida Department of Management Services
4050 Esplanade Way, Suite 285B
Tallahassee, FL 32399

Dear Secretary Rock:


If further information is needed concerning management’s response, please do not hesitate to contact Yolanda Lockett, Auditor Director, at 487-9476 or me at 413-8740.

Sincerely,

[Signature]

Dawn E. Case
Inspector General

DC/yvl

Enclosure

cc: Joint Legislative Auditing Committee
Sherrill F. Norman, Auditor General
Eric Miller, Chief Inspector General
David Zeckman, Chief of Staff
Heather Best, Senior Director of Executive Operations
Elizabeth Stevens, Director of Division of Retirement
Shirley Beauford, Assistant Director of Division of Retirement
Yolanda Lockett, Audit Director
### Audit Findings Status Update Form

<table>
<thead>
<tr>
<th>Status Date</th>
<th>Report/Agency #</th>
<th>Report Title/Agency Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/13/18</td>
<td>2018-077</td>
<td>2017 IT Operational Audit of IRIS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Contact Person</th>
<th>Title</th>
<th>Phone No.</th>
<th>Email Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elizabeth Stevens</td>
<td>Division Director</td>
<td>(850) 778-4400</td>
<td><a href="mailto:Elizabeth.Stevens@dms.myflorida.com">Elizabeth.Stevens@dms.myflorida.com</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activity</th>
<th>Accountability</th>
<th>Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appropriateness of Access Privileges</td>
<td>Responsible Area</td>
<td>Repeat Finding</td>
</tr>
<tr>
<td>Division of Retirement</td>
<td>Yes</td>
<td>4/30/18</td>
</tr>
</tbody>
</table>

#### Finding

<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>12/21/17</td>
</tr>
</tbody>
</table>

**Finding Category**

The access privileges for some IRIS users did not promote an appropriate separation of duties and did not restrict users to only those functions necessary for their assigned job duties.

**Finding**

We recommend that Department management limit user access privileges to IRIS data and IT resources to promote an appropriate separation of duties and restrict users to only those functions necessary for their assigned job duties.

**Recommendation**

The Department concurs with the finding and recommendation. The Department will develop a plan of action to further limit user access privileges where possible. If separation of duties is not feasible, efforts will be made to enhance our compensating controls. The plan will include: (1) assessing job duties assigned to IT staff that have application deployment responsibilities, (2) evaluating the use of log reviews to mitigate any remaining separation of duties issues, or (3) the implementation of other compensating controls should separation of duties not be fully achieved. The Department expects to have the plan finalized by Feb. 28th and will begin implementation afterward.

#### Status Update-6 months

- Open
- Management/Agency Assumes Risk
- Partially Complete
- Complete Pending Verification by AG
- Closed

#### Status Update-12 months

- Open
- Management/Agency Assumes Risk
- Partially Complete
- Complete Pending Verification by AG
- Closed

#### Status Update-18 months

- Open
- Management/Agency Assumes Risk
- Partially Complete
- Complete Pending Verification by AG
- Closed

The division has developed and implemented procedures to restrict the following access:

- Restrict production deployments to system administrators only
- Restrict production deployments to two resources; one primary, one backup
- Restrict production data updates to DBAs only
- Remove developer function from DBAs
- Restrict DBAs to two resources; one primary, one backup
- Enable logging for all production DBA activity
- Remove production deployment function from application security administrators