FLORIDA DEPARTMENT of management SERVICES
We serve those who serve Florida

4050 Esplanade Way
Tallahassee, Florida 32399-0950
Tel: 850.488.2786 | Fax: 850. 922.6149

Rick Scott, Governor

Craig J. Nichols, Agency Secretary

MEMORANDUM

DATE: November 21, 2013

TO: Curtis Unruh, Executive Director

FROM: Walter Sachs, Inspector General

SUBJECT: **Six-Month Follow-up to Auditor General Report No. 2013-182**

In accordance with Chapter 20.055, Florida Statutes, the following is our explanation of the six-month status of findings and recommendations included in the AG published Report No. 2013-182, ***Information Technology Operational Audit of the Northwood Shared Resource Center***. Our response addresses the findings and recommendations in the same order as they appear in the report.

Six-Month Status Report

NSRC Information Technology Operational Audit

General IT Controls

Finding No. 1: Midrange Systems Inventory

NSRC did not have system management software installed on some of the midrange systems that it managed for customer entities. As a result, NSRC was not able to maintain a complete inventory of logical midrange systems managed by the data center.

Recommendation:

NSRC should, in coordination with its customer entities, ensure that appropriate system management software is installed on all midrange systems and establish a complete and accurate inventory of the systems.

Response:

The NSRC concurs with the recommendation. Prior to the audit, the NSRC had acquired and began the process of installing the system management software; which includes inventory functionality. The NSRC anticipates this deployment to be fully implemented by June 1, 2013; however, this date is contingent on the four remaining customer agencies.

Current Status of Recommendation

Of the eleven (11) NSRC customers involved in the deployment of Tivoli End Point Manager, only four have not completed the process: DBPR, DEP, DJJ, and DOH. As of October 2013, new customer FWC joined the deployment process and has brought the number up from four to five agencies who have not yet signed off on deployment.

While progress has been made with each of the original four customers in the deployment of this system management agent, formal sign-off that the deployment captures the universe of all servers under management is outstanding. The issue is being escalated through the regularly scheduled Customer Relationship Management (CRM) meetings.

Office of Inspector General Position:
We recommend the finding remains open. We have reviewed the status of the Tivoli End Point rollout and will continue to follow up on the results of the CRM meetings and the deployment until the remaining five customers is complete.

Finding No. 2: Backup Controls

NSRC did not back up the data on some midrange systems it managed. Additionally, the off-site backup tape storage facility used by NSRC was too close in proximity to the data center.

Recommendation:

NSRC should ensure that midrange system backups are performed in a timely manner. NSRC should also utilize an off-site backup storage facility that is more geographically removed from the NSRC data center.

Response:

The NSRC concurs with recommendation number one. Prior to the audit, the NSRC had acquired funding and began the RFQ process for an enterprise backup solution. The NSRC anticipates this process being fully implemented by the end of the fiscal year 2013/2014.

The NSRC agrees in principle with respect to recommendation number two. The NSRC will investigate a more geographically removed storage facilities for off-site storage of backups. The findings and associated costs will be presented to the NSRC Finance Committee for their final decision.

Current Status of Recommendation

Approval of Phase 1 of the Enterprise Backup solution (a three phase project as currently planned) has been delayed, in part to allow the new NSRC Executive Director time to review the selection process and team's recommendation. Additional delay has been added at the request of the Board of Trustees, to allow for additional technical and cost review. In the meantime, a backup review of the NSRC's largest customer was initiated in October 2013 to ensure that all systems are appropriately protected. Similar system audit

reviews are inherently incorporated into the Enterprise Backup deployment plan and expected to be initiated once that project receives approval.

The NSRC has recently hired an FTE to handle NSRC COOP / Disaster Recovery related projects and issues. This FTE will be tasked to work with the Midrange Manager and the Mainframe Manager, coordinating research into alternatives to the current off-site storage location and delivering their findings to the Executive Director in a comprehensive written manner. Research will need to include distances the DMS OIG has identified as geographically desirable. While initial research can begin December 1, 2013, significant progress will be dependent on the successful launch of the Enterprise Backup Project.

Office of Inspector General Position:
We recommend the finding remains open. We have reviewed the documentation provided by management relative to their phased approach to improving their backup system. We will perform additional follow up at 12 months to determine progress after the launch of the Enterprise Backup project.

Finding No. 3: Continuity of Operations and Disaster Recovery Planning

The NSRC Continuity of Operations Plan Operational Procedures (COOP) and the Disaster Recovery Plan for NSRC lacked required statutory elements and contained incomplete and outdated information. Additionally, contrary to State law, the COOP had not been submitted to the Division of Emergency Management for approval. Also, NSRC staff had not received periodic training on implementing the plans.

Recommendation:

To comply with State law, NSRC should update and complete its COOP and Disaster Recovery Plan to accurately describe the current NSRC environment and submit the COOP to DEM for approval. NSRC should also schedule and provide its staff with periodic continuity of operations and disaster recovery training.

Response:

The NSRC concurs with recommendation number one. Prior to the audit, the NSRC began the process of creating a new COOP and will be submitting the documentation to DEM for approval during the 2013 calendar year. Additionally, the NSRC is in the process of updating the current Disaster Recovery Plan.

The NSRC concurs with recommendation number two. The NSRC will create periodic continuity of operations and disaster recovery training. The NSRC anticipates this process being fully implemented by the end of the fiscal year 2013-2014.

Current Status of Recommendation

The NSRC has recently hired an FTE to handle NSRC COOP / Disaster Recovery related projects and issues. This FTE has been tasked with updating and completing the NSRC's COOP and Disaster Recovery Plan to accurately describe the current NSRC environment and comply with State Law. Currently, the expectation is that the FTE will be able to

produce a 2014 draft that should demonstrate progress has been made within 6 months. The NSRC will also submit this new 2014 COOP / DR Plan to DEM for review and approval. The new FTE is already working to schedule and provide NSRC staff with periodic continuity of operations and disaster recovery training in 2014.

Office of Inspector General Position:
We recommend the finding remains open. We have discussed the plans with NSRC staff and will perform additional follow up procedures at 12 months to determine progress of the COOP and Disaster Recovery Plans.

Finding No. 4: Change Control

NSRC was unable to provide us with a system-generated log of systems software changes that had been applied to the midrange systems. In addition, NSRC did not have sufficient information to permit a comparison of the system-generated logs of mainframe changes to manually-prepared software change documentation.

Recommendation:

NSRC should implement system-generated logs to record, track, and report all system software changes that are made to midrange systems and include sufficient information in mainframe change documentation to provide for reconciliation to system-generated logs.

Response:

The NSRC concurs with the recommendation. Prior to the audit the NSRC requested funds for a log management toolset through the LBR process. The NSRC will procure the toolset in fiscal year 2013/2014 if the LBR funding is approved in the GAA.

Current Status of Recommendation

Mainframe Tech Support now includes a maintenance ID in each change control ticket to indicate what maintenance is being applied. The maintenance ID can be used to list the individual fixes that make up the maintenance. Samples of change control tickets that included maintenance IDs were provided as part of this audit.

The Mainframe Tech Support does not provide system generated logs to record, track, and report all system software changes made to the midrange systems.

Office of Inspector General Position:
We have verified the maintenance information in the change ticket. However, we recommend the finding remains open until additional follow up has been performed at 12 months to determine if NSRC was able to procure the log management toolset.

Finding No. 5: Other Security Controls

Certain NSRC security controls related to user authentication, software patch management, and physical access needed improvement. One of these issues was communicated to NSRC management in connection with our report No. 2011-082.

Recommendation:

NSRC should improve security controls related to user authentication, software patch management, and physical access to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

Response:

The NSRC concurs with the recommendation. Prior to the audit the NSRC procured a patch management toolset and is in the deployment process. Additionally, the NSRC will update its procedures for user authentication and physical access. The NSRC anticipates this process being fully implemented by the end of the fiscal year 2013-2014.

Current Status of Recommendation

The patch management toolset has been deployed to all but three agencies. Each of the three agencies has been approached in an attempt to resolve this issue and efforts to resolve deficits in progress. Anticipated completion date for deployment is June 2014. The NSRC has provided a copy of our Patch Management Overview documentation in relation to this finding.

User authentication and physical access processes are also actively in review and update.

Office of Inspector General Position:

We have reviewed the patch management overview. We recommend the finding remains open. Additional follow up will be performed at 12 months to verify the patch management deployment and the implementation of their updated authentication and physical access processes.

Finding No. 6: Performance Monitoring and Capacity Planning Procedures

As similarly noted in our report No. 2011-082, NSRC had not established written procedures for performance monitoring and capacity planning.

Recommendation:

NSRC should establish written procedures for performance monitoring and capacity planning for its midrange systems.

Response:

The NSRC concurs with this recommendation. The NSRC anticipates these procedures being fully implemented by the end of the fiscal year 2013/2014.

Current Status of Recommendation

New software toolsets have been acquired to monitor performance and are currently being implemented; the most recent Solarwinds Project Status. Written procedures for utilizing these tools are being developed as part of the implementation. Copies of these written procedures were requested and will be provided as part of this audit.

Capacity planning worksheets for bi-annual customer reporting have been revised and formal written process documentation for analyzing the data is in works under the direction of the NSRC Support Services Director. The capacity planning worksheets have been provided as documentation related to this audit.

The anticipated date as to when written procedures for performance monitoring and capacity planning for midrange systems will be completed is in February 2014. Billing model changes were approved by the NSRC Board of Trustees in October 2013, which will encourage customers to review server capacity needs and reduce costs, and could impact current NSRC capacity planning goals and timelines.

Office of Inspector General Position:
We have reviewed the Solarwinds Project status report and capacity planning worksheets. However, we recommend the finding remains open until additional follow up is performed at 12 months to determine if written procedures for performance monitoring and capacity planning for midrange systems have been completed.

Finding No. 7: Access Authorizations

NSRC did not maintain access authorization documentation for some employees and authorization documentation for other employees did not explicitly list the access privileges that had been authorized by management.

Recommendation:

NSRC should maintain documentation of management authorization for employee access privileges that explicitly identifies the access privileges that have been assigned to its employees.

Response:

The NSRC concurs with the recommendation. Prior to the audit the NSRC began modifying the existing procedures. The NSRC anticipates these updated procedures being fully implemented by the end of December 2013.

Current Status of Recommendation

The NSRC employee onboarding and separation process are actively in review, with a new Employee Action Form pending final approval after pilot testing. Final approval is

expected to take place in December 2013. Employee access documentation review has begun with the recent hire of the current NSRC ISM in September 2013.

Office of Inspector General Position:

We recommend the finding remains open until audit procedures can be performed to validate the effectiveness of management's updated procedures and processes.

Finding No. 8: Appropriateness of Access Privileges and Periodic Review of Physical Access

One user account with domain administrator access privileges remained active; however, the user account was no longer being used by the NSRC. Additionally, NSRC staff could not, upon audit request, provide documentation of periodic reviews of the appropriateness of physical access privileges to sensitive facilities.

Recommendation:

NSRC should enhance its review of domain administrator access privileges and deactivate any unnecessary or unused access detected. NSRC should also conduct and document the required periodic reviews of the appropriateness of physical access privileges to sensitive facilities.

Response:

The NSRC concurs with the recommendation number one. Prior to the audit the NSRC began modifying the existing procedures. The NSRC anticipates these updated procedures being fully implemented by the end of December 2013.

The NSRC concurs with the recommendation number two that the process of conducting reviews of physical access be documented. During the fiscal year of 2012/2013, the new NSRC Security Office Staff has been conducting reviews of physical access. The NSRC will document an official procedure for reviews of physical access and anticipates these new procedures being fully implemented by the end of December 2013.

Current Status of Recommendation

On February 18, 2013, the Administrator account for the NSRC's AD use (previously used for workstation deployment and Microsoft deployment tools) was disabled. This information was provided via email on that date to AG auditor Joseph West, along with a screenshot of the account's Administrator Properties post being disabled.

Several methods for periodic review of Domain Administrator accounts are being discussed and implementation is on target by the end of December 2013.

A recent audit by the AG requested current NSRC Photo ID Badge review records. These records are part of an internal review process established and carried out regularly under former NSRC ISM Christine Millett. When Millett retired, the process appears to have gone on hiatus under the subsequent NSRC ISM (2012-2013) but was reactivated when Curtis Unruh became the NSRC Executive Director in September 2013.

Office of Inspector General Position:
We recommend the finding remains open until audit procedures can be performed to validate the effectiveness of the updated procedures being finalized in December. We will test these procedures as a part of our 12 month follow up.

Finding No. 9: Service-Level Agreements

Three NSRC service-level agreements (SLAs) with customer entities lacked certain provisions required by State law.

Recommendation:

For all future SLAs, NSRC should ensure that all required provisions are included.
In addition, NSRC should modify the three SLAs described above to include all provisions required by State law.

Response:

The NSRC concurs with the recommendations. For future SLAs, the NSRC will ensure that the appropriate provisions are included.

Current Status of Recommendation

This has been completed. The SLAs for AHCA, DOH, and DHSMV have all been revised to include the identified provisions required by law.

Office of Inspector General Position:
We have obtained a copy of the revised SLA for the three customers and verified the changes made comply with statue. We recommend the finding be closed.

[1] The scope of this report does not include confidential findings.