DEPARTMENT OF MANAGEMENT
Services

Office of Inspector General
Department of Management Services
4040 Esplanade Way, Suite 135
Tallahassee, Florida 32399-0001
Tel: 850.488.5285
Fax: 850.921.3066
www.dms.MyFlorida.com

Governor Charlie Crist

Secretary Linda H. South

MEMORANDUM

DATE: September 24, 2010

TO: John Wade, Executive Director, SouthWood Shared Resource Center

FROM: Steve Rumph, Inspector General

SUBJECT: **Six-Month Follow-up to Auditor General Report No. 2010-173 SSRC - Data Center Operations**

Pursuant to Section 20.055(5)(g), Florida Statutes, the following is our explanation of the six-month status of findings and recommendations included in the Auditor General's Report No. 2010-173, ***Southwood Shared Resource Center – Data Center Operations.*** Our response addresses the findings and recommendations in the same order as they appear in the report.

Six-Month Status Report

Finding No. 1 - Service-Level Agreements

Contrary to State law, service-level agreements (SLAs) had not been established with some SSRC customer entities.

Recommendation:

The SSRC and customer entities should establish mutually agreed-upon service-level agreements as provided in State law. In connection with developing rules relating to the operation of the State data center system pursuant to Section 282.201(2), Florida Statutes, AEIT should consider establishing guidance to promote the timely execution of SLAs between primary data centers and customer entities.

Response:

The SSRC agrees with the recommendation, and supports the proposed proviso language mandating agencies to execute an SLA for services from the SSRC no later than September 1, 2010.

Current Status of Recommendation

The SSRC is working with all its Customers providing and negotiating Service Level Agreements (SLA) in order to help ensure all SLAs are established, reviewed, and signed by all parties in compliance with the FY 10-11 September 1, 2010, Legislative mandate. The SSRC has signed SLAs with 96% of their customers. However, three agency and two non-agency customers have not signed an SLA. It is anticipated that the three agency customers will sign an SLA by December 31, 2010. Discussions will continue to get the two non-agency customers to sign SLAs.

OIG Position

We agree with the actions taken by the SSRC; however, until all SLAs are signed with customers the finding will remain open.

Finding No. 2 – SLA Performance

In one instance noted, a service-level agreement performance level had not been met by the SSRC.

Recommendation:

The SSRC should continue to review controls to ensure that unplanned outages or major problems, should they occur, are timely detected and reported to applicable customers.

Response:

The SSRC agrees with this recommendation. On September 22, 2009, the SSRC corrected the problem by generating automated emails that alert the IBM technical support team to contact vendors regarding acquisition of new license keys prior to expiration of existing keys. This process is identified in a new operating procedure OP352 – Vendor Software License Key Renewal.

Current Status of Recommendation

On March 15, 2010 the SSRC implemented operating procedure OP352 – Vendor Software License Key Renewal and is utilizing the procedure to ensure license keys are reviewed and renewed prior to expiration.

OIG Position

We agree with the actions taken by the SSRC and recommend this finding be closed.

Finding No. 3 – Tape Management

A data backup tape was not properly accounted for in the SSRC tape management system and contained the commingled data of more than one customer entity, contrary to customer expectations.

Recommendation:

The SSRC should improve the accuracy of its tape management system and, where applicable, ensure that data on backup tapes is appropriately separated pursuant to customer entity expectations.

Response:

The SSRC agrees with this recommendation. On March 10, 2010, the SSRC added additional controls to its tape management system procedure OP906 – Iron Mountain Offsite Procedures. These controls include: acquiring a list of tapes monthly from the various library owners that vault at Iron Mountain to ensure proper location of tapes and automatic 7 day return of any tapes requested from offsite before their expiration date, unless library owners request in writing that tapes are not to be returned. In addition, the SSRC is in the process of establishing a procedure to review and assess stored data in accordance with customer expectations identified in SLA.

Current Status of Recommendation

On March 16, 2010 the SSRC Operations group implemented OP906 – Iron Mountain Offsite Procedures to ensure the proper location of system tapes. The SSRC Storage / Backup platform has instituted procedure STR104 on August 26, 2010 to review tapes randomly for co-mingled data and correct issue immediately.

OIG Position

We agree with the actions taken by the SSRC and recommend this finding be closed.

Finding No. 4 – Timely Removal of Reassigned Employee Access

The SSRC did not remove the access privileges of a reassigned employee in a timely manner.

Recommendation:

The SSRC should enhance its procedures to ensure that the access privileges of reassigned employees are removed in a timely manner.

Response:

The SSRC agrees with this recommendation. The SSRC is currently in the process of establishing an employee transfer process similar to our employee termination process that will allow the manager to review access security privileges for new duties and responsibilities. The anticipated completion date is April 16, 2010.

Current Status of Recommendation

On April 15, 2010 the SSRC implemented procedure IS113 – SSRC Employee Reassignment Security Review to address the issue of reassigned employees within the SSRC.

OIG Position

We agree with the actions taken by the SSRC and recommend this finding be closed.

Finding No. 5 – IT Procedures

The SSRC lacked comprehensive procedures for periodic reviews of access privileges and standardized change control testing.

Recommendation:

The SSRC should establish comprehensive written procedures for the review of access privileges and the testing of systems software changes.

Response:

The SSRC agrees with this recommendation. The SSRC will develop written procedures for reviewing access privileges and the testing of system software changes by April 16, 2010.

Current Status of Recommendation

On April 10, 2010 the SSRC implemented the following procedures to address these issues: IS110 – SSRC Quarterly Review of Computer System Access for Internal SSRC Users, IS111 – SSRC Review of Security Access Requests.

OIG Position

We agree with the actions taken by the SSRC and recommend this finding be closed.

Finding No. 6 – Other Security Controls

Certain SSRC security controls needed improvement in the areas of monitoring security events and authenticating system users.

Recommendation:

The SSRC should implement the appropriate security controls in the areas of monitoring security events and authenticating system users to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

Response:

The SSRC agrees with the recommendation. The SSRC has budgeted for FY10-11 software tools to enhance security controls in the areas of monitoring security events and authenticating users.

Current Status of Recommendation

SSRC's request for discretionary non-direct operational funding was cut by SSRC Board for FY 10-11 based on recommendations from TRW. The SSRC has submitted a request to fund this activity for the FY 11-12 budget.

The SSRC is implementing a 71A (F.A.C.) compliant security program based on FIPS and NIST standards published to implement Title III of the E-Government Act of 2002 (FISMA). SSRC security policies are comprehensive and based upon best practice NIST SP800-53 security classes (management, operational, and technical) and security controls. These are published in the SSRC Information Technology Security Policy Handbook (Draft June 4, 2010) available on the SSRC web site. In this manuscript, each NIST SP800-53 control maps to a specific SSRC numbered security policy. An anticipated completion date is June 30, 2011.

As part of the onboarding process, Shared Transition Service (STS) and Data Center Consolidation (DCC) customers are using FIPS 199 criteria to categorize information resources (Low, Moderate, High) for Confidentiality, Integrity, and Availability. These

categories map to one of three NIST SP800-53 baseline security control sets and to the new SSRC security policies.

OIG Position

We agree with the actions taken by the SSRC; however, until the new security policies have been completed the finding will remain open.

JSR/gz

cc: Kathy Dubose, Staff Director
Joint Legislative Auditing Committee

David W. Martin, Auditor General