REPORT NO. 2012-189
JUNE 2012

SOUTHWOOD SHARED RESOURCE CENTER

DATA CENTER OPERATIONS

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

EXECUTIVE DIRECTOR OF THE SOUTHWOOD SHARED RESOURCE CENTER

Pursuant to Section 282.205, Florida Statutes, the Southwood Shared Resource Center (SSRC) is established within the Department of Management Services (DMS) for administrative purposes only and is a separate budget entity that is not subject to control, supervision, or direction of DMS in any manner. Pursuant to Section 282.203(2), Florida Statutes, the head of SSRC is the Board of Trustees (Board), consisting of representatives from customer entities. The Executive Director is employed by and serves at the pleasure of the Board.

Board members and the customer entities represented and the Executive Director who served during the period April 2011 through September 2011 are listed below:

Board Member	Customer Entity Represented
Tony Powell, Vice Chair to 6-3-11, Chair from 6-4-11	Department of Revenue
David Faulkenberry, Chair to 6-3-11	Department of Management Services
Joe Wright from 6-1-11, Vice Chair from 7-1-11	Department of Management Services
Robert Dillenschneider, Vice Chair from 6-4-11 to 6-30-11	Department of Health
Nelson Hill	Department of Transportation
Kevin Patten	Member at Large
Denise Rodenbough	Department of Highway Safety and Motor Vehicles
Douglas Smith from 7-1-11	Department of Corrections
Kevin Thompson	Agency for Workforce Innovation*

John Wade, Executive Director

*Pursuant to Chapter 2011-142, Laws of Florida, programs from the Agency for Workforce Innovation were to be transferred to the Department of Economic Opportunity and the Department of Education by October 1, 2011.

The audit team leader was Chris Gohlke, CPA, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

SOUTHWOOD SHARED RESOURCE CENTER

Data Center Operations

SUMMARY

Pursuant to Sections 282.203(1)(a) and 282.205(1), Florida Statutes, the Southwood Shared Resource Center (SSRC) was established as a primary data center to serve as an information system utility for customer entities. Our audit focused on evaluating the effectiveness of selected information technology (IT) controls relevant to SSRC data center operations. We also determined the status of corrective actions regarding selected audit findings included in our report No. 2010-173.

The results of our audit are summarized below:

SERVICE-LEVEL AGREEMENTS

Finding No. 1: SSRC had not met some agreed-upon performance requirements or metrics within some of its service-level agreements (SLAs) and did not measure other performance metrics. A similar issue was noted in our report No. 2010-173.

GENERAL IT CONTROLS

Finding No. 2: SSRC had not established written procedures for mainframe performance monitoring.

Finding No. 3: SSRC procedures for the mainframe backup process were outdated. Additionally, as similarly noted in our report No. 2010-173, some backup tapes were not properly accounted for.

Finding No. 4: The *SSRC Continuity of Operations Plan Operational Procedures (COOP)* and the *Recovery Plan* had not been recently updated and SSRC staff had not received periodic training on implementing the plans.

Finding No. 5: SSRC did not have a complete, system-generated record of all systems software changes, and SSRC staff were unable to provide documentation of testing for some software changes. In addition, as similarly noted in our report No. 2010-173, SSRC change control procedures for testing changes to certain types of systems software were not comprehensive.

Finding No. 6: SSRC had not conducted periodic reviews of the appropriateness of access privileges and, as previously noted in our report No. 2010-173, did not have written procedures requiring such reviews for some platforms or comprehensive procedures for granting, modifying, or deactivating access privileges. Additionally, our audit disclosed some inappropriate access privileges at SSRC. A similar finding was noted in our report No. 2010-173.

Finding No. 7: Certain SSRC security controls related to user authentication, security event logging, and data transmission needed improvement. Some of these issues were also noted in our report No. 2010-173.

COST-MEASUREMENT AND DISTRIBUTION METHODOLOGY

Finding No. 8: Certain SSRC personnel costs were not allocated or documented in accordance with Federal requirements.

Finding No. 9: Contrary to State law and Federal requirements, SSRC staff were unable to provide supporting documentation of the methodology used in the process that formed the basis of the billing rates actually charged to customer entities.

Finding No. 10: Contrary to State law, SSRC lacked written policies and procedures for billing customers, managing receivables from customers, and establishing cost-recovery methodologies to be followed.

BACKGROUND

Section 282.201(1), Florida Statutes, provides that agency data centers and computing facilities are to be consolidated into primary data centers to the maximum extent possible by 2019. SSRC was established as one of the primary data centers to which State agencies are to migrate their computing resources.

SSRC is headed by a Board of Trustees (Board), consisting of representatives from customer entities. The Board appointed an Executive Director to be responsible for the daily operation of the data center. SSRC provides a variety of IT services to its customer entities, including equipment hosting and server management services. The customer entities consist of State agencies and other governmental entities that contract with SSRC for the aforementioned IT services. SSRC operates on a cost-recovery basis whereby SSRC bills the customer entities for a portion of its operating costs associated with the specific services provided to each customer entity. Lists of SSRC customer entities and services offered by SSRC are included in this report as EXHIBITS A and B, respectively.

FINDINGS AND RECOMMENDATIONS

Service-Level Agreements (SLAs)

Finding No. 1: SLA Service Levels and Performance Metrics

Section 282.203(1)(h), Florida Statutes, provides that each primary data center shall enter into an SLA with each customer entity to provide services as defined and approved by the Board. Additionally, Section 282.203(3)(d), Florida Statutes, provides that each board of trustees of a primary data center shall provide each customer entity with full disclosure concerning plans for new, additional, or reduced service requirements, including expected achievable service levels and performance metrics.

As a part of our audit, we reviewed the performance of SSRC in meeting the service levels and performance metrics set forth in selected SLAs with customer entities. SSRC had 117 SLAs in place as of June 9, 2011. We reviewed 39 performance requirements and metrics from the following 5 SLAs representing five of the six service categories offered by SSRC (as shown in Exhibit B):

Customer Entity	Service Category
Agency for Workforce Innovation (AWI)	Mainframe Services
Fish and Wildlife Conservation Commission (FWCC)	Storage Management
Department of Education (DOE)	Open Systems Platform
Department of Corrections (DOC)	Shared Transitional Service
Agency for Persons with Disabilities (APD)	Windows Platform

Our audit disclosed that SSRC had not met, or could not demonstrate that it had met, some agreed-upon performance requirements or metrics within the 5 SLAs and did not measure other performance metrics. Specifically:

- The business continuity plan developed by SSRC had not been submitted to AEIT for approval, contrary to the service description within the SLA with AWI.
- SLAs with AWI, FWCC, DOE, DOC, and APD provided for maximum response times for incidents based on severity levels. In response to audit inquiry, SSRC management indicated that they did not have tools in place to measure or monitor the response times and, therefore, SSRC had not evaluated specific compliance with this performance metric.

- The SLA with FWCC provided for the backup server to be available for 99.9 percent of scheduled availability and for a 95 percent success rate on production dataset backups. In response to audit inquiry, SSRC management indicated that they did not have tools in place to measure or monitor these performance metrics and, therefore, SSRC had not evaluated specific compliance therewith.
- The SLA with APD provided for the server to be available for 99.5 percent of scheduled availability. In response to audit inquiry, SSRC management indicated that they did not have tools in place to measure or monitor the server availability percentage and, therefore, SSRC had not evaluated specific compliance with this performance metric.

Through additional audit procedures, we noted that 4 other AWI SLAs included certain monthly performance reporting requirements that were not being met by SSRC. In response to audit inquiry, SSRC management indicated that these requirements were mistakenly included in the SLAs and did not apply to two of the SLA service types. SSRC management also indicated that, as similarly noted above, tools were not in place to meet the reporting requirements for the other two service types.

The inability to measure or monitor the performance metrics provided within the SLAs increases the risk that SSRC may not detect and react to problems or issues in a timely manner. Additionally, mistakenly included SLA provisions and the failure of SSRC to meet the requirements of SLAs increase the risk of customer dissatisfaction. A similar finding regarding SSRC performance in meeting an SLA service requirement was disclosed in our report No. 2010-173.

Recommendation: SSRC should improve its measurement and monitoring of the appropriateness of and compliance with SLA provisions. In part, SSRC should acquire the necessary tools to measure the agreed-upon performance metrics included in customer entity SLAs or modify the SLAs to provide for, where appropriate, other performance metrics that can be measured and monitored for compliance.

General IT Controls

Finding No. 2: Mainframe Performance Monitoring

Ongoing mainframe performance monitoring helps ensure that sufficient performance and capacity exist to meet the requirements of SLAs, minimizes the risk of service disruptions due to insufficient capacity or performance degradation, and assists in identifying excess capacity for possible redeployment.

Our audit disclosed that SSRC had not established written procedures for mainframe performance monitoring. Although SSRC monitored mainframe performance, without written procedures the risk is increased that mainframe performance may not be monitored consistently and in a manner pursuant to management's expectations and that performance problems, should they occur, will not be timely detected and corrected.

Recommendation: SSRC should establish written procedures for mainframe performance monitoring.

Finding No. 3: Mainframe Backup Process

There are a number of steps that an entity can take to minimize the risk of data loss that may occur from unexpected events. One example is routinely backing up data files and programs and securely storing the backups at an off-site location. Such actions maintain the entity's ability to restore data files that, if lost, may otherwise be impossible to recreate.

We requested SSRC written procedures for its mainframe backup process. In response, SSRC staff stated that their existing procedures were outdated and instead provided us with an informal narrative that, according to SSRC staff, was intended to be used as the basis for new, updated procedures. Absent current procedures, the risk is increased that backups may not be performed consistently and in a manner pursuant to management's expectations.

Using reports provided by SSRC denoting the location of its network and mainframe on-site and off-site tapes, we selected a sample of 41 of 5,773 on-site tapes and 40 of 2,527 off-site tapes to verify that the tapes were in the locations noted in SSRC records. Our review disclosed that 12 mainframe tapes (11 on-site and 1 off-site) included in our sample could not be located because the tapes were no longer in use and should have been removed from SSRC records. Additionally, as similarly noted in our report No. 2010-173, 3 on-site mainframe tapes were incorrectly recorded as being off-site. Inaccuracies in location records for backup tapes may limit SSRC's ability to timely and completely recover lost information in the event of a loss of production files. In addition, inaccurate tape backup records increase the risk that backup files may be lost that contain customer information that is confidential or exempt pursuant to Federal or State law.

Recommendation: SSRC should update its written procedures as appropriate to describe management's current expectations for the mainframe backup process and ensure the accuracy of its tape location records.

Finding No. 4: Business Continuity and Disaster Recovery Planning

Business continuity and disaster recovery planning is intended to facilitate a timely and orderly resumption of critical operations in the event of a disaster or other interruption of service. Our audit disclosed that the *SSRC Continuity of Operations Plan Operational Procedures (COOP)* and the *Recovery Plan* for SSRC needed improvement. Specifically:

- It is important that business continuity and disaster recovery plans be clearly documented and updated to reflect current operations. Although the *COOP* included an update date, this field was automatically updated to the current date whenever the document was opened; therefore, SSRC could not demonstrate when the document was last updated. Our review disclosed multiple instances where the *COOP* had not been recently updated. For example, the Information Security Manager for SSRC was hired on August 23, 2010, but her role was not mentioned in the *COOP*. Additionally, another employee who had terminated employment on January 1, 2010, was still referenced in the *COOP*.
- Periodic business continuity and disaster recovery training helps staff to understand their roles and responsibilities. Neither the *COOP* nor the *Recovery Plan* contained schedules or procedures for periodic training and the most recent documentation of training was for *COOP* training that had been offered by the Department of Management Services (DMS) in May 2008.

Under these conditions, the risk is increased that the business continuity and disaster recovery plans may not include the necessary provisions or be executed in a timely and effective manner in the event of an interruption in operations.

Recommendation: SSRC should review and update its *COOP* and *Recovery Plan* to accurately describe the current SSRC environment. SSRC should also ensure that periodic business continuity and disaster recovery training is scheduled and completed.

Finding No. 5: Change Control

Effective change control procedures help to ensure that all changes are tracked, documented, and approved. Comprehensive documentation includes documentation that changes were successfully tested and functioned as intended prior to being implemented.

SSRC was unable to provide us with a system-generated log of systems software changes that had been applied to the Windows, open systems, or mainframe platforms. Alternatively, SSRC provided us a listing of hardware and software change records that had been manually entered by staff into the Service Desk Express (SDE) system that is used for change management activities. SSRC did not have a mechanism in place to verify that all changes made to a platform were actually entered into the SDE system.

Notwithstanding the limitations of manually entered change records, we reviewed selected hardware and software changes recorded in the SDE system. Our review disclosed three software changes for which SSRC staff were unable to provide documentation substantiating that testing had occurred prior to implementation of the changes into the platform's production environment. Without a complete, system-generated record of systems software changes or adequate testing of the changes, the risk is increased that erroneous or unauthorized changes could be moved into the production environment.

Additionally, as also noted in our report No. 2010-173, SSRC had implemented change control procedures that allowed the data center to plan, schedule, and track software changes to the production and test environments; however, the procedures did not address the detailed processes to be used for testing changes to certain types of systems software. Without procedures for testing systems software, testing may not be performed in a consistent manner pursuant to management's expectations.

Recommendation: SSRC should implement system-generated logs to record, track, and report all system software changes that are made to a platform. Additionally, SSRC should ensure that, when applicable, all changes are tested and documentation of the test results is retained to demonstrate that testing occurred as intended by management. SSRC should also update its change control procedures to document management's expectations for systems software testing.

Finding No. 6: Access Privileges

Effective access controls include provisions for the periodic review of the appropriateness of access privileges and for account management controls related to granting, modifying, and deactivating access privileges.

Our audit disclosed that SSRC had not conducted comprehensive periodic reviews of the appropriateness of access privileges for any platform at SSRC. As also noted in our report No. 2010-173, SSRC did not have written procedures for periodically reviewing the access privileges assigned to users of certain system platforms. Additionally, SSRC lacked comprehensive written procedures for granting, modifying, or deactivating access privileges for systems under its management. Under these conditions, the risk is increased that inappropriate access privileges may exist and not be timely detected, as demonstrated by the following inappropriate security attributes (access privileges) that were disclosed in our audit:

- One system identification code (ID) was assigned an inappropriate combination of security attributes that were unnecessary for the system functions for which the system ID was used.
- Four system IDs were active but no longer needed by SSRC. In response to audit inquiry, SSRC staff deleted these IDs on August 22, 2011.
- Four system IDs were not assigned the PROTECTED attribute. The PROTECTED attribute prevents system IDs from being used to log on to the system and protects the system IDs from being revoked through inactivity or unsuccessful access attempts. In response to audit inquiry, SSRC staff assigned the PROTECTED attribute to these four system IDs on August 22, 2011.
- One user ID, shared among seven print operators, was assigned an unnecessary security attribute.

- As similarly noted in our report No. 2010-173, six user IDs were assigned to five former employees. SSRC staff were unable to determine the dates of termination for the five employees and, therefore, could not demonstrate how long the access privileges remained active after termination. In response to audit inquiry, SSRC management stated that a systems project administrator had used five of the user IDs since the former employees had terminated but that the use of three of the five user IDs was no longer necessary and provided documentation showing that the user IDs were deleted on August 22, 2011. Management additionally stated that these three user IDs were legacy IDs belonging to individuals who worked for DMS prior to the creation of SSRC in 2008 and had not been removed at the time of transition to SSRC. Management also stated that the remaining two user IDs were still required and provided documentation showing that the IDs were modified on August 22, 2011, to reflect the user associated with the two user IDs. One user ID was revoked in response to audit inquiry; however, SSRC management could not document the exact date the revocation took place, only that it had taken place by November 29, 2011. Management additionally stated that this user ID was a legacy ID belonging to an individual who worked for DMS prior to the creation of SSRC in 2008 and had not been removed at the time of transition to SSRC.
- Thirty-two user IDs were unnecessarily assigned a security attribute. Additionally, 25 of these user IDs also had an inappropriate combination of security attributes that could allow the user to circumvent an appropriate separation of duties.

We are not disclosing the specific security attributes and combinations thereof to avoid the possibility of compromising SSRC customer entity data and IT resources. However, we have notified SSRC management of the specific details.

Granting inappropriate access privileges to system IDs and current employees and allowing the access privileges of former employees to remain active beyond termination increases the risk that access privileges could be misused by employees or others. Sharing user IDs increases the risk that individuals may not be uniquely identifiable in the event access privileges are used inappropriately. Not assigning the PROTECTED attribute to system IDs increases the risk that the IDs may be used inappropriately by an individual or that the account may be revoked by a denial of service attack.

Recommendation: SSRC should establish and follow written procedures for conducting comprehensive periodic reviews of access privileges for all platforms at SSRC. SSRC should also establish written procedures for granting, modifying, and deactivating access privileges for systems under its management. Additionally, SSRC should ensure that access privileges do not exceed what is necessary for system IDs as well as assigned job duties and enforce an appropriate separation of incompatible duties. Furthermore, SSRC should assign the PROTECTED attribute to system IDs where appropriate and assign individual user IDs to all employees. SSRC should also ensure that the access privileges of former employees are deactivated in a timely manner.

Finding No. 7: Other Security Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain SSRC security controls related to user authentication, security event logging, and data transmission that needed improvement. Some of the issues were also noted in our report No. 2010-173. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising SSRC customer entity data and IT resources. However, we have notified appropriate SSRC management of the specific issues. Without adequate security controls related to user authentication, security event logging, and data transmission, the risk is increased that the confidentiality, integrity, and availability of data and IT resources may be compromised.

Recommendation: SSRC should improve security controls related to user authentication, security event logging, and data transmission to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

Cost-Measurement and Distribution Methodology

Finding No. 8: Allocation of Personnel Costs

Office of Management and Budget (OMB) Circular A-87, Attachment B, Section 8.d.(3), provides that, when a governmental unit uses the cash basis of accounting, the cost of leave is recognized in the period that the leave is taken and paid for. Payments for unused leave when an employee retires or terminates employment are allowable in the year of payment provided they are allocated as a general administrative expense to all activities of the governmental unit or component. However, our analysis of SSRC cost allocations determined that unused leave for retired or terminated employees paid in the 2009-10 fiscal year totaling $11,138 was not allocated as a general administrative expense to all activities in the 2009-10 fiscal year. Instead, these costs were charged to the cost objectives specific to the retired or terminated employees. Although the effect on the allocation results was not significant for the 2009-10 fiscal year, continued SSRC use of an alternative allocation method could result in more significant differences in allocation results in future periods, should there be larger numbers of retirements or other terminations of employment.

OMB Circular A-87, Attachment B, Section 8.h.(4), provides that, where employees work on multiple activities or cost objectives, a distribution of their salaries or wages will be supported by personnel activity reports or equivalent documentation that meets the standards in subsection (5) unless a statistical sampling system or other substitute system has been approved by the cognizant Federal agency. OMB Circular A-87, Attachment B, Section 8.h.(5), provides that personnel activity reports or equivalent documentation must meet the following standards:

- They must reflect an after-the-fact distribution of the actual activity of each employee;
- They must account for the total activity for which each employee is compensated;
- They must be prepared at least monthly and must coincide with one or more pay periods; and
- They must be signed by the employee.

A contractor performed the staff effort analyses as part of the SSRC Rate Analysis for SSRC Services for the 2009-10 fiscal year. He designated (estimated) percentages of staff effort as instructed through his interviews with SSRC management. This staff effort analysis based on estimated percentages, along with service utilization reports and actual expenditures, was used in generating the SSRC Service Rates for the 2009-10 fiscal year. Therefore, salaries and wages were incorporated into the rate charged for services based on an estimate rather than actual activities. As a result, SSRC cost allocation procedures were not in compliance with the requirements of OMB Circular A-87 and SSRC could not demonstrate that salaries and wages had been appropriately and equitably allocated to customer entities.

Recommendation: To comply with Federal requirements and demonstrate the appropriateness and equitability of SSRC costs of services, SSRC should allocate unused leave payments as a general administrative expense to all activities. Additionally, SSRC should utilize personnel activity reports or equivalent documentation to support future cost allocations of salaries and wages.

Finding No. 9: Cost of Services Documentation

Section 282.203(3)(e), Florida Statutes, provides that each board of trustees of a primary data center ensure the sufficiency and transparency of primary data center financial information. Additionally, OMB Circular A-87, Attachment C, Section A.1., provides that all costs and data used to distribute costs included in the central service cost allocation plan should be supported by formal accounting and other records that will support the propriety of the costs assigned to Federal awards.

The 2010-11 fiscal year SSRC billing rates charged to customer entities were calculated based on the estimated cost and utilization of the various SSRC services. SSRC performs this rate calculation process several times before finalizing the rates and each process is called a cycle. Cycle 6 information was used for the final rates charged to customer entities. For testing purposes, we selected six SSRC billing rates used to charge customer entities and noted that, for three of the six SSRC billing rates included in our test, SSRC staff were unable to provide supporting documentation of the methodology used in the Cycle 6 process for determining the estimated utilization of the related SSRC services. SSRC staff were able to provide supporting documentation for the Cycle 5 process that had been performed earlier. The Cycle 6 process resulted in lower billing rates for the three SSRC services than what was calculated in the Cycle 5 process. Consequently, without supporting documentation of the Cycle 6 process that formed the basis of the billing rates actually charged to customer entities, SSRC could not demonstrate that the established rates utilizing the Cycle 6 process were appropriate and equitably applied to the customer entities.

Recommendation: To demonstrate compliance with State law and Federal requirements and the appropriateness and equitability of SSRC billings, SSRC should maintain supporting documentation of the methodology used to determine the estimated utilization of services that is used, along with estimated cost, to establish billing rates actually charged to customer entities.

Finding No. 10: Policies and Procedures

Section 282.203(3)(b), Florida Statutes, provides that each board of trustees of a primary data center establish procedures to ensure that budgeting and accounting procedures, cost-recovery methodologies, and operating procedures are in compliance with applicable laws, rules, and Federal regulations. Additionally, Section 282.203(3)(e)1., Florida Statutes, provides that each board of trustees ensure the sufficiency and transparency of primary data center financial information by, among other things, establishing policies that ensure that cost-recovery methodologies, billings, receivables, expenditure, budgeting, and accounting data are captured and reported timely, consistently, accurately, and transparently.

Our audit disclosed that, contrary to State law, SSRC lacked written policies and procedures for billing customers, managing receivables from customers, and establishing cost-recovery methodologies to be followed. Absent written policies and procedures, the risk is increased that data center billing and cost-recovery functions may not be performed consistently and in a manner pursuant to management and Board expectations.

Recommendation: SSRC should establish written policies and procedures that document management's expectations for billing customers, managing receivables from customers, and establishing cost-recovery methodologies.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, SSRC had taken corrective actions for findings included in our report No. 2010-173 that were within the scope of this audit.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit during the period April 2011 through September 2011 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations at SSRC. An additional objective was to determine the extent to which SSRC corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2010-173.

The scope of our audit focused on selected general IT controls relevant to SSRC data center operations, including selected general IT controls over security and operations. The scope of our audit also included evaluating selected controls applicable to SSRC's governance, migration process, and cost-measurement and distribution methodology.

In conducting our audit, we:

- Interviewed SSRC personnel.
- Obtained an understanding of the services offered by SSRC and the directives, policies, and procedures governing SSRC's operations.
- Obtained an understanding of key SSRC IT controls and toured the SSRC data center. We observed and evaluated the effectiveness of key processes and procedures related to SSRC.
- Obtained an understanding of the IT infrastructure and architecture of SSRC.
- Observed and evaluated selected controls over SSRC IT resource inventory to determine the effectiveness of inventory tracking procedures. Specifically, we reviewed a sample of 15 items of SSRC IT resource inventory from its inventory records as of April 14, 2011, to determine if the equipment could be physically located. We additionally reviewed a sample of 15 items of equipment that were physically located on the floor of the data center on April 21, 2011, to determine if the equipment was properly recorded in the inventory records.
- Observed and evaluated selected controls regarding background screenings for employees with access to SSRC IT resources. Specifically, we reviewed a sample of 25 SSRC employees with potential access to sensitive IT resources to determine whether they had undergone required background checks.
- Obtained an understanding of the statutory requirements and organizational structure of SSRC data center operations and evaluated the effectiveness of SSRC compliance with selected requirements.
- Observed and evaluated logical access control mechanisms utilized by SSRC including password controls, use of remote administration software tools, and assignment of access privileges. Specifically, we reviewed the

access privileges of the six SSRC employees with administrative access privileges for Open Systems as of August 5, 2011, and the five SSRC employees with administrative access privileges for Windows as of August 11, 2011. We also reviewed the access privileges for 67 mainframe user IDs across selected mainframe logical partitions that had been assigned certain security attributes.

- Observed and evaluated the adequacy of SSRC physical security and environmental safeguards in place to protect IT resources. Specifically, we evaluated the appropriateness of access privileges for the 71 individuals with physical access to the SSRC administrative facility as of April 13, 2011, and the 90 individuals with physical access to the SSRC data center as of April 15, 2011.
- Observed and evaluated the adequacy of selected disaster recovery and continuity of operations planning controls, including backup procedures. Specifically, we tested SSRC *COOP*, disaster recovery plan, and other business continuity-related documents to determine if they contained selected provisions. We additionally reviewed a sample of 20 on-site and 20 off-site network tapes as of June 24, 2011, and 21 on-site and 20 off-site mainframe tapes as of August 4, 2011, to determine if SSRC inventory records were accurate and whether all tapes could be located. We also tested an additional 12 on-site network tapes and 11 off-site network tapes to determine the appropriateness of their status as recorded in SSRC inventory records.
- Observed and evaluated the adequacy of selected controls over the modifications of systems software. Specifically, we reviewed a sample of ten successfully completed normal and emergency changes entered into the Service Desk Express system with an open date between January 1, 2011, and August 8, 2011.
- Observed and evaluated controls surrounding processes used by SSRC for performance and capacity monitoring.
- Observed and evaluated SLAs established between SSRC and its customer entities to determine whether selected provisions required in Section 282.203, Florida Statutes, were included. Additionally, we tested 39 selected provisions included in five SLAs to determine whether SSRC was in compliance with these provisions.
- Observed and evaluated the effectiveness of the cost-measurement and cost-allocation methods used by SSRC. Specifically, we tested six selected SSRC approved rates for the 2010-11 fiscal year to determine if both the cost of service and the billable units were identified, reasonable, measureable, appropriately allocated, service-based, transparent, properly documented, and auditable. We also tested five selected cost pools from the 2009-10 fiscal year to determine if all actual costs had been identified and used in the allocation process.
- Observed and evaluated the controls surrounding the billing process utilized by SSRC. Specifically, we reviewed a sample of ten checks selected from a check log and 20 invoices prepared for services rendered by SSRC from the period July 2010 through March 2011 to determine if SSRC customers were properly billed, payments monitored, and collections made for services rendered by SSRC.
- Performed various other auditing procedures as necessary to accomplish the objectives of the audit.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated June 15, 2012, the SSRC Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT C.

EXHIBIT A

LIST OF SSRC CUSTOMER ENTITIES
AS OF SEPTEMBER 19, 2011

Agency for Health Care Administration	Department of Revenue
Agency for Persons with Disabilities	Department of State
Agency for Workforce Innovation	Department of Transportation
Children's Home Society	Department of Veterans' Affairs
Community Based Care of Seminole	Executive Office of the Governor
Community Based Care of Brevard	Florida Fish and Wildlife Conservation Commission
Department of Business and Professional Regulation	Florida Legislature
Department of Children and Family Services	Florida Parole Commission
Department of Citrus	Greater Orlando Aviation Authority
Department of Community Affairs	Justice Administrative Commission
Department of Corrections	Miami-Dade Expressway Authority
Department of Education	Office of the Attorney General
Department of Elder Affairs	Public Service Commission
Department of Environmental Protection	Santa Rosa County
Department of Financial Services	State Attorney - 14th Circuit
Department of Health	State Board of Administration
Department of Highway Safety and Motor Vehicles	Statewide Guardian Ad Litem
Department of Juvenile Justice	Water Management District - Northwest Florida
Department of the Lottery	Water Management District - Suwannee River
Department of Management Services	

EXHIBIT B

LIST OF SERVICES OFFERED BY SSRC
AS OF SEPTEMBER 19, 2011

Service Category	Service Type Detail
Data Center Management	Additional Electrical Circuit
	Print Impressions
	Off-Site Tape Storage Transportation
	Off-Site Tape Administration
	Scheduling Services
	SRC Floor Tiles
	SRC Rack Mounts
	SRC Tape Vault
Mainframe Services	IBM Batch CPU
	IBM CICS CPU
	IBM DB2 CPU
	IBM Middleware
	IBM TSO CPU
	IBM Tape Cartridges
	Mainframe Managed Unisys Service
	Mainframe Mirrored Disk Storage (Tier 1)
	Mainframe Unmirrored Disk Storage (Tier 1)
Open Systems Platform	Electronic Data Interchange (EDI) Translation
	Managed Server - Oracle Premium
	Net Based Services
	UNIX Managed Server (Standard/Premium)
	UNIX Capacity Units
Storage Management	Backup Service
	Mirrored Disk Storage (Tier 1-3)
	Unmirrored Disk Storage (Tier 1-3)
Windows Platform	Hosted Messaging Services (E-mail)
	Windows Managed Server (Standard/Premium)
	Managed SQL Cluster
	Windows Capacity Unit
Shared Transitional Service	Transitional Service

EXHIBIT C
MANAGEMENT'S RESPONSE

State of Florida
Southwood Shared Resource Center
2585 Shumard Oak Boulevard
Tallahassee, Florida 32399-0950
Phone: 850.413.9300
Fax: 850.921.8343
http://ssrc.myflorida.com

Governor
Rick Scott

Executive Director
John Wade

June 15, 2012

Mr. David W. Martin, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our response to your report, *Southwood Shared Resource Center – Data Center Operations – Information Technology Operational Audit.* Our response corresponds with the order of your preliminary and tentative findings and recommendations.

Finding No. 1 – SLA Service Levels and Performance Metrics

SSRC had not met some agreed-upon performance requirements or metrics within some of its service-level agreements (SLAs) and did not measure other performance metrics.

Recommendation

1. SSRC should improve its measurement and monitoring of the appropriateness of and compliance with SLA provisions.

2. SSRC should acquire the necessary tools to measure the agreed-upon performance metrics included in customer entity SLAs or modify the SLAs to provide for, where appropriate, other performance metrics that can be measured and monitored for compliance.

Response

The SSRC concurs with the recommendations however funds are not available for the toolsets needed to accomplish the documented SLA measurement, monitoring and compliance provisions. It is estimated that such tools would cost several hundred thousand dollars to implement, per tool. The SSRC will continue to attempt to seek funding for operational tools through the LBR process.

The SSRC SLAs have been agency driven with many detailed special service objectives in their SLA amendment because the agencies desire assurance of service for specific tasks that are essential to their business. The SSRC needs to refine its current process and only allow amendment items that measurement can be obtained. The SSRC will develop a plan to implement such changes by end of fiscal year 2012/2013.

Finding No. 2 – Mainframe Performance Monitoring

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

SSRC had not established written procedures for mainframe performance monitoring.

Recommendation

1. SSRC should establish procedures for mainframe performance monitoring.

Response

The SSRC concurs with the recommendation.. The SSRC is in the process of defining and documenting procedures for the Omegamon products that is utilized for performance monitoring in our mainframe platform. The scheduled completion date is December 2012.

Finding No. 3 – Mainframe Backup Process

SSRC procedures for the mainframe backup process were outdated. Additionally, some backup tapes were not properly accounted for.

Recommendation

1. SSRC should update its written procedures as appropriate to describe management's current expectations for the mainframe backup process and ensure the accuracy of its tape location records.

Response

The SSRC concurs with the recommendation and will update the recommended procedures by the end of fiscal year 2012/2013. The SSRC has updated, documented and implemented back-up procedures for our mainframe platform as of May 2012.

Finding No. 4 – Business Continuity and Disaster Recovery Planning

The SSRC Continuity of Operations Plan Operational Procedures (COOP) and the Recovery Plan had not been recently updated and SSRC staff had not received periodic training on implementing the plans.

Recommendation

1. SSRC should review and update its COOP and Recovery Plan to accurately describe the current SSRC environment.

2. SSRC should also ensure that periodic business continuity and disaster recovery training is scheduled and completed.

Response

The SSRC concurs with these recommendations and has completed reviewing and

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

updating the COOP and Recovery Plan as of May 2012. In addition, the SSRC has scheduled and completed COOP and disaster recovery training and will continue to periodically schedule this training as of May 2012.

Finding No. 5 – Change Controls

SSRC did not have a complete, system-generated record of all systems software changes, and SSRC staff were unable to provide documentation of testing for some software changes. In addition, SSRC change control procedures for testing changes to certain types of systems software were not comprehensive.

Recommendation

1. SSRC should implement system-generated logs to record, track, and report all system software changes that are made to a platform.

2. SSRC should ensure that, when applicable, all changes are tested and documentation of the test results are retained to demonstrate that testing occurred as intended by management.

3. SSRC should also update its change control procedures to document management's expectations for systems software testing.

Response

The SSRC concurs with recommendation number one; however funds are not available for a system-generated toolset. It is estimated that such a toolset would cost several hundred thousand dollars to implement. The SSRC will continue to attempt to seek funding for operational tools through the LBR process.

With regard to recommendation number two, the SSRC does not control the testing of many of the changes due to the fact that the SSRC does not control the applications. That testing responsibility belongs to the customer agencies. In many cases, it is not technically possible for the SSRC to test the changes. The SSRC will modify our SLAs to clearly identify that it is the customer's responsibility to test after an SSRC change. The SSRC works within the established customer environments tests all changes, when applicable, and concurs with the need for documentation of all applicable test results.

The SSRC concurs with recommendation number three. The SSRC will update its testing procedures to clarify that all applicable changes are tested, that the expectations of customer testing is clear, and that documentation will be kept for the results of all changes that have been tested by the data center. This procedural update will be completed by the end of fiscal year 2012/2013.

Finding No. 6 – Access Privileges

SSRC had not conducted periodic reviews of the appropriateness of access privileges

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

and, did not have written procedures requiring such reviews for some platforms or comprehensive procedures for granting, modifying, or deactivating access privileges. Additionally, our audit disclosed some inappropriate access privileges at SSRC.

Recommendation

1. SSRC should establish and follow written procedures for conducting comprehensive periodic reviews of access privileges for all platforms at the SSRC.

2. SSRC should establish written procedures for granting, modifying, and deactivating access privileges for systems under its management.

3. SSRC should ensure that access privileges do not exceed what is necessary for system IDs as well as assigned job duties and enforce an appropriate separation of incompatible duties.

4. SSRC should assign the PROTECTED attribute to system IDs where appropriate and assign individual user IDs to all employees.

5. SSRC should ensure that the access privileges of former employees are deactivated in a timely manner.

Response

The SSRC concurs with recommendation number one and number two. Prior to the audit, the SSRC had begun the process of establishing written procedures for conducting comprehensive periodic reviews of access privileges for all platforms at the SSRC as well as the granting, modifying, and deactivating access privileges. It is anticipated that this process will be fully implemented by the end of fiscal year 2012/2013.

The SSRC concurs with recommendation number three and number four regarding system IDs as specifically referenced in the mainframe environment. As a result of this audit, the PROTECTED attribute has been verified as assigned to all applicable system IDs. In addition, all employees now have individual user IDs.

The SSRC agrees in principle with respect to recommendation number five. The SSRC ensures that access privileges of former SSRC employees are deactivated in a timely manner. As a result of data center consolidations, there may be instances where the consolidating agency's prior employee IDs have not been revoked and are not known to the SSRC. The SSRC works with the consolidating agencies as part of administrative credential remediation to identify these situations and resolve accordingly. This particular finding was specific to IDs that were left over from the Department of Management Services (DMS) prior to the SSRC being statutorily created. Upon discovery of the IDs in question, they were immediately removed. The SSRC will conduct a review of all IDs to confirm that each is assigned to a current employee. The IDs in question could not have been utilized because the system automatically

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

places the IDs in a revoked status after a preconfigured number of days not in use, so there was no risk associated with this finding.

Finding No. 7 – Other Security Controls.

Certain SSRC security controls related to user authentication, security event logging, and data transmission needed improvement.

Recommendation

1. SSRC should improve security controls related to user authentication, security event logging, and data transmission to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

Response

The SSRC concurs with the recommendation. Previously the SSRC sought funding for the toolset needed to resolve this issue. Funding has been approved for fiscal year 2012/2013. The SSRC is currently in the RFQ process for this toolset and it is expected that the tool will be purchased and implemented by the end of fiscal year 2012/2013.

Finding No. 8 – Allocation of Personnel Costs.

Certain SSRC personnel costs were not allocated or documented in accordance with Federal requirements.

Recommendation

1. To comply with Federal requirements and demonstrate the appropriateness and equitability of SSRC costs of services, SSRC should allocate unused leave payments as a general administrative expense to all activities.

2. SSRC should utilize personnel activity reports equivalent documentation to support future cost allocations of salaries and wages.

Response

The SSRC concurs and will implement allocation of unused leave payments as a general administrative expense to all activities. Further, the SSRC will work to develop some form of personnel activity reports to support cost allocations of personnel costs by the end of fiscal year 2012/2013.

Finding No. 9 – Cost of Services Documentation.

Contrary to State law and Federal requirements, SSRC staff were unable to provide supporting documentation of the methodology used in the process that formed the basis of the billing rates actually charged to customer entities.

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation

1. To demonstrate compliance with State law and Federal requirements and the appropriateness and equitability of SSRC billings, SSRC should maintain supporting documentation of the methodology used to determine the estimated utilization of services that is used, along with estimated cost, to establish billing rates actually charged to customer entities.

Response

The SSRC concurs with the recommendation and in October 2011 implemented a process in which all documentation for each forecast cycle is maintained, including versions. It is important to note that the SSRC has always maintained all supporting documentation for actual utilization and expenditures which supports our agency true-up process each year.

Finding No. 10 – Policies and Procedures.

Contrary to State law and Federal requirements, SSRC lacked written policies and procedures for billing customers, managing receivables from customers, and establishing cost-recovery methodologies to be followed.

Recommendation

1. SSRC should establish written policies and procedures that document management's expectations for billing customers, managing receivables from customers, and establishing cost-recovery methodologies

Response

The SSRC concurs with the recommendation and on April 19, 2012 implemented an Accounts Receivable Collocations Write-Off and Cash Receipts Directives which addresses this recommendation.

If you need additional information concerning this matter, you may contact me at (850) 413-0604.

Sincerely,

John M. Wade, Executive Director

A Certified Tier III Facility