REPORT NO. 2014-052
DECEMBER 2013

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, pursuant to Section 282.203(3)(a), Florida Statutes, 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 July 1, 2012, through June 30, 2013, are listed below:

Board Member	Customer Entity Represented
Kevin Patten, Chair to February 2013	Member at Large
Douglas Smith, Vice Chair to February 2013, Chair from February 2013	Department of Corrections
Denise Rodenbough, Vice Chair from February 2013	Department of Highway Safety and Motor Vehicles
Robert Dillenschneider	Department of Health
Tony Powell	Department of Revenue
Nelson Hill	Department of Transportation
Kristin Pingree to September 2012	Department of Highway Safety and Motor Vehicles
Tony Lloyd	Department of Economic Opportunity
Scott Morgan from February 2013	Member at Large

John Wade, Executive Director to November 2012
Robert E. Poston, Interim Executive Director from December 2012

The audit team leader was Daniel Pearce, CISA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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) 412-2722; 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 operational 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. 2012-189.

The results of our audit are summarized below:

SERVICE-LEVEL AGREEMENTS

Finding No. 1: Contrary to State law, service-level agreements (SLAs) had not been established with some SSRC customer entities.

GENERAL IT CONTROLS

Finding No. 2: As similarly noted in prior audits of SSRC, most recently our report No. 2012-189, some backup tapes were not properly accounted for.

Finding No. 3: As similarly noted in our report No. 2012-189, SSRC did not have a complete, system-generated log of all systems software changes. Also, SSRC staff was unable to provide documentation that approval had occurred prior to implementation for one software change. In addition, as similarly noted in prior audits of SSRC, most recently our report No. 2012-189, SSRC change control procedures for testing changes to certain types of systems software were not comprehensive.

Finding No. 4: As similarly noted in our report No. 2012-189, SSRC had not conducted comprehensive periodic reviews of the appropriateness of access privileges. Additionally, as similarly noted in prior audits of SSRC, most recently our report No. 2012-189, SSRC had not implemented written procedures requiring such reviews, and our audit again disclosed some inappropriate access privileges at SSRC.

Finding No. 5: Certain SSRC security controls related to user authentication and security event logging needed improvement. Some of these issues were also noted in prior audits of SSRC, most recently our report No. 2012-189.

Finding No. 6: SSRC could not provide access authorization documentation for the user access privileges for some employees.

BACKGROUND

Section 282.201(1), Florida Statutes, provides that, unless otherwise exempt by law, all agency data centers and computing facilities are to be consolidated into a primary data center 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 employed 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 entities that contract with SSRC for the aforementioned IT services. 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

Finding No. 1: Service-Level Agreements with Customer Entities

A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. SLAs are necessary to define the IT services provided by SSRC to State agencies and other entities and to ensure that services provided by SSRC support the business objectives of the customer entities. SLAs define the roles and responsibilities of each party. SLAs also set forth the billing methodology and the costs of the services to be paid by customer entities. Section 282.203(1)(i), Florida Statutes, provides that each primary data center shall enter into a SLA with each customer entity to provide services as defined and approved by the Board.

As of June 11, 2013, SSRC was providing various IT services, such as server management and equipment hosting, to a customer base of 41 entities (see EXHIBITS A and B). As of June 11, 2013, signed SLAs existed with 37 customer entities for the services provided to those entities. There were no signed SLAs between SSRC and the remaining 4 customer entities.

Without mutually agreed-upon SLAs that establish in writing the requirements of both SSRC and customer entities, the risk is increased that IT service requirements and SSRC expectations of the customer entities will not be sufficiently met. Under such conditions, the effective, efficient, and secure operation of IT systems could be jeopardized.

Recommendation: SSRC should enter into mutually agreed-upon SLAs with its customer entities as required by State law.

General IT Controls

Finding No. 2: Backup Tapes

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.

Using reports provided by SSRC denoting the location of its network and mainframe tapes, we reviewed listings of 1,953 network and 56 mainframe off-site backup tapes as of June 27, 2013, to verify that the tapes were in the locations indicated by SSRC records. As similarly noted in prior audits of SSRC, most recently our report No. 2012-189, our review disclosed that 8 network tapes and 4 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 backup tape 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 enhance controls to ensure the accuracy of its backup tape location records.

Finding No. 3: Change Control

Effective change control procedures help to ensure that all changes are tracked, documented, and approved. Comprehensive documentation includes documentation that changes were properly approved by management.

As similarly noted in our report No. 2012-189, 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 10 selected hardware and software changes recorded in the SDE system. Our review disclosed 1 software change for which SSRC staff was unable to provide documentation that approval had occurred prior to implementation of the change into the production environment. Without a complete, system-generated log of systems software changes or appropriate approval of the changes, the risk is increased that erroneous or unauthorized changes could be moved into the production environment.

Additionally, as similarly noted in prior audits of SSRC, most recently our report No. 2012-189, 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 all changes are appropriately approved and documentation of the approval is retained. SSRC should also update its change control procedures to document management's expectations for systems software testing.

Finding No. 4: 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.

As similarly noted in our report No. 2012-189, our audit disclosed that SSRC had not conducted comprehensive periodic reviews of the appropriateness of access privileges for any platform at SSRC. Also, as similarly noted in prior audits of SSRC, most recently our report No. 2012-189, SSRC had not established written procedures for periodically reviewing the access privileges assigned to users for all platforms. Without periodic review of the appropriateness of access privileges, the risk is increased that inappropriate access privileges may exist and not be timely detected, as demonstrated by the following inappropriate access privileges that were disclosed in our audit:

- As similarly noted in prior audits of SSRC, most recently our report No. 2012-189, two user IDs were assigned to former SSRC employees. The access privileges of the two former employees remained active for 237 and 398 days.

- As similarly noted in our report No. 2012-189, eight user IDs 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 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.

Recommendation: SSRC should establish and follow written procedures for conducting comprehensive periodic reviews of access privileges for all platforms at SSRC. SSRC should also ensure that the access privileges of former employees are deactivated in a timely manner. Additionally, SSRC should ensure that access privileges enforce an appropriate separation of incompatible duties.

Finding No. 5: 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 and security event logging that needed improvement. Some of the issues were also noted in prior audits of SSRC, most recently our report No. 2012-189. 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 and security event logging, 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 and security event logging to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

Finding No. 6: Access Authorizations

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(1), Florida Administrative Code, provides that information owners shall be responsible for authorizing access to information. Effective access authorization practices include, among other things, the use of access authorization forms to document the user access privileges that management has authorized.

We requested access authorization documentation for users of various systems managed by SSRC to determine if access granted was adequately documented and authorized. SSRC could not provide access authorization documentation for the user access privileges for the selected SSRC employees and contractors included in our tests as described below:

- Five employees with various levels of access privileges to SSRC mainframes as of June 27, 2013.
- Twelve employees and contractors with access privileges to the SSRC open systems platform servers as of July 25, 2013, and July 26, 2013.
- Four employees with administrative access privileges to SSRC-managed network domains as of June 17, 2013.

[1] During the 2012 Legislative Session, HB 5011 that abolished AEIT and reassigned the functions and duties of AEIT to a new State agency was passed by the Legislature and presented to the Governor for signature. The bill was vetoed by the Governor on April 20, 2012. However, AEIT underwent defacto dissolution as the 2012 General Appropriations Act made no appropriations for the funding of positions in AEIT. As of the completion of our audit, rulemaking authority and responsibility for promoting or enforcing compliance with existing AEIT rules had not been established.

The access privileges granted, however, did not appear to be excessive based on the job duties of the SSRC employees and contractors. Nevertheless, these conditions limit management's assurance that access privileges granted to employees and contractors do not exceed what is necessary for the accomplishment of assigned job responsibilities.

Recommendation: SSRC should maintain documentation of management authorization for employee and contractor access privileges in a manner that is retrievable by SSRC management.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, SSRC had taken corrective actions for findings included in our report No. 2012-189 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 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. 2012-189.

The scope of our audit focused on evaluating selected IT controls applicable to SSRC data center operations during the period July 1, 2012, through June 30, 2013, and selected SSRC actions through July 26, 2013.

This audit was designed to identify, for the data center operations and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the data center operations and IT controls included within the scope of the audit, the audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the IT controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and vendors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed SSRC personnel.
- 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.
- Obtained an understanding of the services offered by SSRC and the directives, policies, procedures, and processes governing SSRC operations.
- Evaluated the effectiveness of controls surrounding processes used by SSRC for service request processing, tracking and reporting service-level metrics, performance monitoring, and capacity planning. Specifically, we evaluated the adequacy of fulfillment of 14 selected service metrics across five service types provided by SSRC to customer entities.
- Evaluated the effectiveness of selected disaster recovery and continuity of operations planning controls, including backup procedures. Specifically, we reviewed the SSRC ***Continuity of Operations Plan*** to determine if it contained selected required statutory provisions. We additionally reviewed the location of 1,953 network and 56 mainframe off-site tapes as of June 27, 2013, to determine if SSRC inventory records were accurate.
- Evaluated the effectiveness of selected controls over the modifications of systems software, including software patch management procedures. Specifically, we reviewed 10 of 91 selected changes entered into the Service Desk Express system between July 1, 2012, and June 6, 2013.
- Obtained an understanding of the IT infrastructure and architecture of SSRC.
- Evaluated the effectiveness of password settings in adequately protecting IT resources.
- Evaluated the effectiveness of antivirus controls in place to protect IT resources.
- Evaluated the effectiveness of SSRC physical security and environmental safeguards in place to protect IT resources. Specifically, regarding SSRC physical security, we evaluated the appropriateness of access privileges for 6 of 25 SSRC employees with physical access to the data center floor as of April 24, 2013. Specifically, regarding SSRC environmental controls, we evaluated the effectiveness of fire detection and suppression controls, controls to prevent water damage to equipment, controls for continuity of operations during power outages, and temperature and humidity controls.
- Evaluated the appropriateness of access to various systems managed by SSRC. Specifically, we reviewed the access privileges for 5 of 16 SSRC employees and customer entity staff with administrative access attributes to SSRC mainframes as of June 27, 2013 all 21 current and former SSRC employees and contractors with access to 23 of 225 SSRC open systems platform servers as of July 25, 2013, and July 26, 2013; and 4 of 16 SSRC employees and contractors with administrative access to SSRC-managed domains as of June 17, 2013.
- Evaluated the effectiveness of procedures for performing background screenings and authorizing employee access privileges to IT resources. Specifically, we reviewed 12 of 115 SSRC employees and contractors as of May 20, 2013, to determine whether the SSRC employees and contractors underwent Level 2 security background investigations as a condition of employment and continued employment pursuant to Section 435.04, Florida Statutes.
- 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 November 14, 2013, the 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 JUNE 11, 2013

Agency for Health Care Administration	Department of State
Agency for Persons with Disabilities	Department of the Lottery
Brevard Family Partnership	Department of Transportation
Children's Home Society	Department of Veterans' Affairs
Commission on Human Relations	Division of Emergency Management
Community Based Care of Central Florida	Executive Office of the Governor
COPE Center, Inc.	Florida Fish and Wildlife Conservation Commission
Department of Business and Professional Regulation	Florida Legislature
Department of Children and Families	Greater Orlando Aviation Authority
Department of Citrus	Justice Administrative Commission
Department of Corrections	Miami-Dade Expressway Authority
Department of Economic Opportunity	Northwood Shared Resource Center
Department of Education	Office of Early Learning
Department of Elder Affairs	Public Employees Relations Commission
Department of Financial Services	Public Service Commission
Department of Health	Santa Rosa County
Department of Highway Safety and Motor Vehicles	State Attorney - 14th Circuit
Department of Juvenile Justice	Statewide Guardian Ad Litem
Department of Management Services	Water Management District - Northwest Florida
Department of Military Affairs	Water Management District - Suwannee River
Department of Revenue	

EXHIBIT B
LIST OF SERVICES OFFERED BY SSRC
FOR THE 2012 - 2013 FISCAL YEAR

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	Mainframe - z/OS Processing
	Mainframe - CICS Processing
	Mainframe - DB2 Processing
	Mainframe Storage
	Mainframe Backup\Virtual Storage
Open Systems Platform	Electronic Data Interchange (EDI) Translation
	Managed Server - Oracle Premium
	Net Based Services
	UNIX Managed Server Standard
	Managed SQL Cluster
	UNIX Managed Server Premium
	UNIX Capacity Units
Storage Management	Distributed Backup
	Distributed Storage - Unmirrored/Mirrored
	Tier 4 DOR
Windows Platform	Hosted Messaging Services (Short Term)
	Windows Managed Server Premium
	Windows Capacity Unit
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
Tony K. Powell

November 14, 2013

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 – Service-Level Agreements with Customer Entities

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

Recommendation

1. SSRC should enter into mutually agreed-upon SLAs with its customer entities as required by State law.

Response

The SSRC concurs with this finding in principle. The SSRC will continue to work with the customers which refuse to sign an SLA with the SSRC.

Finding No. 2 – Backup Tapes

As similarly noted in prior audits of SSRC, most recently our report No. 2012-189, some backup tapes were not properly accounted for.

Recommendation

1. SSRC should enhance controls to ensure the accuracy of its backup tape location records.

A Certified Tier III Facility

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

Response

The SSRC agrees with the recommendation in principle. The sampling inaccuracy of 8 out of 1953 tapes tested for the client server tapes is a reasonable percentage, given the immense volume of tapes the SSRC processes on a yearly basis. Additionally, the SSRC standard backup process produces two sets of backup the same backup tape, so if one is not properly accounted for, the matching copy is.

Prior to the current audit and as a result of report No. 2012-189, the SSRC purchased a reconciliation program that is in the last stages of deployment. This software will account for all tapes (the tens of thousands that the SSRC processes each year) and inaccuracies will no longer occur. The reconciliation program deployment will be complete by the end of the calendar year.

Finding No. 3 – Change Control

As similarly noted in our report No. 2012-189, SSRC did not have a complete, system-generated log of all systems software changes. Also, SSRC staff was unable to provide documentation that approval had occurred prior to implementation for one software change. In addition, as similarly noted in prior audits of SSRC, most recently our report No. 2012-189, 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 all changes are appropriately approved and documentation of the approval is retained.
3. SSRC should also update its change control procedures to document management's expectations for systems software testing.

Response

The SSRC concurs in principle with recommendation number #1 and has been requesting funding for such a toolset over the past several years. This particular item is a subset of a much larger issue, full information technology governance. The data center is one portion of the layers of responsibility within this particular change control concept, there are three or more participants that should be accountable. With the acquisition of two new operational toolsets, we believe that we will be better prepared to respond with system generated log information during the next audit.

A Certified Tier III Facility

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

The funding was approved for fiscal year 2012/2013. During the current audit, the SSRC was in the procurement phase of this project. The SSRC is currently in the implementation phase of the project and anticipates the toolset being implemented by the end of fiscal year 2013/2014.

The SSRC agrees with recommendation #2 in principle and as a result will review our internal processes and adjust as necessary. However, the inaccuracy of 1 sampled change that the SSRC processed an inappropriately approved change request is reasonable.

The SSRC concurs with recommendation #3 and will update processes to more clearly address management expectation of the areas support by the data center, by the end of the fiscal year 2013/2014.

Finding No. 4 – Access Privileges

As similarly noted in our report No. 2012-189, SSRC had not conducted comprehensive periodic reviews of the appropriateness of access privileges. Additionally, as similarly noted in prior audits of SSRC, most recently our report No. 2012-189, SSRC had not implemented written procedures requiring such reviews, and our audit again 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 SSRC.
2. SSRC should also ensure that the access privileges of former employees are deactivated in a timely manner.
3. Additionally, SSRC should ensure that access privileges enforce an appropriate separation of incompatible duties.

Response

The SSRC concurs with recommendation # 1 and #2 in principle. Prior to the current audit, the SSRC had begun the process of establishing written procedures for access authorization and provided this documentation to the auditor general to show progress of this finding. Typically the SSRC would lean toward automation of such a finding, however, given that the environment is complex, we are addressing this finding with manual procedures. The new process is in final review and is expected to be rolled out by the end of the calendar year.

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

The SSRC concurs with recommendation #3 regarding the mainframe separation of duties. The SSRC will address and complete this task by the end of the fiscal year 2013/2014.

Finding No. 5 – Other Security Controls

Certain SSRC security controls related to user authentication and security event logging needed improvement. Some of these issues were also noted in prior audits of SSRC, most recently our report No. 2012-189.

Recommendation

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

Response

The SSRC concurs with this recommendation. Previous to report No. 2012-189, the SSRC sought funding for the toolset needed to resolve this issue. The funding was approved for fiscal year 2012/2013. During the current audit, the SSRC was in the procurement phase of this project. The SSRC is currently in the implementation phase of the project and anticipates the recommendation being completed by the end of fiscal year 2013/2014.

Finding No. 6 – Access Authorization

SSRC could not provide access authorization documentation for the user access privileges for some employees.

Recommendation

SSRC should maintain documentation of management authorization for employee and contractor access privileges in a manner that is retrievable by SSRC management.

Response

The SSRC concurs with this recommendation; although the SSRC stores all authorization requests within its current help desk application, we were unable to process the AGs request due to the complex nature of the systems database and limited availability of staff. Additionally, prior to this audit, the

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

SSRC had begun the process of establishing written procedures for access authorization and provided said documentation to the auditor general staff to show evidence of progress of this finding. The new process is in final review and is expected to be rolled out by the end of the calendar year.

Sincerely,

Tony K. Powell,
Executive Director

TP/mf

cc: Margaret Foltz, SSRC Information Technology Manager
Gerry York, SSRC Senior Attorney
Walter Sachs, DMS Inspector General
Yolanda Lockett, DMS Audit Director
George Zimmerman, DMS Senior IT Auditor

A Certified Tier III Facility