REPORT NO. 2013-182
MAY 2013

NORTHWOOD SHARED RESOURCE CENTER

DATA CENTER OPERATIONS

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

EXECUTIVE DIRECTOR OF THE NORTHWOOD SHARED RESOURCE CENTER

Pursuant to Section 282.204, Florida Statutes, the Northwood Shared Resource Center (NSRC) 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 by DMS in any manner. Pursuant to Section 282.203(2), Florida Statutes, the head of NSRC is the Board of Trustees (Board), consisting of representatives from customer entities. The Executive Director is employed by the Board of Trustees and serves at the pleasure of the Board.

Board members and the customer entities represented and the Executive Director who served during November 2012 through February 2013 are listed below:

Board Member	Customer Entity Represented
Grant Sellars, Chair	Department of Highway Safety and Motor Vehicles
Denise Rodenbough (Alternate)	Department of Highway Safety and Motor Vehicles
David Taylor, Vice Chair to 12-17-12	Department of Children and Families
Dan Johnson (Alternate)	Department of Children and Families
Don Sherman from 1-14-13	Department of Children and Families
Fred Schuknecht, Treasurer	Member at Large
Oscar Gertsch (Alternate)	Member at Large
James Deadman	Department of Health
Sandy Barnes (Alternate)	Department of Health
John Boynton	Department of State
Vicki Bradford	Department of Environmental Protection
Warren Sponholtz (Alternate from 11-19-12)	Department of Environmental Protection
Ann Coffin	Department of Revenue
Scott Ward	Agency for Health Care Administration
Michael Magnuson (Alternate)	Agency for Health Care Administration

James Stewart, Interim Executive Director

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 Nancy M. Reeder, CPA, CISA, CFE, Audit Manager, by e-mail at nancyreeder@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.

NORTHWOOD SHARED RESOURCE CENTER

Data Center Operations

SUMMARY

Pursuant to Sections 282.203(1)(a) and 282.204(1), Florida Statutes, the Northwood Shared Resource Center (NSRC) was established as a primary data center to serve as an information-system utility for customer entities. Our information technology (IT) operational audit focused on evaluating selected IT controls relevant to NSRC data center operations. We also determined the status of corrective actions regarding selected audit findings included in our report No. 2011-082.

The results of our audit are summarized below:

GENERAL IT CONTROLS

Finding No. 1: NSRC did not have system management software installed on some of the midrange systems that it managed for customer entities. As a result, NSRC was not able to maintain a complete inventory of logical midrange systems managed by the data center.

Finding No. 2: NSRC did not back up the data on some midrange systems it managed. Additionally, the off-site backup tape storage facility used by NSRC was too close in proximity to the data center.

Finding No. 3: The *NSRC Continuity of Operations Plan Operational Procedures (COOP)* and the *Disaster Recovery Plan* for NSRC lacked required statutory elements and contained incomplete and outdated information. Additionally, contrary to State law, the *COOP* had not been submitted to the Division of Emergency Management for approval. Also, NSRC staff had not received periodic training on implementing the plans.

Finding No. 4: NSRC was unable to provide us with a system-generated log of systems software changes that had been applied to the midrange systems. In addition, NSRC did not have sufficient information to permit a comparison of the system-generated logs of mainframe changes to manually-prepared software change documentation.

Finding No. 5: Certain NSRC security controls related to user authentication, software patch management, and physical access needed improvement. One of these issues was communicated to NSRC management in connection with our report No. 2011-082.

Finding No. 6: As similarly noted in our report No. 2011-082, NSRC had not established written procedures for performance monitoring and capacity planning.

Finding No. 7: NSRC did not maintain access authorization documentation for some employees and authorization documentation for other employees did not explicitly list the access privileges that had been authorized by management.

Finding No. 8: One user account with domain administrator access privileges remained active; however, the user account was no longer being used by the NSRC. Additionally, NSRC staff could not, upon audit request, provide documentation of periodic reviews of the appropriateness of physical access privileges to sensitive facilities.

SERVICE-LEVEL AGREEMENTS

Finding No. 9: Three NSRC service-level agreements (SLAs) with customer entities lacked certain provisions required by State law.

BACKGROUND

Section 282.201(1), Florida Statutes, provides that, unless otherwise exempt by law, it is the intent of the Legislature that all agency data centers and computing facilities be consolidated into a primary data center by 2019. NSRC was established as one of the primary data centers to which State agencies are to migrate their computing resources.

NSRC 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. NSRC provides a variety of IT services to its customer entities, including equipment hosting and server management services. In addition, NSRC provides a variety of mainframe and midrange systems platform services including application hosting, operating system management, online transaction processing, and batch processing. The midrange environment at NSRC consists of logical Windows and Linux servers hosted by the data center. The customer entities consist of State agencies that contract with NSRC for the aforementioned IT services. NSRC operates on a cost-recovery basis whereby NSRC bills the customer entities for a portion of its operating costs associated with the specific services provided to each customer entity. Lists of NSRC customer entities and services offered by NSRC are included in this report as EXHIBITS A and B, respectively.

FINDINGS AND RECOMMENDATIONS

General IT Controls

Finding No. 1: Midrange Systems Inventory

To implement an effective security program, entities need to maintain a complete, accurate, and up-to-date inventory of their systems. System management software aids system administrators in maintaining a comprehensive inventory of logical (physical and virtual) servers and facilitates automated management of those servers.

NSRC did not have system management software installed on some of the midrange systems that it managed for customer entities. As a result, NSRC could not, upon audit request, provide a complete and accurate inventory of its logical midrange systems. Without a complete inventory of logical midrange systems hosted by NSRC, NSRC management could not demonstrate that they had accounted for all midrange systems managed by NSRC when providing us with documentation of controls implemented on the midrange systems. Additionally, the lack of system management software may have limited NSRC's ability to monitor and manage the midrange systems in a manner consistent with management's expectations, as further discussed in Finding No. 2.

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

Finding No. 2: Backup Controls

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. Prudent safeguards also include ensuring that the off-site location is sufficiently separated from the primary storage site so as not to be susceptible to the same hazards. Such actions maintain the entity's ability to restore data files that, if lost, may otherwise be impossible to recreate.

We reviewed backup documentation as of January 29, 2013, for a sample of 25 of 1,156 identified midrange systems managed by NSRC to determine if the systems had been appropriately backed up. Our review disclosed that 2 of the 25 systems included in our sample had not been backed up because NSRC staff were unaware that the systems existed within the custody of NSRC. The failure to appropriately back up system data may limit NSRC's ability to timely and completely recover lost information in the event of a loss of production files.

In addition, the off-site backup storage facility used by NSRC was less than six miles away from the NSRC data center. This close proximity increases the risk that the same hazards or natural disasters affecting the region could compromise both facilities simultaneously.

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

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

Continuity of operations 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. Section 252.365, Florida Statutes, provides requirements related to emergency coordination officers and disaster-preparedness planning. Section 252.365(3)(a), Florida Statutes, provides that disaster preparedness plans must outline a comprehensive and effective program to ensure continuity of essential State functions under all circumstances. Pursuant to Section 252.365(3)(c), Florida Statutes, the Division of Emergency Management (DEM) has released instructions on implementing disaster preparedness plans through its *Continuity of Operations (COOP) Implementation Guide*. Our audit disclosed that the *NSRC Continuity of Operations Plan Operational Procedures (COOP)* and the *Disaster Recovery Plan* for NSRC needed improvement. Specifically:

- Section 252.365(3), Florida Statutes, provides that disaster preparedness (COOP) plans will be approved by DEM. Contrary to State law, the *NSRC COOP* had not been submitted to DEM for approval. Additionally, as of December 10, 2012, portions of the *COOP* and *Disaster Recovery Plan* were still marked as draft.
- It is important that continuity of operations and disaster recovery plans be clearly documented and updated to reflect current operations. Contrary to Section 252.365(3)(b), Florida Statutes, the *COOP* and *Disaster Recovery Plan* did not identify the alternate processing facility, related infrastructure, or certain personnel who were essential to the execution of the plans. Additionally, the *COOP* and *Disaster Recovery Plan* had not been recently updated to reflect current information or adjustments needed as a result of testing the *Disaster Recovery Plan*. For example, former NSRC employees and retired systems were still referenced in the plans.
- Periodic continuity of operations and disaster recovery training helps staff to understand their roles and responsibilities. Contrary to Section 252.365(3)(b), Florida Statutes, NSRC did not include continuity of operations or disaster recovery training as a part of new hire or annual staff training.

Under these conditions, the risk is increased that the *COOP* and *Disaster Recovery Plan* may not include the necessary provisions or be executed in a timely and effective manner in the event of an interruption in operations.

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

Finding No. 4: Change Control

Effective change control procedures help to ensure that all changes are tracked, documented, and approved. NSRC was unable to provide us with a system-generated log of systems software changes that had been applied to the midrange systems. In addition, although NSRC retained system-generated logs of mainframe changes, neither the logs nor NSRC manually-prepared change documentation included sufficient information for NSRC management to compare the change documentation with the logs for the purpose of ensuring, on a post-implementation basis, that all software changes were documented and authorized. Without a complete, system-generated log of systems software changes, the risk is increased that erroneous or unauthorized software changes, should they be moved into the production environment, will not be timely detected by management.

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

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 NSRC security controls related to user authentication, software patch management, and physical access that needed improvement. One of the issues was communicated to NSRC management in connection with our report No. 2011-082. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising NSRC customer entity data and IT resources. However, we have notified appropriate NSRC management of the specific issues. Without adequate security controls related to user authentication, software patch management, and physical access, the risk is increased that the confidentiality, integrity, and availability of data and IT resources may be compromised.

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

Finding No. 6: Performance Monitoring and Capacity Planning Procedures

Each IT function needs complete, well-documented policies and procedures to describe the scope of the function and its activities. Sound policies and procedures provide benchmarks against which compliance can be measured and contribute to an effective control environment.

Our audit disclosed that NSRC had not established written procedures for performance monitoring and capacity planning for the midrange systems managed by the NSRC. Although NSRC monitored performance and conducted capacity planning for the midrange systems, absent written procedures the risk is increased that performance monitoring and capacity planning may not be conducted consistently and in a manner pursuant to management's expectations. In addition, performance and capacity problems, should they occur, may not be timely detected and corrected. A similar finding was disclosed in our report No. 2011-082.

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

Finding No. 7: 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 NSRC to determine if access granted was adequately documented and authorized. NSRC did not maintain access authorization documentation for the user access privileges for many of the NSRC employees included in our tests or samples as described below:

- Six of the seven employees with update access privileges to NSRC network resources as of December 3, 2012. NSRC staff provided access authorization documentation for one employee; however, the documentation did not explicitly authorize update access to NSRC network resources.
- The 6 employees included in our sample selected from 47 employees with various levels of access privileges to NSRC mainframes as of December 4, 2012.
- The three employees with administrative access privileges to the NSRC virtual private networking system as of December 3, 2012.
- Six of the seven employees with administrative access privileges to the NSRC intrusion prevention system as of December 10, 2012. NSRC staff provided access authorization documentation for one employee; however, the documentation did not explicitly authorize administrative access to the NSRC intrusion prevention system.
- Eight of the nine employees with administrative access privileges to the NSRC network domain as of December 17, 2012.

The access privileges granted, however, did not appear to be excessive based on the job duties of the NSRC employees. Nevertheless, these conditions limited management's ability to ensure that employee access privileges granted to employees do not exceed what is necessary for the accomplishment of assigned job responsibilities.

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

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

Effective access controls include measures that limit user access privileges to only what is necessary in the performance of assigned job responsibilities. Unnecessary accounts should be deactivated or otherwise secured. Appropriately restricted access privileges help protect data and IT resources from unauthorized disclosure, modification, and destruction.

We reviewed the ten accounts with administrative access privileges to the NSRC network domain as of December 17, 2012. Our review disclosed that one system account existed with no identifiable owner and was no longer being used by NSRC. Accounts with unnecessary access privileges increase the risk of access privileges being misused. The existence of the unused account with elevated access privileges indicates a need for an improved NSRC

[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.

review of domain administrator accounts. In response to audit inquiry, NSRC staff deactivated the account as of February 19, 2013.

Effective access controls also include provisions for the periodic review of the appropriateness of physical access privileges to sensitive facilities. Additionally, the NSRC Physical Security Guide, Section XII, states that the Physical Security Section of NSRC will perform physical reviews of the Technology Center. NSRC staff could not, upon audit request, provide documentation of periodic reviews of the appropriateness of physical access privileges to sensitive facilities. Without periodic access reviews, the risk is increased that inappropriate physical access may not be timely detected or corrected.

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

Service-Level Agreements

Finding No. 9: Service-Level Agreements

Section 282.203(1)(i), Florida Statutes, provides that each primary data center shall enter into a service-level agreement (SLA) with each customer entity to provide services as defined and approved by the Board. Section 282.203(1)(i)1., Florida Statutes, provides requirements for primary data center SLAs.

As a part of our audit, we reviewed three recently executed NSRC SLAs to determine if they met the requirements of Section 282.203(1)(i)1., Florida Statutes. Our review disclosed that the SLAs did not include some required provisions. Specifically:

- Two SLAs did not specifically identify the legal authority under which the service-level agreements were negotiated and entered into by the parties, contrary to Section 282.203(1)(i)1.b., Florida Statutes.
- Two SLAs did not specify the conditions for contract renewal, contrary to Section 282.203(1)(i)1.c., Florida Statutes.

The lack of the above-described SLA provisions may limit the ability of NSRC and its customer entities to ensure that contractual expectations are met.

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

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, NSRC had taken corrective actions for findings included in our report No. 2011-082 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 November 2012 through February 2013 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 NSRC. An additional objective was to determine the extent to which NSRC corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2011-082. The scope of our audit focused on selected general IT controls relevant to NSRC data center operations, including selected general IT controls over security and operations.

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 NSRC staff.
- Obtained an understanding of key NSRC IT controls and toured the NSRC data center. We observed and evaluated the effectiveness of key processes and procedures related to NSRC.
- Obtained an understanding of the statutory requirements and organizational structure of NSRC data center operations and evaluated the effectiveness of NSRC compliance with selected requirements. Specifically, we evaluated the adequacy of three recently executed SLAs established between NSRC and its customer entities to determine whether selected provisions required in Section 282.203(1)(i)1., Florida Statutes, were included.

- Obtained an understanding of the services offered by NSRC and the directives, policies, procedures, and processes governing NSRC operations.
- Evaluated the effectiveness of controls surrounding processes used by NSRC for service request processing, tracking and reporting service-level metrics, performance monitoring, and capacity planning.
- Evaluated the effectiveness of selected disaster recovery and continuity of operations planning controls, including backup procedures. Specifically, we reviewed the *NSRC COOP* and *Disaster Recovery Plan* for NSRC as of December 10, 2012, to determine if they contained selected required statutory provisions. We additionally reviewed a sample of 25 of 610 off-site network tapes as of January 24, 2012, to determine if NSRC inventory records were accurate and whether all tapes could be located. We also reviewed backup documentation as of January 29, 2013, for a sample of 25 of 1,156 identified midrange systems managed by NSRC to determine if the systems had been appropriately backed up.
- Evaluated the effectiveness of selected controls over NSRC IT resource inventory to determine the effectiveness of inventory-tracking procedures. Specifically, we reviewed a sample of 25 of 1,607 items of NSRC IT resource inventory from its inventory records as of January 3, 2013, to determine if the equipment could be physically located. We additionally reviewed a sample of 25 items of equipment that were physically located on the floor of the data center on February 14, 2013, to determine if the equipment was properly recorded in the inventory records.
- Evaluated the effectiveness of selected controls over the modifications of systems software, including software patch management procedures. Specifically, we reviewed a sample of 25 of 796 changes entered into the ServiceCenter system between July 1, 2012, and January 3, 2013. We additionally reviewed patching documentation as of January 28, 2013, for a sample of 25 of 1,156 identified midrange systems managed by NSRC to determine if the systems had been appropriately patched.
- Obtained an understanding of the IT infrastructure and architecture of NSRC.
- Tested the effectiveness of password settings and remote administration controls to evaluate their effectiveness in adequately protecting IT resources.
- Evaluated the effectiveness of antivirus and network controls in place to protect IT resources.
- Evaluated the effectiveness of NSRC physical security and environmental safeguards in place to protect IT resources. Specifically, we evaluated the appropriateness of access privileges for a sample of 14 of 133 NSRC employees with physical access to the data center floor as of November 15, 2012.
- Evaluated the appropriateness of access to various systems managed by NSRC. Specifically, we reviewed all 10 users with update access to NSRC network resources as of December 3, 2012; a sample of 7 of 62 users with various levels of access to NSRC mainframes as of December 4, 2012; all 3 users with administrative access to the NSRC virtual private networking system as of December 3, 2012; all 7 users with administrative access to the NSRC intrusion prevention system as of December 10, 2012; and all 10 users with administrative access to the NSRC domain as of December 17, 2012.
- Evaluated the effectiveness of procedures for performing background screenings and authorizing employee access privileges to IT resources. Specifically, we reviewed all 7 NSRC employees with update access to NSRC network resources as of December 3, 2012; a sample of 6 of 47 NSRC employees with various levels of access to NSRC mainframes as of December 4, 2012; all 3 NSRC employees with administrative access to the NSRC virtual private networking system as of December 3, 2012; all 7 NSRC employees with administrative access to the NSRC intrusion prevention system as of December 10, 2012; and all 9 NSRC employees with administrative access to the NSRC domain as of December 17, 2012.
- 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 response letter dated May 21, 2013, the Interim Executive Director provided responses to our preliminary and tentative findings. The response is included as EXHIBIT C.

EXHIBIT A
LIST OF NSRC CUSTOMER ENTITIES
AS OF FEBRUARY 2013

Agency for Health Care Administration
Agency for Persons with Disabilities
Department of Business and Professional Regulation
Department of Children and Families
Department of Citrus
Department of Environmental Protection
Department of Health
Department of Highway Safety and Motor Vehicles
Department of Juvenile Justice
Department of Revenue
Department of State

EXHIBIT B
LIST OF SERVICES OFFERED BY NSRC
AS OF FEBRUARY 2013

Service Category	Service Type Detail
Data Center Management	Data Center Hosting
	Print Services
	Network-to-Network Interface
	Other Network Services
Mainframe Services	IBM Processing
	Application Hosting
	Operating System Management
	Online Transaction Processing
	Batch Processing
	Mainframe Managed Tape Storage
	Mainframe Managed Services
Midrange Systems Platform Management	Midrange Systems Application Hosting
	Operating System Management
	Online Transaction Processing
	Batch Processing
Database Systems Platform Management	IBM Mainframe Database Administration Support
	Midrange Database Administration Support
Storage Management	Managed Disk Storage
	Managed Tape Storage
	Backup Services
Disaster Recovery	Disaster Recovery Service
Professional Services	IT Consulting
	Research
	Strategic Planning
	Architectural Design, Implementation
	Migration Assistance
	Security Response
	Issue Management
	Systems Monitoring
	Problem Diagnostics
	Troubleshooting
	Security Management
	Capacity Planning/Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT C
MANAGEMENT'S RESPONSE

State of Florida
Northwood Shared Resource Center

Rick Scott
Governor

James Stewart, *Interim,*
Executive Director

May 21, 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, *Information Technology Operational Audit of the Northwood Shared Resource Center Data Center Operations*. Our response corresponds with the order of your preliminary and tentative findings and recommendations.

Finding No. 1: Midrange Systems Inventory

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

Recommendation

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

Response

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

Finding No. 2: Backup Controls

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

Recommendation

1. NSRC should ensure that midrange system backups are performed in a timely manner.

2. NSRC should also utilize an off-site backup storage facility that is more geographically removed from the NSRC data center.

Response

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

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

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

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

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

Recommendation

1. To comply with State law, NSRC should update and complete its COOP and Disaster Recovery Plan to accurately describe the current NSRC environment and submit the COOP to DEM for approval.

2. NSRC should also schedule and provide its staff with periodic continuity of operations and disaster recovery training.

Response

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

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

Finding No. 4: Change Control

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

Recommendation

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

Response

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

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 5: Other Security Controls

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

Recommendation

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

Response

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

Finding No. 6: Performance Monitoring and Capacity Planning Procedures

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

Recommendation

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

Response

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

Finding No. 7: Access Authorizations

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

Recommendation

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

Response

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

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

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

EXHIBIT C (CONTINUED)
MANAGEMENT'S RESPONSE

Recommendation

1. NSRC should enhance its review of domain administrator access privileges and deactivate any unnecessary or unused access detected.

2. NSRC should also conduct and document the required periodic reviews of the appropriateness of physical access privileges to sensitive facilities.

Response

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

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

Finding No. 9: Service-Level Agreements

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

Recommendation

1. For all future SLAs, NSRC should ensure that all required provisions are included.

2. In addition, NSRC should modify the three SLAs described above to include all provisions required by State law.

Response

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

Sincerely,

James Stewart
Interim Executive Director