REPORT NO. 2013-012
SEPTEMBER 2012

# FLORIDA STATE UNIVERSITY

## NORTHWEST REGIONAL DATA CENTER

## DATA CENTER OPERATIONS

## Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

## EXECUTIVE DIRECTOR OF THE NORTHWEST REGIONAL DATA CENTER

The Florida State University (University) is the administrative host institution and fiscal agent for the Northwest Regional Data Center (NWRDC). The NWRDC Charter establishes a Policy Board (Board) as the governing body for NWRDC. The Board's primary function is to establish and promulgate policies for NWRDC. The Executive Director, who is selected by the Board, is responsible for the overall administration of NWRDC.

Board members and the customer entities represented and the Executive Director who served during the period September 2011 through March 2012 are listed below:

| Board Member | Customer Entity Represented |
|---|---|
| Mehran Basiratmand, Chair | Florida Atlantic University |
| Michael Barrett, Vice Chair | Florida State University |
| Stephen Bowen, K-12 Representative | Florida State University Schools |
| Michael Dieckmann | University of West Florida |
| Levis Hughes through 2-23-12 | Department of Education |
| Ted Duncan from 2-24-12 | Department of Education |
| George Ellis | University of South Florida |
| Keith (Kit) Goodner | Department of Education |
| Michael A. James | Florida A&M University |
| Gene Kovacs | State University System of Florida Board of Governors |
| Randy McCausland, Technical Committee Chair | Florida State University |
| Tony Powell | Department of Revenue |
| Peter M. Taylor, Management Committee Member | Florida International University |

Tim Brown, Executive Director

The audit team leader was Bill Allbritton, CISA, and the audit was supervised by Heidi Burns, CPA, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CITP, 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.

# FLORIDA STATE UNIVERSITY
# NORTHWEST REGIONAL DATA CENTER

Data Center Operations

## SUMMARY

**Pursuant to Section 1004.649(1), Florida Statutes, the Northwest Regional Data Center (NWRDC) at the Florida State University (University) was designated as a primary data center for the purpose of serving its State agency customers. Our audit focused on evaluating the effectiveness of selected information technology (IT) controls relevant to NWRDC data center operations.**

**The results of our audit are summarized below:**

**NWRDC GOVERNANCE**

**Finding No. 1: It is not clear statutorily whether the State laws and administrative rules that govern the State primary data centers are applicable to NWRDC.**

**SERVICE-LEVEL AGREEMENTS**

**Finding No. 2: NWRDC did not have written service-level agreements (SLAs) in place with 34 of its educational entity customers.**

**GENERAL IT CONTROLS**

**Finding No. 3: Some aspects of NWRDC's security management needed improvement.**

**Finding No. 4: NWRDC lacked written procedures addressing the detailed requirements for documenting and tracking hardware and systems software changes, emergency changes, and the periodic review of changes. In addition, NWRDC did not have a complete, system-generated record of all hardware and systems software changes. NWRDC also lacked documentation of the authorization, testing, approval, and implementation of mainframe and internal systems software changes for 12 changes included in our sample.**

**Finding No. 5: Certain NWRDC security controls related to user authentication, disclosure of sensitive security information, and monitoring needed improvement.**

**Finding No. 6: NWRDC's *Disaster Recovery Plan* did not address recovery or testing procedures for its internal systems.**

**Finding No. 7: Although management had informally designated all NWRDC positions as special trust positions, level 2 background screenings that included national criminal record checks and fingerprinting had not been completed for some NWRDC employees.**

**Finding No. 8: NWRDC had not established written procedures for mainframe or open systems performance monitoring.**

**COST-MEASUREMENT AND DISTRIBUTION METHODOLOGY**

**Finding No. 9: Contrary to Federal requirements, NWRDC was unable to demonstrate, for many data center services, that the established billing rates and charges were appropriate and equitably applied to its customers based on the costs and utilization of data center services. Additionally, NWRDC reported a working capital reserve balance that exceeded what is considered reasonable for normal operating expenses pursuant to Federal requirements.**

## BACKGROUND

Section 282.201(1), Florida Statutes, as amended by Section 1 of Chapter 2012-142, Laws of Florida, 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. Section 1004.649(1), Florida Statutes, designated NWRDC as a primary data center for the purpose of serving its State agency customers.

NWRDC is an auxiliary operation of the University and is headed by a Policy Board (Board), consisting of representatives from customer entities. The Board selects an Executive Director to be responsible for the daily operation of the data center. In its capacity as the administrative host institution and fiscal agent, the University is the contracting authority for NWRDC and provides legal support and executive oversight. All NWRDC positions are filled with employees of the University and follow University policies for payroll, leave, and other personnel actions.

NWRDC provides a variety of IT services to its customer entities, including mainframe processing and storage, server hosting and managed data storage (referred to as open systems services), and fiber usage and maintenance. The customer entities consist of State agencies, universities, colleges, school districts, city and county governments, and various consortia and non-profit groups that contract with NWRDC for the aforementioned IT services. NWRDC operates on a cost-recovery basis whereby NWRDC bills the customer entities for a portion of its operating costs associated with the specific services provided to each customer entity. Lists of NWRDC customer entities and services offered by NWRDC are included in this report as EXHIBITS A and B, respectively.

## FINDINGS AND RECOMMENDATIONS

### NWRDC Governance

#### Finding No. 1: State Laws and Rules Governing the State Data Center System

Section 282.201, Florida Statutes, establishes a State data center system including all primary data centers, other nonprimary data centers, and computing facilities. Section 282.203, Florida Statutes, prescribes the required duties of primary data centers. Additionally, pursuant to Section 282.201(2)(e), Florida Statutes, the Agency for Enterprise Information Technology (AEIT)[1] shall develop and establish rules relating to the operation of the State data center system. The rules must address, among other things, identifying standards for hardware and operations systems software and other operational software, including security and network infrastructure, for the primary data centers. At the time of our audit, AEIT had drafted administrative rules to govern the State data center system; however, the rules had not yet been adopted. The draft rules addressed such data center matters as financial reporting, cost recovery and billing, service-level agreements, and enterprise standards.

Our audit disclosed that Section 1004.649(1), Florida Statutes, could be clarified with regard to the extent to which NWRDC is subject to State laws and AEIT rules governing the State data center system. As previously discussed, Section 1004.649(1), Florida Statutes, designates NWRDC as a primary data center for the purpose of serving its State

[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.

agency customers. In addition, Section 1004.649(1), Florida Statutes, provides that NWRDC shall comply with certain specified requirements, including operating under a governance structure that represents its customers proportionally, maintaining an appropriate cost-allocation methodology, and entering into service-level agreements (SLAs) with each State agency customer. However, NWRDC is not explicitly exempted in law from the requirements as set forth in Section 282.203(1), Florida Statutes, for the primary data centers in the State data center system. For example, Section 282.203(1)(c), Florida Statutes, provides that each primary data center shall comply with rules adopted by AEIT, pursuant to Section 282.201(6), Florida Statutes.

The State University System was, however, specifically exempted from the provisions of Chapter 282, Florida Statutes, in a Governance Agreement, dated March 24, 2010, between the Board of Governors of the State University System and the Presiding Officers of the Florida House of Representatives and the Florida Senate. Consequently, it is not clear statutorily whether the provisions of Chapter 282, Florida Statutes, governing the primary data centers that are not also listed in Section 1004.649(1), Florida Statutes, are applicable to NWRDC. It is also not clear whether NWRDC should comply with AEIT rules. Clarifying the governance structure and expectations for NWRDC with regard to its responsibilities as a primary data center would enhance its accountability in serving State agency customers in connection with the consolidation of State agency data centers.

**Recommendation: The Legislature should consider amending Section 1004.649, Florida Statutes, to clarify the governance structure and expectations for NWRDC as a primary data center, including whether NWRDC is subject to State primary data center system requirements as set forth in Section 282.203(1), Florida Statutes.**

## Service-Level Agreements

### Finding No. 2: Service-Level Agreements

Effective IT practices dictate that when one entity (customer) depends upon another (service provider) for significant technology resources, a formal service-level agreement (SLA) that defines the responsibilities of both parties should be negotiated and in place. Responsibilities detailed may include provision of services, system availability, reliability and performance, capacity requirements, user support, security administration, continuity planning, cost, billing and payment procedures, monitoring, and dispute resolution procedures.

Section 1004.649(1)(c), Florida Statutes, provides that NWRDC shall enter into an SLA with each State agency customer to provide services as defined and approved by the Board. Our audit disclosed that NWRDC had executed SLAs with its State agency customers with the exception of four State agencies that received only minimal services from NWRDC, were not billed by NWRDC on a monthly basis, and paid only a nominal fee to NWRDC. Additionally, we tested the NWRDC SLAs with the two State agency customers that were part of the State's consolidation effort, the Department of Education (DOE) and the Department of Revenue (DOR), and determined that the SLAs included the six provisions required in the aforementioned State law.

However, NWRDC has traditionally operated under informal agreements with many of its legacy educational customer entities and did not have written SLAs in place with 34 of its educational customer entities. In response to audit inquiry, NWRDC management indicated that they are currently working with these customer entities to execute signed SLAs. The absence of written agreements between NWRDC and these customer entities for the provision of IT services increases the risk that the parties will not perform their responsibilities at a sufficient level to meet performance expectations.

**Recommendation: NWRDC should execute written SLAs with all of its customer entities that define each party's responsibilities, expectations, and dispute resolution procedures.**

## General IT Controls

### Finding No. 3: Security Management

Effective security management includes establishing an entitywide information security program as the foundation of an entity's security control structure and as a reflection of senior management's commitment to addressing security risks. The program establishes a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of the procedures.

Our audit disclosed that some aspects of NWRDC's security management needed improvement. Specifically:

- Although the NWRDC's draft security policy requires the maintenance of an information security program that establishes guidelines for the protection of NWRDC and client information resources and identifies roles and responsibilities at all levels, NWRDC had not developed such a program. The absence of a well-designed information security program may result in inadequate or improperly implemented controls, increasing the risk that sensitive or critical IT resources may not be sufficiently protected.
- NWRDC did not have written security policies and procedures for establishing, issuing, suspending, modifying, and closing NWRDC employee accounts or for the review of employee accounts and access privileges. Without written security policies and procedures, the risk is increased that security controls may not be followed consistently and in a manner pursuant to management's expectations.

**Recommendation: NWRDC should develop and maintain an information security program. The program should include appropriate written security policies and procedures to ensure the confidentiality, integrity, and availability of the data and IT resources in its custody and include provisions for the management of employee accounts and access privileges.**

### Finding No. 4: 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.

NWRDC change management policy included guidance as to when certain hardware and systems software changes can be made and when weekly change management meetings are to be scheduled. However, NWRDC lacked written procedures addressing the detailed requirements for documenting and tracking the authorization, testing, and implementation of hardware and systems software changes. Additionally, NWRDC did not have written emergency change procedures or procedures for a periodic review process to prevent or detect unauthorized changes. The lack of written procedures increases the risk that hardware and systems software changes will not be authorized, tested, or implemented in a consistent manner pursuant to management's expectations.

Upon audit request, NWRDC was unable to provide a system-generated log of all hardware and systems software changes that had been applied to NWRDC's internal systems (the computing platforms used in the day-to-day operation and administration of the data center in support of servicing its customer base), open systems (server platforms supporting customer entity services), or the mainframe. Alternatively, NWRDC provided us a listing of hardware and software change records that had been manually entered into a spreadsheet used for change

management activities. However, NWRDC did not have a mechanism in place to verify that all changes made to a platform were actually entered into the spreadsheet. Notwithstanding the limitations of manually entered change records, we reviewed a sample of 12 software changes from 42 successfully completed software and hardware changes to the mainframe and internal systems recorded on the spreadsheet from January 1, 2011, through December 20, 2011. Our review disclosed that, for all 12 changes included in our sample, NWRDC staff were unable to provide documentation substantiating that the changes had been appropriately authorized, tested, approved for production, and implemented.

Without a complete, system-generated record of systems software and hardware changes and adequate documentation tracking the change control process, the risk is increased that erroneous or unauthorized changes could be moved into the production environment without timely detection.

**Recommendation: NWRDC should supplement its change management policy with written procedures addressing the detailed requirements for documenting and tracking systems software and hardware changes, emergency changes, and the periodic review of changes. Additionally, NWRDC should implement system-generated logs to record, track, and report all system software changes that are made to each platform. Furthermore, NWRDC should maintain documentation that demonstrates the appropriate authorization, testing, approval, and implementation of systems software changes.**

### 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 NWRDC security controls related to user authentication, disclosure of sensitive security information, and monitoring that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising NWRDC customer entity data and IT resources. However, we have notified appropriate NWRDC management of the specific issues. Without adequate security controls related to user authentication, disclosure of sensitive information, and monitoring, the risk is increased that the confidentiality, integrity, and availability of data and IT resources may be compromised.

**Recommendation: NWRDC should improve security controls related to user authentication, disclosure of sensitive information, and monitoring to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.**

### Finding No. 6: Disaster Recovery Planning

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 IT service.

Although disaster recovery planning was the responsibility of each customer entity receiving open systems services, NWRDC maintained a detailed *Disaster Recovery Plan* for the recovery and continuity of operations for its mainframe customer entities. The *Disaster Recovery Plan*, however, did not address recovery or testing procedures for NWRDC's internal systems.

The lack of a comprehensive disaster recovery plan may jeopardize NWRDC efforts to timely, efficiently, and effectively resume IT operations with minimal loss and processing disruption in the event of an actual disaster.

**Recommendation: NWRDC should incorporate its internal systems into its *Disaster Recovery Plan*.**

### Finding No. 7: Background Screenings

Effective security controls include the performance of security background screenings for new employees and the periodic re-performance of screenings for existing employees who are in sensitive or special trust positions. Such positions typically include IT employees with elevated access privileges or responsibilities for the custody of sensitive IT resources. Because of the sensitive nature of customer entity data and IT resources housed at NWRDC, management informally designated all NWRDC positions as special trust positions. In August 2011, a formal policy was adopted by the Board to require that all newly hired NWRDC employees be subject to level 2 background screenings, pursuant to Section 435.04(1)(a), Florida Statutes, including fingerprinting for Statewide criminal history records checks through the Department of Law Enforcement and national criminal records checks through the Federal Bureau of Investigation. In addition, the policy provided for current employees having direct, logical access to any type of data for which security background checks are required to be subject to level 2 background screenings. In accordance with the policy, some NWRDC employees had been subjected to level 2 background screenings. However, our review of background screening records for a sample of 13 of 35 NWRDC employees disclosed that 7 employees had been subjected to level 1 (Statewide) background screenings but not level 2 (national) background screenings.

The absence of a national security background check, including fingerprinting, increases the risk that a person with a criminal record may be employed in a position of special trust or responsibility and gain access to confidential or sensitive customer entity data and IT resources.

**Recommendation: NWRDC should complete Statewide and national background screenings, including fingerprinting, for all of its employees. Additionally, NWRDC should update its policy to formally designate all NWRDC positions as special trust positions.**

### Finding No. 8: Performance Monitoring

Ongoing 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 NWRDC had not established written procedures for mainframe or open systems performance monitoring. Although NWRDC monitored performance, without written procedures the risk is increased that mainframe and open systems performance may not be monitored consistently and in a manner pursuant to management's expectations and that performance problems, should they occur, may not be timely detected and corrected.

**Recommendation: NWRDC should establish written procedures for mainframe and open systems performance monitoring.**

**Cost-Measurement and Distribution Methodology**

## Finding No. 9: Compliance with Federal Guidelines

While University Policy OP-D-1, *Auxiliary Operations*, requires that a rate methodology be prepared to show a detailed and auditable structure of the auxiliary operation's billing rate, the Policy further states that the auxiliary's rate schedule may reflect separate billing rates for different users of goods and services and that external users may be billed a higher rate than internal users for the same goods or services. In addition, the Policy allows for the billing rates charged to external users to generate revenues in excess of costs. As defined components of the State, the University and State agency customers of NWRDC, such as DOE and DOR, are part of the State of Florida Financial Reporting Entity and, therefore, funds passing between the State agencies and NWRDC are considered funds passed within the same reporting entity for services rendered. State agencies' use of Federal awards for payments to NWRDC for data processing services must comply with applicable Federal guidelines. Our review of NWRDC's cost measurement and distribution methodology disclosed deficiencies that would prevent State agencies from demonstrating that payments made to NWRDC comply with Office of Management and Budget (OMB) Circular A-87. Specifically:

- OMB Circular A-87 provides that billing rates used to charge Federal awards shall be based on the estimated costs of providing the services, including an estimate of the allocable central service costs. OMB Circular A-87, Attachment C, Section A.1., provides that all costs and other data used to distribute the 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. OMB Circular A-133 Compliance Supplement states that all users of services are to be billed in a consistent manner, i.e., all users (including users outside the governmental unit) are to be charged the same rate for the same service. The 2011-12 fiscal year NWRDC billing rates charged to customer entities were calculated based on the estimated cost and utilization of the various NWRDC services. Our test of 22 non-mainframe services from the NWRDC Service Catalog disclosed that NWRDC could not, upon audit request, provide documentation to fully support how billing rates were determined for 17 of the services. In addition, for 4 of the remaining 5 services, the documented rates included depreciation charges that were not supported by appropriate property or depreciation records. We further noted that, for mainframe services, NWRDC assigned fixed rates based on estimated costs and utilization to all but two customer entities. These two customer entities were assigned a fixed rate, one at a new customer rate and the other at a negotiated rate. Under these conditions, NWRDC could not demonstrate that the established rates and charges were appropriate and equitably applied to its customer entities based on the costs and utilization of data center services.
- OMB Circular A-87 states that a comparison of the total revenues generated by each billed service to the actual allowable costs, including documented depreciation expense, of the service will be made at least annually, and an adjustment will be made for the difference between the revenues and the allowable costs. A reasonable level of working capital reserve, in addition to the full recovery of costs, is allowable. A working capital reserve, as part of retained earnings, of up to 60 days cash expenses for normal operating purposes is considered reasonable. NWRDC submitted a schedule comparing total revenues generated by NWRDC services to the allowable costs of these services for the fiscal year ended June 30, 2011, to the Department of Financial Services (DFS) for inclusion in the State's 2013 Statewide Cost Allocation Plan (SWCAP). This schedule disclosed total revenues of $8,768,000 and OMB Circular A-87 allowable expenditures of $6,934,000, resulting in a fund balance for the fiscal year of $1,834,000. Based on the expenditures reported on the SWCAP schedule, NWRDC's allowable working capital reserve of up to 60 days cash expenses for normal operating purposes under OMB Circular A-87 should not have exceeded $1,156,000. In response to audit inquiry, NWRDC management indicated that they failed to include depreciation expense in the SWCAP schedule and, if depreciation expense was considered, the balance would not be excessive. In these circumstances, the SWCAP schedule does not support the reasonableness of the rates charged to Federal awards by State agencies served by NWRDC.

Although actual costs examined within our audit period predate the July 1, 2011, effective date, Section 1004.649, Florida Statutes, provides that, for the purpose of serving its State agency customer entities, NWRDC shall maintain an appropriate cost-allocation methodology that accurately bills State agency customer entities based solely on the actual direct and indirect costs of the services provided to State agency customer entities and prohibits the subsidization of non-State agency customer entities costs by State agency customer entities. The revenue and cost comparison, along with any associated adjustment, for the fiscal year ended June 30, 2012, cannot be determined until actual costs are calculated after June 30, 2012.

**Recommendation: To demonstrate compliance with State law and Federal requirements and the appropriateness and equitability of NWRDC billings, NWRDC should maintain supporting documentation for the methodology used to determine the estimated utilization of services used, along with estimated costs, to establish billing rates actually charged to customer entities. In addition, once actual costs for the fiscal year ended June 30, 2012, are known and NWRDC prepares the comparison between total revenues and allowable costs, NWRDC should make the appropriate adjustments to customer billings and maintain a reasonable level of working capital reserve to operate from one billing cycle to the next pursuant to OMB Circular A-87. Also, NWRDC, in consultation with DFS, should make adjustments to the State's 2013 SWCAP to correct the reported expenditures for allowable depreciation for the fiscal year ended June 30, 2011.**

## 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 September 2011 through April 2012 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 NWRDC.

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

In conducting our audit, we:

- Interviewed NWRDC personnel.
- Obtained an understanding of the services offered by NWRDC and the directives, policies and procedures, and key processes governing NWRDC's operations.
- Obtained an understanding of key NWRDC IT controls and toured the NWRDC data center. We observed and evaluated the effectiveness of key processes and procedures related to NWRDC.

- Obtained an understanding of the IT infrastructure and architecture of NWRDC.
- Observed and evaluated selected controls over NWRDC IT resource inventory to determine the effectiveness of inventory tracking procedures. Specifically, we sampled 20 of 960 items of NWRDC IT resource inventory listed on inventory records as of October 5, 2011, and October 10, 2011, to determine if the equipment could be physically located. We additionally reviewed a sample of 6 items of equipment that were physically located on the floor of the data center on November 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 NWRDC IT resources. Specifically, we sampled 13 of 35 NWRDC employees with potential access to sensitive IT resources to determine whether they had undergone required background screenings.
- Obtained an understanding of the statutory requirements and organizational structure of NWRDC data center operations and evaluated the effectiveness of NWRDC compliance with selected requirements.
- Observed and evaluated logical access control mechanisms utilized by NWRDC including password controls, use of remote administration software tools, assignment of access privileges, and network devices used to protect IT resources. Specifically, we reviewed six accounts with administrative access privileges on the mainframe as of January 11, 2012; seven accounts with administrative access privileges on the NWRDC network infrastructure as of November 28, 2011; and the three user accounts with domain administrator access privileges as of January 11, 2012.
- Observed and evaluated the adequacy of NWRDC physical security and environmental safeguards in place to protect IT resources.
- Observed and evaluated the adequacy of selected disaster recovery and continuity of operations planning controls, including backup procedures. We additionally reviewed the off-site storage of mainframe backup tapes for 6 of 59 tapes stored as of November 7, 2011, and 6 of 58 tapes stored as of November 14, 2011, to determine if NWRDC inventory records were accurate and whether specific tapes could be located.
- Observed and evaluated the adequacy of selected controls over the modifications of systems software. Specifically, we reviewed on a sample basis 12 software changes out of 42 successfully completed software and hardware changes entered into the NWRDC change tracking spreadsheet from January 1, 2011, through December 20, 2011.
- Observed and evaluated controls surrounding processes used by NWRDC for performance and capacity monitoring.
- Observed and evaluated established controls for executing SLAs between NWRDC and its customer entities. Additionally, we tested two State agency customer entity SLAs to determine if the SLAs included the six provisions required in Section 1004.649(1)(c), Florida Statutes.
- Observed and evaluated the effectiveness of the cost-measurement, cost-allocation, and cost-adjustment methods used by NWRDC. Specifically, we tested NWRDC approved rates for 1 mainframe service and 22 non-mainframe services for the 2011-12 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. In addition, we evaluated the process used to adjust data center charges to actual costs as of June 30, 2011.
- Observed and evaluated the controls surrounding the billing process utilized by NWRDC. Specifically, we reviewed on a sample basis 25 of 1,142 checks selected from a check log for the period October 2010 through September 2011 and 25 of 2,799 invoices prepared for services rendered by NWRDC for the period July 2010 through September 2011 to determine if NWRDC customer entities were properly billed, payments monitored, and collections made for services rendered by NWRDC.
- 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 September 4, 2012, the NWRDC 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 NWRDC CUSTOMER ENTITIES
## AS OF JANUARY 22, 2012

| | |
|---|---|
| Agency for Enterprise Information Technology | Florida Surplus Lines Service Office |
| Agency for Healthcare Administration | Franklin County School District |
| Agency for Persons with Disabilities | Gadsden County School District |
| Alachua School District | Gulf County School District |
| Auditor General | Hillsborough County School District |
| Bay County School District | Holmes County School District |
| Board of Governors | Jackson County School District |
| Calhoun County School District | Jefferson County School District |
| Chipola College | Learnsomething, Inc. |
| City of Jacksonville | Lee County School District |
| College Center for Library Automation | Leon County Research and Development Authority |
| Department of Business and Professional Regulation | Leon County School District |
| Department of Children and Family Services | Liberty County School District |
| Department of Economic Opportunity | Madison County School District |
| Department of Education | Miami-Dade County School District |
| Department of Financial Services | Nassau County School District |
| Department of Health | New College of Florida |
| Department of Highway Safety and Motor Vehicles | Orange County School District |
| Department of Juvenile Justice | Palm Beach Clerk and Comptroller |
| Department of Revenue | Palm Beach County Government |
| Department of Transportation | Palm Beach County School District |
| Escambia County School District | Panhandle Area Educational Consortium |
| Executive Office of the Governor | Polk County School District |
| Florida A & M Developmental Research School | Santa Rosa County School District |
| Florida A & M University | Southwood Shared Resource Center |
| Florida Association of Court Clerks | St. Johns County School District |
| Florida Atlantic University | Suwannee County School District |
| Florida Atlantic University School | Tallahassee Memorial Healthcare |
| Florida Center for Advising and Academic Support | Taylor County School District |
| Florida Center for Library Automation | University of Central Florida |
| Florida College at Jacksonville | University of Florida |
| Florida Guardian Ad Litem Office | University of North Florida |
| Florida Gulf Coast University | University of South Florida |
| Florida Institute of Government | University of West Florida |
| Florida International University | Wakulla County School District |
| Florida State University | Walton County School District |
| Florida State University School | Washington County School District |

## EXHIBIT B
## LIST OF SERVICES OFFERED BY NWRDC
## AS OF APRIL 1, 2012

| Service Category | Service Type Detail |
|---|---|
| Mainframe Services | Batch Processing |
| | CICS Processing |
| | TSO Processing |
| | Shadow Direct Processing |
| | Shadow Web Processing |
| | DB2 Processing |
| | |
| Open Systems Platform | Raised Floor Space |
| | Technical Personnel |
| | Support and Monitoring |
| | Core Network Port Access |
| | VPN Tunnel |
| | VPN Clients |
| | Managed Primary SATA Storage |
| | Tier 1 Storage |
| | Tier 2/Offsite Storage |
| | Tier 3 Storage |
| | Backup Storage |
| | Performance Packages |
| | Remote Replication |
| | Internal Replication |
| | Fibre Channel Ports |
| | Unmanaged Windows/Linux Virtual Server |
| | Business Continuity Add-On Service |
| | Electrical Circuits |
| | Analog Line for Remote Access |
| | Disaster Recover Workspace Subscription |
| | |
| Tallahassee Fiber Loop (TFL) | Setup and Configuration for TFL |
| | Access to Dark Fiber on NWRDC-Owned TFL |
| | Maintenance Service on TFL |
| | Lateral Segment Maintenance Provided by Vendor |
| | TFL Core Network Port Access |

## EXHIBIT C
## MANAGEMENT'S RESPONSE

NWRDC™
Northwest Regional Data Center

2048 East Paul Dirac Drive
Tallahassee, FL 32310-3752
850.245.3500 Phone
850.245.3570 Fax

David W. Martin
AUDITOR GENERAL
STATE OF FLORIDA
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450
September 4, 2012

Dear Mr. Martin,

I apologize for the delay in our response to your July 31st letter. Attached is our response to the preliminary and tentative audit findings and recommendations resulting from the recent Information Technology Operational Audit of the Northwest Regional Data Center conducted by your office. Please let us know if there are any questions or if we can provide any further information. Thank you.

Sincerely,

Tim Brown
Executive Director
Northwest Regional Data Center

Cc:
Martha Little, Inspector General, The Florida State University
Michael Barrett, Assoc. VP and CIO, The Florida State University; Vice-Chair of NWRDC Policy Board
Mehran Basiratmand, CTO, Florida Atlantic University; Chair of NWRDC Policy Board

## EXHIBIT C (CONTINUED)
## MANAGEMENT'S RESPONSE

### NWRDC Response

**Finding No. 1: It is not clear statutorily whether the State laws and administrative rules that govern the State primary data centers are applicable to NWRDC.**

**Recommendation: The Legislature should consider amending Section 1004.649, Florida Statutes, to clarify the governance structure and expectations for NWRDC as a primary data center, including whether NWRDC is subject to State primary data center system requirements as set forth in Section 282.203(1), Florida Statutes.**

NWRDC Response: While this finding is not for NWRDC, we stand ready to work with the Legislature, The State University System, and The Florida State University (our administrative host) to better define NWRDC's role as a primary data center.

**Finding No. 2: NWRDC did not have written service-level agreements (SLAs) in place with 34 of its educational entity customers.**

**Recommendation: NWRDC should execute written SLAs with all of its customer entities that define each party's responsibilities, expectations, and dispute resolution procedures.**

NWRDC Response: NWRDC agrees with this finding and will continue its efforts to execute written agreements with all customers.

**Finding No. 3: Some aspects of NWRDC's security management needed improvement.**

**Recommendation: NWRDC should develop and maintain an information security program. The program should include appropriate written security policies and procedures to ensure the confidentiality, integrity, and availability of the data and IT resources in its custody and include provisions for the management of employee accounts and access privileges.**

NWRDC Response: As stated, NWRDC currently has a security policy under development. NWRDC will work with its Policy Board to complete and implement this policy by June 30th, 2013.

**Finding No. 4: NWRDC lacked written procedures addressing the detailed requirements for documenting and tracking hardware and systems software changes, emergency changes, and the periodic review of changes. In addition, NWRDC did not have a complete, system-generated record of all hardware and systems software changes. NWRDC also lacked documentation of the authorization, testing, approval, and implementation of mainframe and internal systems software changes for 12 changes included in our sample.**

**Recommendation: NWRDC should supplement its change management policy with written procedures addressing the detailed requirements for documenting and tracking systems software and hardware changes, emergency changes, and the periodic review of changes. Additionally, NWRDC should implement system-generated logs to record, track, and report all system software changes that are made to each platform. Furthermore, NWRDC should maintain documentation that demonstrates the appropriate authorization, testing, approval, and implementation of systems software changes.**

## EXHIBIT C (CONTINUED)
## MANAGEMENT'S RESPONSE

NWRDC Response: NWRDC agrees with this finding and has already begun improving its change management process. As part of the FY 12-13 budget, NWRDC included an automated change management system. Planning for its implementation is currently underway.

**Finding No. 5: Certain NWRDC security controls related to user authentication, disclosure of sensitive security information, and monitoring needed improvement.**

**Recommendation: NWRDC should improve security controls related to user authentication, disclosure of sensitive information, and monitoring to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.**

NWRDC Response: NWRDC agrees with this finding and has already taken steps to improve its security controls.

**Finding No. 6: NWRDC's Disaster Recovery Plan did not address recovery or testing procedures for its internal systems.**

**Recommendation: NWRDC should incorporate its internal systems into its Disaster Recovery Plan.**

NWRDC Response: NWRDC agrees with this finding. Funds were budgeted for improvements for back office disaster recovery for FY 12-13 and work is already underway. NWRDC will complete disaster recovery planning for its back office environment by June 30th, 2013.

**Finding No. 7: Although management had informally designated all NWRDC positions as special trust positions, level 2 background screenings that included national criminal record checks and fingerprinting had not been completed for some NWRDC employees.**

**Recommendation: NWRDC should complete Statewide and national background screenings, including fingerprinting, for all of its employees. Additionally, NWRDC should update its policy to formally designate all NWRDC positions as special trust positions.**

NWRDC Response: NWRDC agrees with this finding and will review its policy on background checks with the NWRDC Policy Board and its administrative host, The Florida State University.

**Finding No. 8: NWRDC had not established written procedures for mainframe or open systems performance monitoring.**

**Recommendation: NWRDC should establish written procedures for mainframe and open systems performance monitoring.**

NWRDC Response: Although NWRDC does regularly monitor performance of the systems it is responsible for, we agree that we do not have a written policy stating such. We will work with the NWRDC Policy Board to implement such a policy by June 30th, 2013.

**Finding No. 9: Contrary to Federal requirements, NWRDC was unable to demonstrate, for many data center services, that the established billing rates and charges were appropriate and equitably applied to its customers based on the costs and utilization of data center services. Additionally, NWRDC reported a working capital reserve balance**

## EXHIBIT C (CONTINUED)
## MANAGEMENT'S RESPONSE

**that exceeded what is considered reasonable for normal operating expenses pursuant to Federal requirements.**

**Recommendation: To demonstrate compliance with State law and Federal requirements and the appropriateness and equitability of NWRDC billings, NWRDC should maintain supporting documentation for the methodology used to determine the estimated utilization of services used, along with estimated costs, to establish billing rates actually charged to customer entities. In addition, once actual costs for the fiscal year ended June 30, 2012, are known and NWRDC prepares the comparison between total revenues and allowable costs, NWRDC should make the appropriate adjustments to customer billings and maintain a reasonable level of working capital reserve to operate from one billing cycle to the next pursuant to OMB Circular A-87. Also, NWRDC, in consultation with DFS, should make adjustments to the State's 2013 SWCAP to correct the reported expenditures for allowable depreciation for the fiscal year ended June 30, 2011.**

**NWRDC Response:** NWRDC agrees with this finding. Since completion of this audit, NWRDC has revised its 2013 SWCAP report for the fiscal year ending June 30, 2011 to include deprecation. With this revision, our 2013 SWCAP report showed a negative working capital cash balance in total. Subsequently, we were requested by DFS and the federal auditor to complete the reconciliation by service for our 2013 SWCAP report. This report did indeed show that NWRDC had over recovered its costs in the Tallahassee Fiber Loop ($92,723) and Software as a Service ($55,438) for that fiscal year. However, we also noted in the report that NWRDC had already credited this over recovered amount to its customers in the fiscal year beginning July 1, 2011. Funds over recovered for FY 11-12 were also credited to customers. This revised report has been provided to the Department of Financial Services. NWRDC has documented all rates in our FY 2012-13 Service Catalog and continues to review our rates to ensure their compliance with OMB Circular A-87. This will be completed for the next budget proposal to the NWRDC Policy Board in May, 2013.