REPORT NO. 2011-082
JANUARY 2011

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 Children and Family Services (DCFS) for administrative purposes only and is a separate budget entity that is not subject to control, supervision, or direction by DCFS in any manner. Pursuant to Section 282.203(2), Florida Statutes, the head of NSRC is the Board of Trustees, 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 July 2010 through November 2010 are listed below:

Board Member	Customer Entity Represented
Ann Coffin, Chair	Department of Revenue
Barbara Palmer, Vice Chair	Department of Children and Family Services
John Boynton	Department of State
Keith Goodner	Department of Health
Terry Kester	Department of Business and Professional Regulation
Fred Schuknecht	Department of Juvenile Justice
Doug Smith	Department of Corrections
Alexandra Weimorts	Agency for Persons with Disabilities

James Stewart, Interim Executive Director

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

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; 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.

The results of our audit are summarized below:

Finding No. 1: NSRC did not maintain documentation supporting how the estimated utilization of the various NSRC services was determined. This estimate, along with the estimated cost, formed the basis for billing rates charged to customer entities for NSRC services.

Finding No. 2: NSRC documentation and calculations did not demonstrate that the composition of the NSRC Board of Trustees was equitable or consistent with the provisions of State law.

Finding No. 3: Contrary to law, NSRC could not provide documentation of the NSRC Board of Trustees' approval of the 2009-10 fiscal year Service Catalog (portfolio of services offered to NSRC customers).

Finding No. 4: NSRC lacked written policies and procedures for some important data center functions.

Finding No. 5: NSRC had not completely tested the effectiveness of its Computer Disaster Recovery Plan since the July 1, 2009, inception of NSRC.

Finding No. 6: Some NSRC staff shared generic user identification codes (IDs) for NSRC server administration functions, limiting NSRC's ability to establish accountability for server administration actions.

Finding No. 7: Some NSRC password and logon controls needed improvement.

BACKGROUND

Section 282.201(1), Florida Statutes, provides that agency data centers and computing facilities are to be consolidated into primary data centers to the maximum extent possible by 2019. Pursuant to Chapter 2009-80, Section 10, Laws of Florida, effective July 1, 2009, NSRC was established as a primary data center to which State agencies are to migrate their computing resources.

Pursuant to Chapter 2010-148, Section 8, Laws of Florida, all data center functions performed, managed, operated, or supported by those State agencies with resources and equipment currently located in a State primary data center, excluding application development, shall be transferred to the primary data center, and those agencies shall become full service customer entities by December 31, 2010. During the audit period, the applicable agencies were in the process of transferring data center functions to NSRC.

NSRC is headed by a Board of Trustees, 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. 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. Table 1 provides a list of NSRC customer entities as of November 2010. A list of services offered by NSRC is included in this report as EXHIBIT A.

Table 1
List of NSRC Customer Entities

Agency for Persons with Disabilities
Department of Children and Family Services
Department of Citrus
Department of Health
Department of Juvenile Justice
Department of Revenue
Department of State

Pursuant to Section 282.201(2)(a), Florida Statutes, the Agency for Enterprise Information Technology (AEIT) is responsible for collecting and maintaining information necessary for developing policies relating to the data center system. In addition, pursuant to Section 282.201(2)(f), Florida Statutes, AEIT is to develop and establish rules relating to the operation of the State data center system that comply with applicable Federal regulations. AEIT is also responsible, pursuant to Section 282.201(2)(e), Florida Statutes, for developing and submitting to the Legislature by December 31, 2010, an overall consolidation plan for State data centers.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: NSRC Billing Rates

Section 282.203(3)(e), Florida Statutes, provides that each board of trustees of a primary data center ensure the sufficiency and transparency of primary data center financial information. In a letter to the United States Department of Health and Human Services dated December 24, 2008, the Assistant Secretary for Administration for the Department of Children and Family Services stated that the NSRC cost allocation will be included in Section 2 – Billed Services of the State's Statewide Cost Allocation Plan. The Office of Management and Budget (OMB) Circular A-87, Attachment C, State/Local Wide Central Service Cost Allocation Plans, provides that all costs and data used to distribute costs included in the Plan should be supported by formal accounting and other records that will support the propriety of the costs assigned to Federal awards.

To recover all costs of NSRC services, NSRC established billing rates for each service provided by the data center. For the 2009-10 and 2010-11 fiscal years, NSRC management developed a Service Catalog that listed and described services provided by NSRC. The NSRC billing rates charged to customer entities were calculated based on the estimated cost and utilization of the various NSRC services. Our audit disclosed that, for the billing rates charged to customers during the 2009-10 and 2010-11 fiscal years, NSRC could not, upon audit request, provide documentation supporting how the estimated utilization of the various NSRC services was determined. This estimate, along with the estimated cost, formed the basis for billing rates charged to customer entities for NSRC services.

Subsequent to the end of the 2009-10 fiscal year, NSRC compared its actual costs for the fiscal year, which according to NSRC records totaled approximately $24.6 million, with 2009-10 customer billings. Based on the comparison,

NSRC billings exceeded actual costs by approximately $3.1 million and NSRC planned to make adjustments to future customer billings to account for the differences. Without supporting documentation for the establishment of billing rates for NSRC services, NSRC could not demonstrate that the established rates were appropriate and equitably applied to the customer agencies based on utilization of data center services.

Recommendation: To demonstrate compliance with State law and Federal guidelines and the appropriateness and equitability of NSRC billings, NSRC should maintain supporting documentation for the establishment of billing rates, including documentation as to how the estimated utilization of NSRC services was determined.

Finding No. 2: NSRC Board of Trustees

Section 282.203(2), Florida Statutes, provides that each primary data center be headed by a board of trustees. Section 282.203(2)(a)1., Florida Statutes, provides that, for each of the first two fiscal years that a data center is in operation, board membership is to be based on projected customer entity usage rates for the fiscal operating year of the data center. According to AEIT management, primary data centers use the billing rates as a measure of entity usage rates.

Our audit disclosed that NSRC documentation and calculations did not demonstrate that the composition of the Board was equitable or consistent with the provisions in State law. As described in finding No. 1, NSRC was unable to provide documentation of the basis for the estimated utilization of NSRC services used in the establishment of billing rates and, therefore, could not demonstrate the appropriateness of the projected customer entity usage rates used to determine Board membership. In addition, we noted that the calculation used by NSRC to determine the membership of the NSRC Board of Trustees was not consistent with the requirements of Section 282.203(2)(a)1. and 4., Florida Statutes. Specifically, Section 282.203(2)(a)4.e., Florida Statutes, provides that a single trustee having one vote shall represent, collectively, all customers with less than 4 percent of the total usage. Our audit disclosed that three NSRC customer agencies met the statutory criteria for one collective representative. However, two of the three agencies were represented on the Board with separate trustees, each of whom had one vote. The third agency had no Board representation. In addition, our audit disclosed that another agency was granted two votes but only met the required level of entity utilization for one vote, contrary to Section 282.203(2)(a)4.a., Florida Statutes.

Recommendation: NSRC should provide the Board of Trustees with the documentation and calculations to establish Board representation based on documented customer entity usage rates in a manner consistent with State law.

Finding No. 3: NSRC Services

Section 282.203(3)(g), Florida Statutes, requires each board of trustees of a primary data center to approve the portfolio of services offered by the data center. NSRC is to offer, develop, and provide services as defined and approved by the Board of Trustees. Although NSRC management developed a 2009-10 Service Catalog (portfolio of services offered to NSRC customers), contrary to State law, NSRC could not, upon audit request, provide documentation of the Board of Trustees approval of the Service Catalog.

Recommendation: NSRC should ensure that all future Service Catalogs are approved by the Board of Trustees as required by State law.

Finding No. 4: IT Policies and 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. Also, Section 282.203(3)(b), Florida Statutes, provides that each board of trustees of a primary data center is to establish procedures for the primary data center to ensure that budgeting and accounting procedures, cost-recovery methodologies, and operating procedures are in compliance with laws governing the State data center system. NSRC lacked written policies and procedures for the following data center functions:

- Periodically reviewing the appropriateness of access privileges assigned to users of certain systems.
- Capturing, documenting, and reporting timely, consistently, and accurately the cost-recovery methodologies, billings, receivables, expenditures, budgeting and accounting data.
- Monitoring system hardware performance and capacity-related issues.
- Transferring State agency resources and equipment to the primary data center.

Absent written policies and procedures, the risk is increased that data center controls may not be followed consistently and in a manner pursuant to management and Board expectations.

Recommendation: NSRC should establish written policies and procedures to document management and Board expectations for the performance of its important data center functions.

Finding No. 5: Disaster Recovery Planning

Disaster recovery plans are an important element of effective internal control over IT operations. Section 282.203(1)(g), Florida Statutes, requires that each primary data center maintain an effective disaster recovery plan. NSRC has developed a Disaster Recovery Plan to ensure the continuation of normal computer services in the event of an emergency or disaster. Also, the NSRC Disaster Recovery Plan states that the Plan will be tested on at least an annual basis at an alternate recovery site (hot site). However, NSRC had not completely tested the effectiveness of the Plan since the inception of NSRC on July 1, 2009. NSRC conducted an incident management exercise in June 2010 to focus on NSRC's ability to respond to a crisis situation; however, this exercise did not test NSRC implementation of its alternate recovery site. When a disaster recovery plan has not been completely tested for feasibility or weaknesses, there is an increased risk that, in the event of an actual disaster, recovery measures may not function as intended and IT operations may not be timely restored.

Recommendation: NSRC should completely test the effectiveness of its Disaster Recovery Plan on an annual basis.

Finding No. 6: User Identification

The effectiveness of access controls is dependent, in part, on the ability to uniquely identify system users. Unique identification of individual users assists in the assignment of specific access privileges and provides a mechanism for attributing system actions to a responsible user.

NSRC Operating Procedure No. 50-2 states that each person who uses equipment to access systems that reside at NSRC will have a unique personal identifier. Our audit disclosed, however, that six NSRC employees shared generic

user identification codes (IDs) and passwords in the administration of the certain agency servers. Administration access privileges provide, among other capabilities, the capability to grant access to the computer servers and install software. Without the ability to uniquely identify server administrators, the ability of NSRC to establish accountability for server administration actions is limited.

Recommendation: NSRC should assign unique personal identifiers to each employee who is authorized to perform server administration functions as required by its Operating Procedure.

Finding No. 7: Security Controls – Password and Logon Controls

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed that some NSRC password and logon controls needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising customer entity data and IT resources. However, we have notified appropriate NSRC management of the specific issues. Without adequate password and logon controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that customer entity data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: NSRC should implement the appropriate password and logon controls to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

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 from June 2010 to November 2010 in accordance with applicable 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 audit were to determine the effectiveness of selected IT controls related to NSRC data center operations 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.

The scope of our audit focused on evaluating selected IT controls relevant to NSRC data center operations, including selected general IT controls over operations and security, governance of NSRC, and the data center consolidation migration process.

In conducting our audit, we:

- Interviewed NSRC personnel.
- 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.

- Examined systems software and network components on a sample basis to determine whether access to systems software was appropriate and whether appropriate password and logon controls were in place. Specifically, we sampled 10 systems software and network components within the NSRC infrastructure accessed by customer entities to evaluate the appropriateness of access and sampled 14 systems software and network components to evaluate password and logon controls.
- Tested the effectiveness of background screenings of NSRC staff with access to customer entity IT resources. Specifically, we sampled 30 staff members to determine whether individuals holding positions of trust had undergone required background checks and fingerprinting.
- Tested the effectiveness of selected controls over the modification of systems software. Specifically, we tested 27 changes to systems software and network components implemented between July 1, 2010, and August 27, 2010, to determine whether the changes were authorized, tested, and documented.
- Observed and evaluated the adequacy of NSRC physical controls and environmental safeguards in place to protect IT resources.
- Evaluated the adequacy of selected disaster recovery and continuity of operations planning controls.
- Evaluated on a sample basis the effectiveness of tape handling procedures. Specifically, we sampled 30 tapes from the mainframe and mid-range environments to determine whether an accurate inventory was maintained for the onsite and offsite tapes.
- Examined on a sample basis the NSRC IT resource inventory to evaluate the effectiveness of inventory and equipment tracking procedures. Specifically, we sampled 30 items on the IT resource inventory to determine if the inventory and the surplus inventory was properly tracked by NSRC.
- Inspected service-level agreements established between NSRC and its customer entities to determine whether all provisions required in Section 282.203(1)(i)1., Florida Statutes, were included.
- Obtained an understanding of the statutory requirements of NSRC data center operations and evaluated the effectiveness of NSRC's compliance with selected requirements.
- Obtained an understanding of the data center consolidation process and services provided or offered by NSRC.
- Obtained an understanding and evaluated the effectiveness of the NSRC cost measurement and distribution methodology and the billing process used by NSRC.

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 January 14, 2011, the Interim Executive Director provided responses to our preliminary and tentative findings. This letter is included at the end of this report as EXHIBIT B.

EXHIBIT A
LIST OF SERVICES OFFERED BY NSRC

Professional Services	Professional Services – NSRC staff
Data Center Management	SRC Raised Floor Space
	Off-Site Tape Storage – Mainframe
	Off-Site Tape Storage - Midrange
	Print Services
	Network to Network Interface - Local
	Network to Network Interface – DMZ
	Network to Network Interface – IPSEC Lan-Lan VPN
	Bandwidth
	DNS Domain Hosting
	Simple Server Load Balancing
	Complex Server Load Balancing
Mainframe Services	Batch Processing
	CICS Processing
	DB2 Processing
	IMS Processing
	TSO Processing
	Unisys Batch and Online Processing
	IBM Tape Cartridges
	Unisys Tape Cartridges
	IBM Print Management
	Unisys Print Management
Open Systems Platform	Managed Server – LINUX
	Managed Server – LINUX EOSL Surcharge
	Managed Server – Oracle Premium
	Managed Server – SQL Server
	Managed Server – UDB Server
	Network Services
Storage Management	Backup Service
	Tier 1 Disk Storage
	Tier 2 Disk Storage
	Tier 3 Disk Storage
	IBM Mainframe Disk Storage
	Unisys Mainframe Disk Storage
Windows Platform	Managed Server – Windows
	Managed Server – Windows EOSL Surcharge
Disaster Recovery	Disaster Recovery Services

Source: NSRC 2009-10 Service Catalog, dated November 2, 2009

THIS PAGE INTENTIONALLY LEFT BLANK

EXHIBIT B
MANAGEMENT'S RESPONSE

State of Florida
Northwood Shared Resource Center

Rick Scott
Governor

James Stewart
Interim, Executive Director

January 14, 2011

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

Dear Mr. Martin:

Thank you for your December 15 letter accompanying the preliminary findings and recommendations of your report to be prepared on the Information Technology Operational Audit of the Northwood Shared Resource Center (NSRC), Data Center Operations.

The NSRC generally concurs with the findings of your report. Enclosed is NSRC's response to the specific recommendations you provided. If you or your staff have additional questions, please have them contact James Stewart at 921-0182.

Sincerely,

James Stewart

Mr. James Stewart
Interim Executive Director

Enclosure

1940 North Monroe Street, Suite 80 Tallahassee, Florida 32399

Mission: To provide customers with consistent and secure computing power, expert support, creative technology solutions, and continuity of service.

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS
Information Technology Operational Audit of the
NORTHWOOD SHARED RESOURCE CENTER (NSRC)
DATA CENTER OPERATIONS

Finding No. 1
NSRC Billing Rates

Recommendation: To demonstrate compliance with State law and Federal guidelines and the appropriateness and equitability of NRSC billings, NSRC should maintain supporting documentation for the establishment of billing rates, including documentation as to how the estimated utilization of NSRC services was determined.

Response: The NSRC agrees with this finding. The documentation to support the development of the units for Fiscal Year 2009-10 and 2010-11 was not made available to the audit staff and therefore could not be substantiated.

The units that were created for Fiscal Year 2010-11 were based on ten months of "actuals" and two months of estimates. Since the rates are required to be created and approved in time for July 1st billing, this is the most accurate process that is available to the NSRC for rate development relative to the subsequent year.

Finding No. 2
NSRC Board of Trustees

Recommendation: NSRC should provide the Board of Trustees with the documentation and calculations to establish Board representation based on documented customer entity usage rates in a manner consistent with State law.

Response: The NSRC agrees with the finding that the NSRC Board of Trustees membership is incorrect. This finding was addressed and corrected at the December 16, 2010 Board of Trustees meeting. A spreadsheet showing current and recast representation and number of votes granted for each customer agency was developed by the NSRC according to Sections 282.203(2)(a)1. and 282.203(2)(a)4. Florida Statutes and presented to the Board of Trustees at the meeting. Based on this spreadsheet, the Board of Trustees appointed the trustee from the Department of State as the single trustee to represent all three customer agencies having less than four percent of the total usage (Department of State, The Agency for Persons With Disabilities, and The Department of Citrus). The trustee from The Agency for Persons With Disabilities was eliminated from the board. The Department of Revenue had their number of votes reduced from two to one.

1

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 3
NSRC Services

Recommendation: NSRC should ensure that all future Service Catalogs are approved by the Board of Trustees as required by State law.

Response: The NSRC agrees in principle with this finding and will ensure that the Board of Trustees approves the Service Catalog in addition to the Service Rates on an annual basis. However, though not reflected in the minutes, the document that was presented to the Board includes a listing of the services as well as a description for each service. The rates were also included in that same document, as well. The service descriptions for the document were extracted from the Service Catalog.

Finding No. 4
IT Policies and Procedures

Recommendation: NSRC should establish written policies and procedures to document management and Board expectations for the performance of its important data center functions.

Response:

Bullet 1: Phase I of a periodic access review process was initiated in February 2010 and implemented October, 2010. The next review is due February 15, 2011. In October, 2010, Phase II was added which includes an administrative review of all access privileges and administrator rights. Managers will assure appropriate access or rights to systems or hardware under their control.

NSRC Standard Operating Procedure (SOP) S-1 has been updated to include this in policy and procedure statements. It will be submitted to the board for approval in January 2011.

Bullet 2: The NSRC agrees with the finding and will create policies by June 30, 2011 relative to cost recovery methodologies, billing, receivables, expenditures, budgeting and accounting. In addition, the NSRC will establish written procedures for the same by December 30, 2011.

Bullet 3: The NSRC agrees with the finding and will create policies by June 30, 2011 relative to monitoring system hardware performance and capacity planning. In addition, the NSRC will establish written procedures for the same by December 30, 2011.

2

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Bullet 4: The NSRC agrees with the finding. NSRC currently uses the Department of Children and Families' (DCF) process and staff for transferring State agency resources and equipment to the primary data center. The NSRC will establish a written policy and procedure for transferring State agency resources and equipment to the NSRC by May 30, 2011, prior to the next Data Center consolidation initiative.

Finding No. 5
Disaster Recovery Planning

Recommendation: NSRC should completely test the effectiveness of its Disaster Recovery Plan on an annual basis.

Response: NSRC utilizes the same Disaster Recovery Plan developed at DCF before the NSRC was created in 2009. The plan was tested annually at the offsite location for 15 years prior to the creation of NSRC. The NSRC recovery team is composed of the same staff that tested the recovery plan while at DCF. NSRC was not able to test in 2009 or 2010 due to lack of travel funds for the team to travel to Philadelphia. The 2010 tabletop was the only viable alternative. While this exercise did not simulate or allow onsite testing, it did provide a valuable piece of disaster planning that had never been tested—the initial response and planning prior to the team restoring offsite.

Plans are underway for testing in spring of 2011. NSRC is working with SunGard to set up a date prior to the start of hurricane season and the end of the current contract. This will be a full onsite test.

Finding No. 6
User Identification

Recommendation: NSRC should assign unique personal identifiers to each employee who is authorized to perform server administration functions as required by its Operating Procedure.

Response: NSRC has been transitioning administrative rights for agency servers new to NSRC under Data Center consolidation. We understand the risks of using shared accounts for access to systems and we are working to address these instances. NSRC will be asking each agency to create unique user-ids for each NSRC staff person that needs access to the individual agencies systems or administrator accounts and make the agencies aware of our Password and Account Control policies applicable to such users and systems. NSRC will correct existing systems that currently have shared accounts no later than March 31, 2011.

NSRC will also share our audit findings with customer agencies so that they can reconcile policy differences to the recommendations.

3

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

NSRC will revise SOP 50-2 to allow a reasonable grace period to bring transitioning agencies into compliance. The amount of time will vary by agency depending on the number of servers and systems and the complexities involved.

Finding No. 7
Security Controls – Password and Logon Controls

Recommendation: NSRC should implement the appropriate password and logon controls to ensure the continued confidentiality, integrity, and availability of customer entity data and IT resources.

Response: NSRC has revised NSRC SOP 50-2 to include a policy that requires login controls and complex passwords whenever possible and tighter controls when options are limited. The corresponding procedures suggest compliance methodologies and alternatives when appropriate.

NSRC SOP 50-2 has been updated to include this in policy and procedure statements. It will be submitted to the board for approval in January.

NSRC will revise SOP 50-2 to allow a reasonable grace period to bring transitioning agencies into compliance. The amount of time will vary by agency depending on the number of servers and systems and the complexities involved.