A Report
to the
Montana
Legislature

Information Systems Audit

SABHRS: Procurement Card Processing and Select Access Controls

Department of Administration

March 2011

Legislative Audit
Division

11DP-04

Fraud Hotline
Help eliminate fraud, waste, and abuse in state government.
Call the Fraud Hotline at:

(Statewide)
1-800-222-4446
(in Helena)
444-4446

Information Systems Audits

Information Systems (IS) audits conducted by the Legislative Audit Division are designed to assess controls in an IS environment. IS controls provide assurance over the accuracy, reliability, and integrity of the information processed. From the audit work, a determination is made as to whether controls exist and are operating as designed. We conducted this IS audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our finding and conclusions based on our audit objectives.

Members of the IS audit staff hold degrees in disciplines appropriate to the audit process. Areas of expertise include business, accounting, education, computer science, mathematics, political science, and public administration.

IS audits are performed as stand-alone audits of IS controls or in conjunction with financial-compliance and/or performance audits conducted by the office. These audits are done under the oversight of the Legislative Audit Committee which is a bicameral and bipartisan standing committee of the Montana Legislature. The committee consists of six members of the Senate and six members of the House of Representatives.

Direct comments or inquiries to:
Legislative Audit Division
Room 160, State Capitol
P.O. Box 201705
Helena, MT 59620-1705
(406) 444-3122

Reports can be found in electronic format at:
http://leg.mt.gov/audit

LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors
Cindy Jorgenson
Angie Grove

March 2011

The Legislative Audit Committee
of the Montana State Legislature:

We conducted an Information Systems audit of the Statewide Accounting, Budgeting, and Human Resources System (SABHRS) maintained and operated by the Department of Administration. SABHRS is used to assist in the administration of financial and human resource records within state government. The focus of the audit was to ensure specific controls are in place and processes are working as intended.

This report contains three recommendations for strengthening controls over programmer access, eliminating access through generic accounts, and updating agency security manuals.

We wish to express our appreciation to department personnel for their cooperation and assistance.

Respectfully submitted,

/s/ Tori Hunthausen

Tori Hunthausen, CPA
Legislative Auditor

Room 160 • State Capitol Building • PO Box 201705 • Helena, MT • 59620-1705
Phone (406) 444-3122 • FAX (406) 444-9784 • E-Mail lad@mt.gov

Table of Contents

Figures and Tables

Figures

Appointed and Administrative Officials

Department of Administration

Janet R. Kelly, Director

Sheryl Olson, Deputy Director

Dick Clark, Chief Information Officer

Paul Christofferson, Administrator, State Accounting Division

Paula Stoll, Administrator, State Human Resource Division

Cheryl Grey, Chief, SABHRS Finance and Budget Bureau

Randy Morris, Chief, HR Information Services Bureau

MONTANA LEGISLATIVE AUDIT DIVISION

INFORMATION SYSTEMS

SABHRS: Procurement Card Processing and Select Access Controls

Department of Administration

MARCH 2011 11DP-04 REPORT SUMMARY

All state financial transactions are ultimately administered through SABHRS including payments to contractors, employee payroll, collection of tax revenues, and payment of State expenses. All users have varying levels of access to the system, so the department should ensure all access is controlled and monitored accordingly.

Context

The Statewide Accounting, Budgeting, and Human Resources System (SABHRS) is a statewide computer application implemented by the State of Montana to assist state agencies in reporting the disposition, use, and receipt of public resources (§17-1-102 (2), MCA). SABHRS also assists in the administration of human resource information, including the generation of a biweekly payroll. SABHRS is used to record and monitor the movement of all state resources.

On an annual basis, an Information Systems audit is conducted of controls over SABHRS. Because we review SABHRS annually, this audit was limited to specific access and procurement card processing controls.

Results

Overall SABHRS has controls in place in the specific areas we tested. However, we identified areas where controls over system access can be strengthened.

Human Resources Information Services Bureau (HRIS) programmers assist with the development of new processes and reports, implement vendor developed upgrades, and correct errors in programming code or data. We determined HRIS programmers have extensive access to the production environment. However, we noted this access has only been used once or twice a year in the past. Programmers with access to modify the production environment could make unapproved changes to data.

We also identified the use of three generic accounts in SABHRS. Each of these superuser accounts are required by the system to manage processes. However, we determined they can be accessed by department database administrators. The access allowed through these roles does not correspond to their job duties. Additionally, these accounts are accessed through the use of a single login and shared password. The use of generic accounts with a single, shared login decreases accountability. Without monitoring and access control, the potential exists an unauthorized change can be made to SABHRS without being able to identify the specific user.

In order to use SABHRS, individuals must be granted access. Agency security officers use SABHRS security manuals to manage access. Due to the complexity of access roles, there is potential for creating incompatible access. As such, it is important to ensure all documentation provides a clear understanding of the access control environment.

Recommendation Concurrence	
Concur	3
Partially Concur	0
Do Not Concur	0
Source: Agency audit response included in final report.	

For a complete copy of the report or for further information, contact the Legislative Audit Division at 406-444-3122; e-mail to lad@mt.gov; or check the website at http://leg.mt.gov/audit.
Report Fraud, Waste, and Abuse to the Legislative Auditor's FRAUD HOTLINE
Call toll-free 1-800-222-4446, or e-mail lad@mt.gov.

Chapter I – Introduction

Introduction

The Statewide Accounting, Budgeting, and Human Resources System (SABHRS) is a statewide computer application implemented by the State of Montana and managed by the Department of Administration (DOA) to assist state agencies in reporting the disposition, use, and receipt of public resources (§17-1-102(2), MCA). SABHRS also assists in the administration of human resource information, including the generation of a biweekly payroll.

On an annual basis, an Information Systems audit is conducted of controls over SABHRS, including a review of modifications made to system processing during the previous year. Because we review SABHRS annually, this audit was limited to specific access and procurement card processing controls. The intent of the SABHRS audit is to identify and test specific controls over the application to ensure the system continues to operate as intended. Based on our work, we provide a limited distribution memorandum detailing the SABHRS control environment to Legislative Audit Division Staff for consideration during other audits. This report presents the findings of our review and includes recommendations for strengthening controls.

Background

SABHRS includes two subsystems: Financials (FS) and Human Resources Management (HR). While comprising a single system these two subsystems are managed and operated independently. Each of these subsystems is used by accounting and human resource staff at the agency level to assist in the management of financial and human resource business operations. Within each of these subsystems are modules providing different processing areas to users.

The FS subsystem is used to:

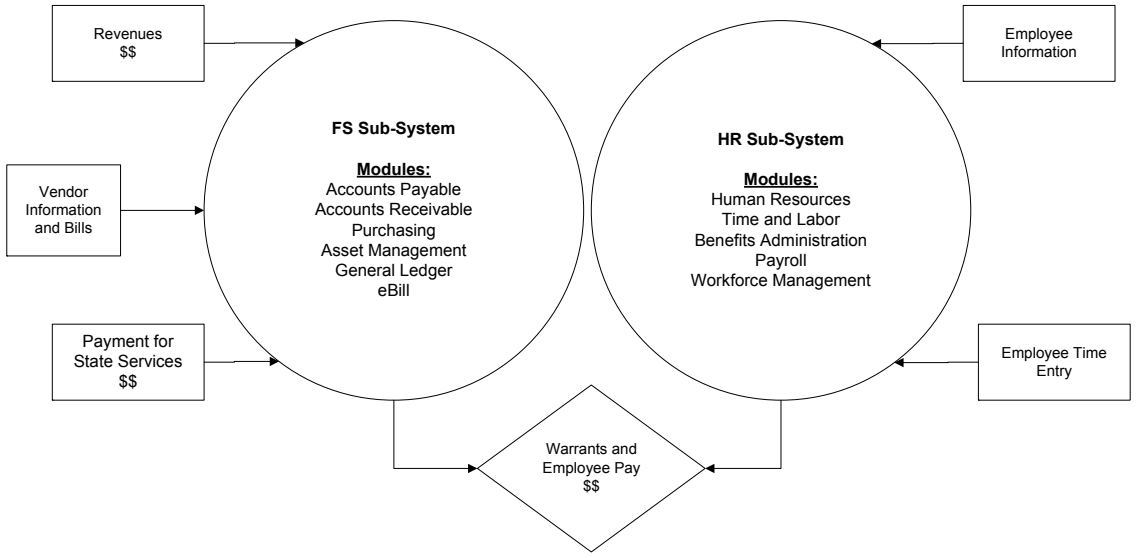
- Process vouchers and payments to vendors.
- Process incoming payments and billing statements.
- Generate journal entries for each transaction and post to the General Ledger.
- Manage purchase order transactions and records.
- Store procurement card transaction records.
- Record state assets and calculate depreciation.

The HR subsystem is used to:

- Record and maintain employment records for state employees.
- Record, validate, and approve employee time.
- Record and calculate benefits for state employees.
- Calculate individual employee payroll.

The following figure provides an overview of the SABHRS system.

Figure 1
SABHRS Overview



Source: Compiled by the Legislative Audit Division from information obtained from the Department of Administration.

The responsibilities for all SABHRS maintenance and support are divided among three DOA entities:

- SABHRS Finance and Budget Bureau (SFABB) is responsible for managing the financial system.
- Human Resources Information Services Bureau (HRIS) is responsible for the human resources system.
- State Information Technology Services Division is responsible for providing technical support.

Audit Scope and Objectives

We focused our work on specific system controls and procurement card processing controls. Our objectives were to:

1. Determine if specific controls within SABHRS operate as intended, including:
    - Ensuring access to specific business processes is limited.

    Results for all other controls reviewed were included in the limited distribution memorandum.

2. Determine if specific controls related to system procurement card processes are working as expected, including:
    - Determining if cardholder data is stored in accordance with the Payment Card Industry Data Security Standard.
    - Determining if procurement card transaction data is complete.
    - Determining if a user can manually create a procurement card transaction.
    - Ensuring a user cannot both create and approve a procurement card transaction.
    - Determining if expense account assignments for procurement card transactions are correctly disbursed among funds.
    - Determining if scheduled payments to the procurement card vendor are reconciled against transaction data for accuracy.

Audit Methodology

Methodology included interview of staff, query and analysis of SABHRS data, review of agency documentation, and observation of SABHRS operations. Specifically we:

- Interviewed DOA:
    - HRIS management and staff
    - SFABB management and staff
    - Office of Finance and Budget accounting staff
- Queried SABHRS:
    - HR and FS subsystems for specific user access
    - FS subsystem for procurement card transaction data
    - FS subsystem to determine status of budget checking
- Observed:
    - Procurement card database tables
    - Procurement card reconciliation reports
    - Creation of agency to agency fund transfers

We evaluated the control environment using state policies, SABHRS security policies, and criteria established by the IT Governance Institute and National Institute of Standards and Technology. The audit was conducted in accordance with Government Auditing Standards published by the United States Government Accountability Office.

Summary

The following table provides an overall summary of the results of our audit.

Table 1
Summary of Audit Results

Control Areas	Audit Objectives	Testing Results
Input	#1–manual transactions #2–transaction data complete	Pg 11–conclusion
Processing	#1–processing controls	Pg 11–conclusion
Output	#2–reconciliation	Pg 11–conclusion
Access	#1–access	Pg 6-8–recommendations

Source: Compiled by the Legislative Audit Division.

Prior Audit Follow-Up

In the previous SABHRS audit report we made two recommendations to DOA. Both recommendations were implemented. The first recommended DOA segregate user access roles to prevent State Accounting Division (SAD) personnel from creating a vendor, and subsequently creating and approving a payment voucher for that vendor. Specific business transactions within SABHRS require the use of preapprovals. This process creates the potential for users within SAD to bypass segregation of duties controls. DOA has since restricted SAD personnel from creating vouchers using preapprovals.

We also recommended DOA change the way HRIS personnel access requests are approved and reviewed. Each functional area within the HR subsystem requires specific permissions to perform business processes. During the prior audit, we identified users within HR modules that should not have access to those areas. The department made changes to the SABHRS security manual requiring all requests for HR access be approved by the functional supervisors for any affected module. Additionally, HRIS has modified its review process to include monthly reviews of the permissions associated with roles.

Chapter II–SABHRS Access

Introduction

System controls are a combination of automated and manual processes and activities which help ensure data confidentiality, integrity, and availability. Although there can be thousands of system controls, some have more impact on system performance than others. For this audit of the Statewide Accounting, Budgeting, and Human Resources System (SABHRS), we focused on system controls related to user access. Because the Department of Administration (DOA) had an access related recommendation from the last audit we reviewed controls to determine if excessive access still existed.

Programmer Access is Not Restricted

The Human Resources Information Services Bureau (HRIS) manages the modules within the SABHRS Human Resources Management (HR) subsystem. HRIS programmers assist with the development of new processes and reports, implement vendor developed upgrades, and correct errors in programming code or data. Most of the programmers' work is performed in either the development or testing environments of SABHRS, as opposed to directly in the SABHRS production environment where the business of the State actually occurs.

During our previous audit we identified concerns surrounding unnecessary access to the production environment by HRIS personnel including programmers. While the agency has changed the process for granting access to the HR subsystem and removed most of the user access, it did not remove the access for the programmers. HRIS programmers have extensive access to the SABHRS application production environment. This access includes the ability to make changes to any SABHRS data such as payroll, update benefit information, and change employee information. These duties are not part of the programmers' job responsibilities.

Programmers with access to modify the production environment could make unapproved changes to data. Such changes can have intentional or unintentional negative impacts on sensitive HR records. In addition, unapproved and unmonitored changes are difficult to detect and thus difficult to correct. Industry standards, including those adopted by the agency, note duties are to be separated and programmer access to the system's production environment should be limited.

Programmers require access to the application to enable them to correct errors when they occur. Management interviews noted it would create hardships if the problem occurred during overnight hours and they had to request access in order to correct the problem. While it is unknown how frequently this access will be needed in any given

year, historically this access has been used only once or twice a year. In comparison, the SABHRS Finance and Budget Bureau, which manages the Financials (FS) subsystem, does not maintain full time access for its programmers. Rather, access is requested on an as-needed basis and removed immediately after the designated task has been completed.

RECOMMENDATION #1

We recommend the Department of Administration limit all Human Resource Information Services programmer access to modify the SABHRS production environment by assigning access only when needed.

Generic Accounts Used to Manage Processes

We identified the use of three generic accounts in SABHRS. All three accounts are effectively super user accounts which allow a user to make changes to any data in SABHRS. These accounts are required by the system to manage processes. However, we determined each of these accounts can also be accessed by department database administrators. These accounts are accessed through the use of a single login and shared password. The use of generic accounts with a single, shared login decreases accountability.

The department stated the generic accounts are required to perform specific maintenance operations on SABHRS. There are currently three database administrators who have access to these roles through the shared login. Although administrators believe the access is needed for system maintenance, the access allowed through these roles does not correspond to job duties. The access provided by these roles includes access to all areas of FS and HR in the production environment, including the ability to make changes to SABHRS data. Department database administrators stated all activity using these accounts is recorded by the system and if problems arise, a report can be generated for review.

Industry best practices state organizations should ensure that requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges are documented and controlled by user account management. An approval procedure outlining the data to be accessed and system owner granting the access privileges should be included. These procedures should apply to all users, including administrators (super users), for normal and emergency cases. State policy also requires all users to have a unique login.

Without access controls and regular monitoring of activity, the potential exists an unauthorized change can be made to SABHRS database tables and DOA would not be able to identify the specific user. SABHRS management and database administrators state these roles are required to perform specific maintenance in SABHRS and cannot be removed. However, in order to increase accountability the necessary access should be more closely monitored to ensure the access granted through these accounts is not used improperly.

RECOMMENDATION #2

We recommend the Department of Administration strengthen controls over user access by actively monitoring the use of generic system accounts.

Security Documentation Should Accurately Reflect Access Controls

In order for agency personnel to use SABHRS, they must be granted access to the application. Agency security officers use SABHRS security manuals to determine if employees need access and what level of access should be allowed. Access roles have been created to implement user access. Each access role relies on supporting permissions delineating which SABHRS screens users can access and dictates if users can view, change, or delete SABHRS information.

The security manuals provided to agencies for FS and HR document all access accounts to SABHRS, the level of access those accounts provide, and how they should be used and assigned. Following a review of several SABHRS accounts in both FS and HR, we identified inconsistencies between the account descriptions we reviewed in the manuals and what actually existed in the system. We noted that for several roles the security manuals only describe the major function of the role and its associated access. However, some roles have permissions associated with them which grant access to other areas of SABHRS and are not discussed in the security manuals. According to SABHRS management, the security manuals do not maintain all security documentation; internal documentation also provides security information.

Industry best practices state that organizations should perform regular management review of all accounts and the underlying related privileges. In the case of SABHRS the underlying privileges are the permissions associated with each role. Because any permission can be assigned to multiple roles, there is the potential for creating

incompatible access and allowing users to negatively impact the system or view data they should not see. The previous two sections in this chapter identify areas of incompatible access.

The security manuals do not explicitly state when or under what circumstances generic accounts should be used and by whom. The account descriptions we reviewed in the manuals also do not provide enough detail regarding the specific permissions associated with each role. This is critical because agency security personnel use the security manuals to assign appropriate access to SABHRS. In many instances, a single user can be assigned multiple access roles with supporting permissions. Thus it is important the security manuals provide specific details on all access roles. SABHRS internal documentation may provide more details, but it is still important to ensure all documentation provides a clear understanding of the access control environment.

RECOMMENDATION #3

We recommend the Department of Administration assure security documentation accurately reflects access controls.

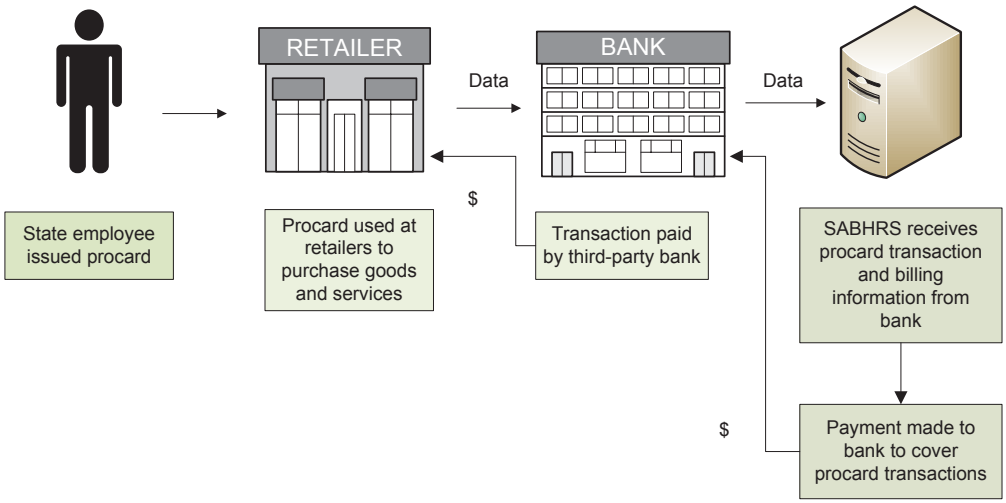
Chapter III–Procurement Card Data Controls

Introduction

During our last audit we noted the Department of Administration (DOA) began using existing processes in the Purchasing module in the Statewide Accounting, Budgeting, and Human Resources System (SABHRS) for the management of information from the use of State procurement cards (procards). As a result, one of our audit objectives was to determine if specific system controls related to procards are working as expected.

Procards are credit cards issued to, and used by, State personnel to purchase products or services on behalf of the State or to pay travel expenses associated with job duties. Cardholders purchase items from merchants who then bill the bank. The bank pays the merchant and bills the State. The State then pays the bank for the purchases made by the cardholder. The figure below illustrates this process.

Figure 2
Procard Transaction



Source: Compiled by the Legislative Audit Division from information obtained from the Department of Administration.

The responsibility for administering procards rests with each individual agency. Data for each card and all procard transaction data is stored within SABHRS and each agency's personnel manage the cards using SABHRS data. DOA accounting personnel reconcile SABHRS procard data against statements from the vendor to ensure the amount billed to the State reflects the amount paid to the vendor. Because of the

sensitive nature of procard data and the need for accurate transaction information, we identified and tested select controls within SABHRS to ensure system procard processes are working as intended.

Controls Ensure Procard Data is Secure

State of Montana procards carry the logo of one of the major payment card industry vendors who participate in the Payment Card Industry Security Council. Because of this, procards are subject to some of the provisions contained within the Payment Card Industry Data Security Standard (PCI-DSS). We reviewed processes in place for the storage and security of procard account information within SABHRS including observation of database tables, querying the database to determine assigned access, and observing users without proper access attempt to view card data. We determined DOA has controls designed to secure data according to the PCI-DSS.

Controls Exist to Ensure Transaction Data is Complete

Working with DOA, we identified a number of transaction data elements which are necessary for DOA personnel to perform their duties. Examples of required elements include the transaction date, merchant name, transaction amount, card number, etc. We queried the SABHRS FS database to determine if any transactions lacked any of the required data elements. We determined controls exist to ensure procurement card transaction data is complete.

Controls Exist to Detect Manual Transactions

Many transaction based systems allow users to create manual transactions outside of the normal process. For procards, the normal process occurs when a cardholder presents a procard for payment to a merchant and the card is swiped. The transaction data is then imported into SABHRS via an interface with the bank. Our testing determined if there were any methods which would allow a user to enter transaction data outside of this process.

We met with DOA personnel and observed all procard management screens in SABHRS. We determined there is no way for a user to create a manual transaction through the application. We identified a number of different reconciliations performed using SABHRS transaction data against statements sent by the vendor. According to DOA additional reconciliations are performed by some agencies against claims submitted by employees. These reconciliations are designed to detect manipulation in a procard transaction amount. We determined controls exist to detect manual transactions.

Payments to the Bank are Reconciled

The State of Montana pays the bank for all procard transactions once per month. Payments are made via electronic funds transfer directly to the bank. In order to ensure the State is paying the correct amount, DOA accountants reconcile the bank billing statement against reports generated by SABHRS. DOA generates the transaction report based on billing dates and expense accounts. If DOA finds a discrepancy during this process they will contact the agency with the discrepancy and work to correct the problem. Because payments to the bank will only be sent once DOA has approved the transaction amount, we determined scheduled payments to the procurement card bank are reconciled against transaction data for accuracy.

CONCLUSION

Based on the above procurement card audit work, we conclude:

Controls exist to secure transaction data.

Controls exist to ensure data is complete.

Manual transaction entries can be detected.

Payments to the bank are reconciled.

Department of Administration

Department Response

DEPARTMENT OF ADMINISTRATION
DIRECTOR'S OFFICE

A-1

BRIAN SCHWEITZER, GOVERNOR — JANET R. KELLY, DIRECTOR

STATE OF MONTANA

(406) 444-2032
FAX (406) 444-6194

MITCHELL BUILDING
125 N. ROBERTS, RM 155
PO BOX 200101
HELENA, MONTANA 59620-0101

March 11, 2011

Ms. Tori Hunthausen, CPA
Legislative Auditor
Legislative Audit Division
PO Box 201705
Helena, MT 59620-1705

RE: Audit #11DP-04: SABHRS: Procurement Card Processing and Select Access Controls

Dear Ms. Hunthausen:

The Department of Administration has reviewed Audit #11DP-04: SABHRS: Procurement Card Processing and Select Access Controls. Our responses to the recommendations are below.

Recommendation #1

We recommend the Department of Administration limit all Human Resource Information Services programmer access to modify the SABHRS production environment by assigning access only when needed.

Response: Concur. The Department's Human Resources Information Services Bureau will create a role for the bureau's programmers that will limit access to modify data, but still provide the access that is required on a regular basis to perform production payroll support.

Recommendation #2

We recommend the Department of Administration strengthen controls over user access by actively monitoring the use of generic system accounts.

Response: Concur. The Department's Database Infrastructure, Design and Support Section will strengthen controls over user access and implement a process to monitor the use of generic accounts.

Recommendation #3

We recommend the Department of Administration assure security documentation accurately reflects access controls.

Response: Concur. The Department's SABHRS Finance and Budget Bureau and Human Resources Information Services Bureau will review and update security documents as part of the 9.1 upgrade to ensure future documentation accurately reflects access controls.

I want to thank you and your staff for their hard work and careful examination during this audit. Our department always looks upon the audit process as an opportunity to improve our operations and performance.

The Department's Corrective Action Plan (CAP) is enclosed.

Sincerely,

Janet R. Kelly, Director
Department of Administration

Enclosure

Preliminary Response
Corrective Action Plan (CAP): Audit Report #11DP-04
SABHRS: Procurement Card Processing and Select Access Controls
Department of Administration
March 11, 2011

Agency	Recommendation #	Does this affect a federal program?	CFDA # (if previous YES)	Management View	CAP – Corrective Action Plan	Person responsible for CAP	Target Date
61010 DOA	**Recommendation #1** We recommend the Department of Administration limit all Human Resources Information Services programmer access to modify the SABHRS production environment by assigning access only when needed.	No		Concur	The Department's Human Resources Information Services Bureau will create a role for the bureau's programmers that will limit access to modify data, but still provide the access that is required on a regular basis to perform production payroll support.	Randy Morris (HRIS)	9/2/2011
61010 DOA	**Recommendation #2** We recommend the Department of Administration strengthen controls over user access by actively monitoring the use of generic system accounts.	No		Concur	The Department's Database Infrastructure, Design and Support Section will strengthen controls over user access and implement a process to monitor the use of generic accounts.	Dave Carlson (SITSD)	9/30/11
61010 DOA	**Recommendation #3** We recommend the Department of Administration assure security documentation accurately reflects access controls.	No		Concur	The Department's SABHRS Finance and Budget Bureau and Human Resources Information Services Bureau will review and update security documents as part of the 9.1 upgrade to ensure future documentation accurately reflects access controls.	Cheryl Grey (SFABB) and Randy Morris (HRIS)	9/2/2011 (SFABB) 12/30/2011 (HRIS)