REPORT OF

THE

STATE AUDITOR

Data Center
Governor's Office of Information Technology

Information Technology Audit
November 2008

LEGISLATIVE AUDIT COMMITTEE
2008 MEMBERS

Representative James Kerr
Chair

Representative Dianne Primavera
Vice-Chair

Senator Jim Isgar
Representative Rosemary Marshall
Representative Frank McNulty
Senator David Schultheis
Senator Jack Taylor
Senator Lois Tochtrop

Office of the State Auditor Staff

Sally Symanski
State Auditor

Dianne Ray
Deputy State Auditor

Jonathan Trull
Manjula Udeshi
Legislative Auditors

STATE OF COLORADO

Sally Symanski, CPA
State Auditor

OFFICE OF THE STATE AUDITOR
303.869.2800
FAX 303.869.3060

Legislative Services Building
200 East 14th Avenue
Denver, Colorado 80203-2211

November 3, 2008

Members of the Legislative Audit Committee:

This report contains the results of an information technology audit of the Governor's Office of Information Technology's Data Center. The audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The report presents our findings, conclusions, and recommendations, and the responses of the Governor's Office of Information Technology.

Sally Symanski

TABLE OF CONTENTS

SALLY SYMANSKI, CPA
State Auditor

Data Center
Governor's Office of Information Technology
Information Technology Audit
October 2008

Authority, Purpose, and Scope

This information technology audit was conducted pursuant to Section 2-3-103, C.R.S., which authorizes the Office of the State Auditor to conduct audits of all departments, institutions, and agencies of state government. The audit work, performed from May to August 2008, was conducted in accordance with generally accepted government auditing standards. Our audit was a follow-up audit to the 2007 SAS 70 review of the Governor's Office of Information Technology Data Center related to services provided to users of the Colorado Financial Reporting System (COFRS) and the Colorado Personnel and Payroll System (CPPS), related Employee Data Base (EMPL)/Human Resources Data Warehouse (HRDW) and Document Direct interfaces, and Data Center housing and hosting services. Our audit determined the implementation status of the 2007 recommendations by reviewing each of the areas covered in the prior report that resulted in a recommendation. We acknowledge the assistance and cooperation provided by the Governor's Office of Information Technology.

Overview

As of July 1, 2008, the Governor's Office of Information Technology (OIT) became officially responsible for the operations of the State's primary Data Center. The Data Center, which is also known as the General Government Computer Center, has 9,075 square feet of raised floor space containing the computer room, server farm, office space, service center, and print and distribution areas. The purpose of the Data Center is to perform services for state agencies who are its customers, including computer processing, maintaining system software, statewide telecommunications networking, server hosting, secure housing for customer-owned server and network equipment, and disaster recovery planning. The Data Center operates 24 hours per day, seven days a week, including holidays.

The Data Center is vital to state operations and houses critical applications that make it possible for state agencies to provide efficient and effective services to people living and conducting business in Colorado. For example, the Data Center houses the Driver's License Information System which is used to issue over 600,000 adult driver's licenses and State IDs per year. The Data Center also supports several statewide, financial applications used commonly by all state agencies, including COFRS, the accounting system for Colorado government and CPPS, the state employee personnel and payroll system.

OIT's Chief Operating Officer is responsible for Data Center operations and reports both administratively and operationally to the State Chief Information Officer. Day-to-day management of the Data Center is the responsibility of the Computing Services Manager. Approximately 60 full-time equivalents (FTEs) are directly involved with Data Center operations. The Data Center is cash-funded by user agencies which include more than 110 billable customers, such as state departments, institutions, and agencies. For Fiscal Year 2009, the Data Center received an appropriated spending authority of approximately $14.1 million and 94.3 full time equivalents (FTE) to provide computer services to state agencies.

Summary of Key Findings

During our 2008 follow-up we evaluated the actions taken by the Data Center to implement the recommendations listed in the 2007 SAS 70 Report. We assessed the status of the 2007 recommendations as *Implemented*, *Partially Implemented*, *Not Implemented*, or *Deferred* (i.e., implementation date proposed by the Data Center not yet reached). Overall, we found that the Data Center has not implemented the recommendations from the 2007 SAS 70 Report. Through our testing, we determined that the Data Center has only implemented 1 of the 13 recommendations from the 2007 Report. The key findings identified during the audit are:

- **System Access**. We found that the Data Center has not implemented a formal process to validate that agency Top Secret Security (TSS) administrators have either suspended or marked terminated employees' TSS Access IDs as not being recycled for a determined time period. More fundamentally, we found that the Data Center cannot identify all TSS Access IDs belonging to terminated users because (1) there is no unique or common identifier attached to TSS Access IDs; (2) some agency TSS administrators re-assign the Access IDs of terminated and transferred employees to new employees; and (3) employees with multiple TSS Access IDs issued by different agencies are not easily identified upon termination.

- **Customer Service Level Agreements.** We found that the Data Center failed to establish Service Level Agreements (SLAs) for new customers added during our audit period and continued to lack SLAs for the Data Center's existing customers. Without written SLAs for all customers, Data Center management cannot ensure that customer requirements are being met according to agreed-upon time lines. Additionally, critical services may not be provided (e.g., data sets not backed up) because the responsibilities of Data Center and agency staff are not clearly identified.

- **Management of new systems.** We found that Data Center staff are not using the server build checklist, as required, to document the steps completed and deviations from the standard server build process. Additionally, we found that the Data Center lacks a centralized inventory of servers hosted and housed at the Data Center, including important information about each server such as server location, date placed in service, and configuration details. Without the specific details about each server's configuration, it will

be difficult and time consuming for Data Center staff to properly build a new server in the event the old server fails.

- **Use of anti-virus on servers.** We found that anti-virus software had only been installed on 4 of the 42 Linux servers housed in the Data Center. For the Data Center's non-Linux based servers, we learned from Data Center management that the anti-virus software is not configured to scan periodically for virus infections. Active virus scans are an important control for protecting Data Center servers and the systems contained on those servers from infection. As such, all servers should be running properly updated anti-virus software configured to perform regular, active virus scanning.

- **Vendor documentation.** We found that the Data Center failed to implement the 2007 recommendation with regard to vendor performance reporting. Data Center procedures require that vendor performance reports, regardless of value, be completed mid-cycle for all contracts less than 13 weeks in duration and quarterly for all contracts greater than 13 weeks long. Through interviews and a review of existing documentation, we found that program managers are not completing vendor performance reports as required by Data Center procedures.

- **Management of data center visitors.** As part of our 2008 follow up, we again tested the Data Center and building reception staff's compliance with established visitor access control procedures and continued to find non-compliance. Specifically, we selected a sample of 15 days and obtained the visitor log for each day. We noted that approximately 5 percent of visitors did not sign out as required by Data Center procedures. We also observed that visitor access control procedures are not consistently followed by reception staff. For example, we observed one instance in which reception staff issued a visitor badge to a non-state employee without retaining photo identification. We observed another instance in which a visitor was allowed access to the Data Center's work space without being escorted by Data Center staff.

- **Management oversight.** Overall, we found that Data Center management has failed to act on prior audit recommendations and has not established a process to ensure that control activities and procedures are updated and designed to achieve management's objectives. During our 2008 follow-up, we again found that the Data Center's control descriptions are outdated and prior audit recommendations were not acted upon. Specifically, the Data Center failed to implement 12 of the 13 recommendations contained in the 2007 SAS 70 Report.

Our recommendations and the responses from the Governor's Office of Information Technology can be found in the Recommendation Locator and in the body of the report.

This page intentionally left blank.

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
1	15	Redesign the cover sheet to document staff's review of Top Secret security violation and profile change logs to include the exceptions found and the details of the follow-up actions taken as part of the review.	Agree	Implemented
2	18	Implement additional controls to ensure that Top Secret Security Access Identifications (Access IDs) belonging to terminated and transferred employees are identified and suspended by: (a) developing formal procedures agency TSS administrators must follow when setting up new TSS Access IDs and for handling TSS Access IDs belonging to terminated employees and transfers; (b) working with the Department of Personnel & Administration to add state employee ID numbers (EIDs) to each TSS Access ID user profile; (c) developing an automated program to match the CPPS listings of terminated and transferred employees to the names and EIDs associated with active TSS Access IDs and generating and distributing reports containing the names and TSS Access IDs of terminated and transferred employees; (d) utilizing the reports of terminated and transferred employees with TSS Access IDs to verify that agency TSS administrators have taken appropriate action and follow up as appropriate.	a. Agree b. Agree c. Agree d. Agree	a. January 2009 b. January 2010 c. October 2009 d. October 2009
3	21	Develop written Service Level Agreements (SLAs) for all customers identifying the agreed-upon services to be provided, the time requirements for those services, and performance measures the Data Center should meet. Provide a list of critical services with agreed-upon response times to operations personnel so customer requests can be prioritized appropriately.	Agree	Ongoing
4	22	Implement a server build configuration check-off sheet to be completed by the Data Center's hosted server staff and maintained in Data Center customer files or a centralized database. Inventory existing servers housed and hosted at the Data Center and maintain a central server file containing pertinent server information.	Agree	January 2009

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
5	24	Protect the Data Center's computing environment against virus infection by establishing project milestones for installing anti-virus software on the remaining Linux servers and configuring the anti-virus software on Data Center servers to periodically scan for viruses.	a. Agree b. Agree	a. December 2008 b. Implemented
6	26	Periodically review changes to all supported statewide applications to ensure that only authorized code is moved into production and assess budget and personnel resources to determine if the purchase and installation of version control software is feasible.	Agree	Implemented and Ongoing
7	28	Improve controls over system outages by: (a) requiring that all outages be reported to management; (b) discussing outages on a weekly basis with Data Center management; (c) designating a staff person as the outage administrator.	Agree	Implemented
8	29	Identify and train a backup person to ensure the Data Center's System Management Facility information is processed correctly and any problems are addressed timely in the absence of the primary staff member.	Agree	Implemented
9	31	Require Data Center staff to complete vendor performance reports as required by existing procedures and evaluate and modify the Data Center's procedures to incorporate the requirements of Senate Bill 07-228 for personal services contracts in excess of $100,000.	Agree	June 2009
10	32	Establish a written document retention policy and communicate this policy to all staff.	Agree	December 2008

RECOMMENDATION LOCATOR
Agency Addressed: Governor's Office of Information Technology

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date
11	34	Improve visitor access controls by: (a) implementing a process to designate responsibility to the employee host to ensure visitors successfully follow visitor control procedures; (b) including additional space on the log sheet for employees to sign acceptance of visitor arrival and document departure; (c) communicating and reinforcing visitor control procedures with all Data Center employees and building reception staff.	Agree	January 2009
12	35	As part of the three-year state data center restructuring process, re-engineer the power and signal cable ducts at the Data Center to provide separation and help ensure safety and performance.	Agree	January 2011
13	37	Ensure the Data Center's controls are accurate and complete and all outstanding audit recommendations are addressed by: (a) holding periodic meetings with Data Center management staff to discuss and update control activities; (b) periodically evaluating the effectiveness of current and proposed controls; (c) developing a plan with established milestones for implementing all audit recommendations; (d) requiring Data Center management to periodically report on the status of all outstanding recommendations to management staff within the Governor's Office of Information Technology.	Agree	January 2009 and Ongoing

This page intentionally left blank.

Overview

With passage of Senate Bill 08-155, the Division of Information Technologies Data Center (Data Center) within the Department of Personnel & Administration, formerly the Colorado Information Technology Services Data Center, was officially transferred to the Governor's Office of Information Technology (OIT) as of July 1, 2008. The Data Center, which is also known as the General Government Computer Center, is the result of the consolidation of several data centers over the last 30 years. The Data Center has 9,075 square feet of raised floor space containing the computer room, server farm, office space, service center, and print and distribution areas. The purpose of the Data Center is to perform services for state agencies who are its customers, including computer processing, maintaining system software, statewide telecommunications networking, server hosting, secure housing for customer-owned server and network equipment, and disaster recovery planning. The Data Center operates 24 hours per day, seven days a week, including holidays.

Data Center Services and Infrastructure

The Data Center houses the State's mainframe for traditional legacy systems. It also houses a growing number of servers for state agencies. Customers are able to utilize the physical infrastructure of the Data Center and manage their mid-range server platforms themselves or turn over varying levels of control and responsibility for their servers to the Data Center. The Data Center has expanded its services beyond mainframe processing by coordinating and facilitating the acquisition and support of server-class computing resources for its customers. Data Center customers can now receive client-server infrastructure support, web-based application development assistance, and new technology consulting. Customers continue to rely heavily on the Data Center to deliver traditional database processing, online access, tape and disk storage, and printing services.

The Data Center provides a full range of server support, ranging from server housing (providing floor space and power and network connections only) to full server hosting (complete operating system, hardware, and application package installation). For housed servers, Data Center staff are only responsible for ensuring the customer's server has sufficient power and network connections. State agency staff are responsible for all other activities. For hosted servers, Data Center staff are responsible for installing, configuring, and maintaining the server's operating system and agency specified applications. At the time of our audit, the Data Center hosted almost 240 servers and housed approximately 305 servers. To support its server hosting activities, the Data Center has recently invested in Storage Area Network

(SAN) technologies, enterprise-class backup solutions such as dedicated infrastructure and automated tape libraries, and physical support features such as Keyboard Video Mouse (KVM) switches, multiple-zoned power feeds, and protective racks and cabinets.

The Data Center is vital to state operations and houses critical applications that make it possible for state agencies to provide efficient and effective services to people living and conducting business in Colorado. For example, the Data Center houses the Driver's License Information System which is used to issue more than 600,000 adult driver's licenses and state IDs per year. Additionally, the Data Center supports several statewide, financial applications used commonly by all state agencies. These statewide applications are the Colorado Financial Reporting System (COFRS), the accounting system for Colorado government; the Financial Data Warehouse (FDW), a research and reporting tool for COFRS information; KRONOS, a timekeeping and leave-tracking system for state employees; Applicant Data System (ADS), a system for tracking state job applicants and the application process; the Colorado Personnel and Payroll System (CPPS), the state employee personnel and payroll system; the Human Resources Data Warehouse (HRDW), a research and reporting tool used to maintain current and historical employee information; and Document Direct, an online reporting repository for customer-identified mainframe reports. Data Center staff are responsible for managing these statewide financial applications, including updating, maintaining, modifying, and expanding the programs and administering related databases.

Data Center Management, Organization, and Funding

From March 2007 through June 30, 2008, the Data Center Director was responsible for Data Center operations and reported operationally to the State Chief Information Officer (CIO) and administratively to the Executive Director of the Department of Personnel & Administration. As of July 1, 2008, OIT's Chief Operating Officer (COO) is responsible for Data Center operations and reports both administratively and operationally to the CIO. Day-to-day management of the Data Center is the responsibility of the Computing Services Manager. Approximately 60 full-time equivalents (FTEs) are directly involved with Data Center operations. These FTE work within the following Data Center work groups or teams:

- **Computing Services Operating System (OS), Technical Support, and Software Support Teams.** These teams offer mainframe application hosting services and provide the platform where many of the statewide applications run. These groups maintain and manage the mainframe system and software and apply appropriate patches or upgrades to that environment.

- **Computer Operations Team.** This team maintains the mainframe hardware and peripherals, prints mainframe reports, provides mainframe tape handling, and monitors the mainframe system and batch processing. Computer Operations monitors the environmental health of the Data Center's computer room and works with Capitol Complex to maintain a computer-friendly environment. Computer Operations also provisions power from the power distribution unit for use by customers wishing to house servers at the Data Center. The Service Center, administratively located within the Computer Operations Team, is the single point of contact for the Data Center's customers. The Service Center provides service desk support, job scheduling and monitoring, and system monitoring for the Data Center and its customers.

- **Server Management Team.** This team provides and maintains the hardware and operating systems for agency-owned servers hosted at the Data Center.

- **Storage Management Group.** This group provides data storage and management services to customers using the Data Center's mainframe and hosted servers. Customers housing servers at the Data Center are responsible for their own data storage needs.

- **Technology Management Unit (TMU).** The TMU provides statewide application services for those applications used commonly among all state agencies.

- **Information Security Operations Center (ISOC).** ISOC is responsible for the overall security of the Data Center and the State Multi-Use Network (MNT). Responsibilities include perimeter security at the Internet gateway, mainframe security provisioning through the use of Top Secret Security (TSS) software, incident response, change processing through security variance requests, systems administration of security devices, and monitoring MNT traffic.

- **Business and Administrative Services Group.** This group provides business and administrative support services required to operate the Data Center. Services include budget preparation, accounting, personnel functions, word processing, and switchboard/receptionist services at the Data Center.

The Data Center is cash-funded by user agencies, which include more than 110 billable customers, such as state departments, institutions, and agencies. Billable items include computer processing time, data storage space, printing charges, and database support. Funds for these services are appropriated to each customer, with the Data Center receiving matching cash spending authority. For Fiscal Year 2009,

the Data Center received an appropriated spending authority of approximately $14.1 million and 94.3 full time equivalents (FTE) to provide computer services to state agencies.

Audit Scope and Methodology

In 2007, the Office of the State Auditor (OSA) contracted with BKD, LLP (BKD) to perform a SAS 70 review of the Data Center related to services provided to users of COFRS and CPPS, related Employee Data Base (EMPL)/Human Resources Data Warehouse (HRDW) and Document Direct interfaces, and Data Center housing and hosting activities. SAS 70 (Statement on Auditing Standards No. 70, *Service Organizations*) is a standard developed by the American Institute of Certified Public Accountants (AICPA). The purpose of a SAS 70 review is to allow a service organization like the Data Center to disclose its control activities and processes to its customers (state agencies) and customers' auditors (Office of the State Auditor). BKD's 2007 SAS 70 Report, when coupled with an understanding of controls in place at state agencies, allows the OSA to evaluate the State's system of internal control surrounding transactions processed through COFRS and CPPS.

This audit is a follow-up audit to BKD's 2007 SAS 70 Report, *Report on Controls Placed in Operation and Tests of Operating Effectiveness, Division of Information Technologies, Data Center and Technology Management Unit, Period from July 1, 2006 through June 30, 2007* (2007 Report). The purpose of this follow-up audit was to determine the implementation status of the 2007 recommendations. The follow-up reviewed each of the areas covered in the prior report that resulted in a recommendation, including control activities related to organization and relationships, human resources management, facility management, technology acquisition and management, management of third-party services, logical security, configuration management, and server housing and hosting. The 2007 Report made 13 recommendations that addressed concerns in these areas. The Data Center either agreed (11 recommendations) or partially agreed (2 recommendations) with all recommendations in the 2007 SAS 70 Report.

Data Center Controls

Chapter 1

As discussed in the Overview, the Data Center hosts the State's official accounting and financial reporting systems which are comprised of the Colorado Financial Reporting System (COFRS) and the Colorado Personnel and Payroll System (CPPS). As a service organization, the Data Center is responsible for designing and putting in place data processing controls to provide reasonable, but not absolute, assurance over such things as the following:

- Protection of data files, programs, and equipment against loss or destruction
- Prevention of unauthorized access to and use of data records, programs, and equipment
- Proper handling of input and output data records
- Reliable processing of data records

In 2007, the Office of the State Auditor (OSA) contracted with BKD, LLP (BKD) to perform a SAS 70 review of the Data Center related to services provided to users of COFRS and CPPS, related Employee Data Base (EMPL)/Human Resources Data Warehouse (HRDW) and Document Direct interfaces, and Data Center housing and hosting activities. Overall, BKD found that the Data Center's description of controls presented fairly, in all material aspects, the relevant aspects of the Data Center's controls that had been placed in operation as of June 30, 2007. Additionally, BKD found that the controls were suitably designed to provide reasonable assurance that the Data Center's specified control objectives would be achieved if the described controls were complied with satisfactorily and state agencies applied the application controls at the agency level contemplated in the design of the Data Center's controls. However, BKD identified control deficiencies in several areas. BKD also identified several areas in which control objectives and activities were operating as intended, but industry best practices were not being followed. In total, BKD made 13 recommendations to the Data Center. The Data Center either agreed or partially agreed with all recommendations.

During our 2008 follow-up we evaluated the actions taken by the Data Center to implement the recommendations listed in the 2007 Report. We assessed the status of the 2007 recommendations as *Implemented*, *Partially Implemented*, *Not Implemented*, or *Deferred* (implementation date proposed by Data Center not yet

reached). If we determined that a prior recommendation was not implemented or partially implemented, we then evaluated compensating controls placed in operation by the Data Center to determine if the previously identified control deficiency still existed. Overall, as discussed below, we found that the Data Center has not implemented the recommendations from the 2007 Report. Through our testing, we determined that the Data Center has only implemented 1 of the 13 recommendations from the 2007 Report.

System Access

A cornerstone of information security is to control access to computer resources (data files, software, production libraries, and computer-related facilities and equipment). The following two sections discuss improvements the Data Center should make to better control access to its computing environment.

Review of Top Secret Security Violation Logs

Mainframe user access as well as access to data sets is controlled through Top Secret, a commercially developed access control software. Top Secret logs security violations and changes to a user's security profile. The Data Center's Mainframe Security Administrator is required to review the security violation logs weekly and the security profile change logs monthly. Suspicious activities are to be identified and investigated. In the 2007 Report BKD found that the Data Center lacked a formal process for documenting the weekly and monthly reviews of violation and security profile change logs. As such, Data Center management could not determine with certainty that the reviews were being conducted. This could allow violations or inappropriate profile changes to occur undetected.

BKD recommended that the Data Center implement a standard procedure for documenting both the weekly and monthly reviews of the security violation logs and the security profile change logs within Top Secret (2007 Report Recommendation No. 1). BKD suggested that the Data Center create a cover sheet which would include the report name, date of the report, printed name of reviewer, signature of reviewer, date the review was completed, and any follow-up actions taken. The Data Center agreed to implement the recommendation by November 30, 2007, by creating a cover sheet to include the report name and date, the name and signature of the reviewer, the review date, exceptions found, and follow-up actions taken.

2008 Auditor Assessment: *Implemented; 2008 Recommendation.*

During our 2008 follow-up we found that the Data Center created and began using a cover sheet to document the Mainframe Security Administrator's review of the security violation and security profile change logs. The cover sheet is completed electronically and includes the report name, date of the report, date the review was completed, and the electronic initials of the reviewer. We selected a random sample of 15 instances when Data Center staff were required to review security violation logs. We found a cover sheet documenting that each of those logs had been reviewed. We then selected a random sample of two instances when Data Center staff were required to review security profile change logs and also found a cover sheet documenting that each of those logs had been reviewed.

Although the Data Center implemented this recommendation, we believe more needs to be done to identify improper access. Specifically, the Data Center's cover sheet does not include the exceptions found and follow-up actions taken by staff. Without these components, Data Center management cannot determine with certainty that appropriate follow-up actions are taken when violations and unauthorized profile changes are identified.

Recommendation No. 1:

The Governor's Office of Information Technology should redesign the cover sheet used by staff to document their review of Top Secret security violation and profile change logs to include the exceptions found and the details of the follow-up actions taken as part of the review.

Governor's Office of Information Technology Response:

Agree. Implementation date: Implemented.

The Top Secret security violation instructions and cover sheet were redesigned and now include the exceptions found and the follow-up actions taken by staff.

Review of Top Secret Access for Terminated Employees

Best practices and State Cyber Security Policies require that agencies have a process in place to identify and correctly address changes in access rights for system users with changes in employment status. During the 2007 SAS 70, BKD found that there was not a clear procedure for identifying and tracking employees who had a change in status, such as promotions or transfers, but were not terminated. BKD recommended that the Data Center create an exception report showing terminated employees and identifying all individuals who were not terminated but had a change in employment status. Additionally, BKD recommended that the Data Center implement a formal process to validate that terminated employees' Top Secret Security Access Identifications (TSS Access IDs) are either suspended or marked as not to be recycled for a determined time period, or remain active due to a status change (2007 Report Recommendation No. 2). The Data Center agreed to implement the recommendation by December 31, 2007.

2008 Auditor Assessment: *Partially Implemented*.

We found that the Data Center made some progress in implementing this recommendation by generating weekly termination reports listing all state employees terminated or transferred during the week. The weekly reports identify the status of each employee listed as either "T" for terminated or "O" for transferred or other status change (e.g., full-time employee goes on leave). The Mainframe Security Administrator reviews the terminated reports and manually compares the list of terminated and transferred employees to the list of active users in Top Secret. For those terminated and transferred employees with an active TSS Access ID or mainframe ID, the Mainframe Security Administrator notifies the corresponding agencies' TSS administrators. It is then the responsibility of the agencies' TSS administrators to suspend the accounts. Top Secret automatically deletes the suspended accounts after six months.

We assessed this prior recommendation as partially implemented for two reasons. First, the Data Center has not implemented a formal process to validate that agency TSS administrators have either suspended or marked terminated employees' TSS Access IDs as not being recycled for a determined time period, or left the IDs active due to a status change. Second, and more fundamentally, we found that the Data Center cannot identify all TSS Access IDs belonging to terminated users for the following reasons:

- There is no unique or common identifier (State Employee ID or Social Security Number) attached to TSS Access IDs. As such, mainframe users cannot be accurately cross referenced with terminated users in CPPS (the State's personnel system). Currently, Data Center staff manually match the names of terminated employees in CPPS to the names attached to the TSS Access IDs. This process is ineffective because in some cases employees have identical or similar names. Additionally, the agency TSS administrators often abbreviate or shorten the names of employees when establishing their TSS Access ID (e.g., "Bob" is entered instead of "Robert"). Also, upon marriage, a state employee may change her name or have it updated in CPPS, but this information is not typically updated in Top Secret. As such, the name attached to the TSS Access ID may not match the name of the terminated employee in CPPS.

- Some agency TSS administrators re-assign the Access IDs of terminated and transferred employees to new employees. Re-assigning Access IDs makes it difficult to trace historical events associated with the recycled ID and can make it difficult to ensure all Access IDs belonging to terminated employees are identified and suspended. Additionally, recycling Access IDs increases the risk that the new user may inherit access privileges that are in excess of their job responsibilities.

- We also found that some state employees require multiple TSS Access IDs issued by different agencies. For example, some employees at the Department of Human Services require TSS Access IDs from the Department of Revenue to verify the lawful presence status of public assistance claimants in the Driver's License Information System. In addition to this access, these employees also require a TSS Access ID from the Department of Human Services to process public assistance payments. This is problematic because only the agency for which the employee currently works receives the termination notification. As such, the TSS Access IDs established by the other state agencies will likely remain active.

The Data Center needs to take several steps to ensure all TSS Access IDs belonging to terminated employees are identified and suspended. First, the Data Center should develop formal procedures specifying how agency TSS administrators are to set up new TSS Access IDs and handle TSS Access IDs belonging to terminated and transferred employees. At a minimum, the procedures should require that each new TSS Access ID includes the user's full name as listed in CPPS. The policy should also require that TSS Access IDs belonging to terminated and transferred employees be suspended and not recycled. The Data Center should distribute the policy to the

agency TSS administrators and provide training as appropriate. Second, the Data Center should work to add state employee ID numbers (EIDs) to each TSS Access ID user profile. This will allow for a more accurate match between TSS Access IDs and information contained in CPPS. Third, the Data Center should develop an automated program to match the CPPS listings of terminated and transferred employees to the names and EIDs, as available, associated with active TSS Access IDs. A report containing the TSS Access IDs belonging to terminated and transferred employees should then be provided to the agency TSS administrators for suspension. Finally, Data Center staff should utilize the reports to verify that the agency TSS administrators have taken appropriate action in a timely manner and follow up as appropriate.

Recommendation No. 2:

The Governor's Office of Information Technology should implement additional controls to ensure that the Top Secret Security Access Identifications (TSS Access IDs) belonging to terminated and transferred employees are identified and suspended by:

a. Developing formal procedures agency TSS administrators are required to follow when setting up new TSS Access IDs and for handling TSS Access IDs belonging to terminated employees and transfers. At a minimum, the procedures should require that new TSS Access IDs include the user's full name as included in CPPS and that the TSS Access IDs belonging to terminated and transferred employees be suspended and not recycled.

b. As time and funding permit, working with the Department of Personnel & Administration to add state employee ID numbers (EIDs) to each TSS Access ID user profile.

c. Developing an automated program to match the CPPS listings of terminated and transferred employees to the names and EIDs, as available, associated with active TSS Access IDs. A report containing the names and TSS Access IDs of terminated and transferred employees should then be distributed to all agency TSS administrators for suspension.

d. Utilizing the reports of terminated and transferred employees with TSS Access IDs to verify that agency TSS administrators have taken appropriate action in a timely manner and follow up as appropriate.

Governor's Office of Information Technology Response:

a. Agree. Implementation date: January 2009. Staff are developing a procedure which will establish requirements for agencies to suspend, rather than recycle, IDs belonging to terminated and transferred employees. This process will be reviewed during TSS administrator training, which is scheduled to be held in late December. Further, the Governor's Office of Information Technology will provide guidance to agencies regarding entering a user's full name from CPPS in the TSS Access IDs.

b. Agree. Implementation date: January 2010. The Governor's Office of Information Technology will work with the Department of Personnel & Administration to add EIDs to TSS Access ID user profiles. Once OIT receives the necessary information regarding names and associated EIDs, such information will be disseminated to the agency TSS administrators for entry into the TSS Access ID user profiles. It is anticipated that OIT will begin this project in February 2009.

c/d. Agree. Implementation date: October 2009. Staff are developing an automated report for matching terminated and transferred employees to TSS Access IDs. Once this report has been finalized, it will be forwarded to the TSS administrators for suspension of the identified user IDs. The Governor's Office of Information Technology staff will then follow up to ensure that appropriate action was taken. Until the automated report is complete, OIT will continue to use its current manual process in determining if Top Secret access for terminated and transferred employees has been suspended.

Management of Information Systems

The following six sections discuss the Data Center's day-to-day management of its computing resources and include recommendations for documenting and monitoring customer service levels and server configurations, detecting computer viruses, managing change, and monitoring and managing system performance.

Customer Service Level Agreements

The Data Center provides different services to state agency customers, including services related to COFRS, CPPS, and technology housing and hosting services. For the housing and hosting services, there are many variations in service expectations among Data Center customers. Service Level Agreements (SLAs) are written agreements between a service organization and its customers specifying acceptable levels of performance. SLAs are necessary to ensure the Data Center's housing and hosting services meet state agencies' needs and expectations and help guide Data Center staff in setting work priorities. Although the Data Center made some improvements in this area based on prior audit recommendations in 2005 and 2001, BKD continued to find problems. Specifically, BKD found that no signed SLAs were available for new services added during State Fiscal Year 2007. BKD also found that the documentation of SLAs for existing Data Center customers could be improved to provide a clearer indication of the services to be provided, clarify residual user responsibilities, and assist in SLA performance assessments.

In the 2007 Report, BKD recommended that the Data Center ensure that current, signed SLAs are on file and tracked for all Data Center server housing and hosting customers. SLAs should clearly define services to be provided by the Data Center, responsibilities of the user, and performance measures that the Data Center should meet (2007 Report Recommendation No. 3).

2008 Auditor Assessment: *Deferred.*

The Data Center agreed to implement the recommendation by September 30, 2008, by describing and tracking its services in an actionable "Service Catalog." Service Catalog is a commercially developed application that can be used to provide standardized services; initiate, assign, track, and document user requests; document agreed upon services and response times; and perform billing where appropriate. During our 2008 follow-up, we found that the Data Center failed to establish SLAs for new customers because it does not have sufficient licenses to utilize Service Catalog. Additionally, we continued to find that SLAs or similar agreements do not exist for the Data Center's existing customers. Data Center management reports that implementation of Service Catalog is cost prohibitive and as such, the 2007 recommendation will not be implemented by September 30, 2008. The Data Center reports that it is currently investigating alternative automated solutions.

Without written SLAs for all customers, Data Center management cannot ensure that customer requirements are being met according to agreed-upon time lines. Additionally, critical services may not be provided (e.g., data sets

not backed up) because the responsibilities of Data Center and agency staff are not clearly identified. As such, we recommend that the Data Center implement an alternative, manual process for documenting the agreed-upon service level expectations of its customers until a more automated solution can be identified. Additionally, once SLAs are established for all customers, Data Center management should provide Data Center operations staff with a list of critical services with agreed upon response times. Operations staff can then utilize the list to prioritize their work.

Recommendation No. 3:

The Governor's Office of Information Technology should develop written Service Level Agreements (SLAs) for all customers specifically identifying the agreed-upon services to be provided, the time requirements for those services, and performance measures the Data Center should meet. The Data Center should provide operations personnel a list of critical services with agreed upon response times so that customer requests can be prioritized appropriately.

Governor's Office of Information Technology Response:

Agree. Implementation date: Ongoing for SLA development; Implemented for tracking commitments in SLAs. The Governor's Office of Information Technology is working on developing Service Level Agreements for all of its current customers and will process SLAs for its new customers. Additionally, OIT instituted a process to track conformance to commitments expressed in all SLAs.

Management of New Systems

As discussed in the overview, the Data Center hosts almost 240 servers. For these hosted servers, Data Center staff are responsible for installing, configuring, and maintaining the server's operating system. Server configuration refers to the methodical process of installing an operating system and selecting the specific system options necessary to securely and effectively utilize the server for computer processing. Servers should be configured to meet the business needs of the user, and server configurations can vary dramatically. It is important that detailed documentation be maintained on the original configuration in case a server needs to be rebuilt or reconfigured. Failure to document the completion of the original build process can result in the omission of key steps during reconfiguration that are

necessary to ensure the hosted server's implementation meets Data Center standards and customer specifications.

During the 2007 SAS 70, BKD found that the Data Center's hosted server team does not maintain the documentation of the hosted server build process. Specifically, BKD noted that although the Data Center's server team members use a "Server Build Document" to guide them through the process of deploying a new server and assisting the customer through the installation of the agency's application on its server, staff do not document the server build steps. In the 2007 Report BKD recommended that the Data Center implement a server build configuration check-off sheet to be completed by the Data Center's hosted server staff. BKD further recommended that the check off sheet be maintained in the appropriate Data Center customer file for each system (2007 Report Recommendation No. 7). The Data Center agreed to implement the recommendation by March 1, 2008, by documenting the server build tasks completed, the person completing the tasks, and variations from the normal build process. The Data Center agreed to save the check-off sheets for future reference.

2008 Auditor Assessment: *Not Implemented.*

During our 2008 follow-up we learned that the Data Center has not taken steps to implement this recommendation. As discussed in the 2007 Report, Data Center staff continue to utilize a server build checklist when configuring a new server or assisting customers. However, as identified in 2007, we again found that Data Center staff are not using the checklist to document the steps completed and the deviations from the standard server build process. Additionally, we found that the Data Center lacks a centralized inventory of the servers hosted and housed at the Data Center, including important information about each server such as server location, date placed in service, and configuration details. Without the specific details about each server's configuration, it will be difficult and time consuming for Data Center staff to properly build a new server in the event the old server fails.

Recommendation No. 4:

The Governor's Office of Information Technology should implement a server build configuration check-off sheet to be completed by the Data Center's hosted server staff. The completed check-off sheet, along with other pertinent server information, should be maintained in Data Center customer files or a centralized database. The Data Center should also inventory the existing servers housed and hosted at the Data

Center and maintain a central server file containing pertinent information such as configuration details, date placed in service, and server location.

Governor's Office of Information Technology Response:

Agree. Implementation date: January 2009. A check-off sheet was developed and will be used for all new server builds. Data Center staff are in the process of developing central server files for all the servers hosted and housed. The files will contain information such as configuration details, date placed into service, and server location.

Use of Anti-virus on Servers

All servers should be running properly updated anti-virus software configured to perform regular, active virus scanning. During the 2007 SAS 70, BKD observed that the active virus scans were disabled on the Data Center's servers. Data Center staff reported that the virus scans were disabled because they could result in slower server performance during the scan. BKD further noted that the Linux servers were not utilizing any form of anti-virus software because it is commonly thought within the industry that a properly configured Linux system is more resistant to attack than servers running other operating systems. BKD argued, however, that an improperly configured Linux system could make these servers vulnerable to attack. Therefore, in the 2007 Report BKD recommended that the Data Center consider the purchase and installation of anti-virus software for the Linux servers, and that all servers be set to periodically scan for virus infections (2007 Report Recommendation No. 6). By March 1, 2008, the Data Center agreed to implement the recommendation by installing anti-virus software on the Linux servers and scheduling regular virus scans on all servers located at the Data Center.

2008 Auditor Assessment: *Partially Implemented.*

During the 2008 follow-up we learned that the Data Center purchased anti-virus software for the 42 Linux servers housed in the Data Center. As of August 2008, however, the anti-virus software had only been installed on four of the Linux servers. We reviewed the configuration of the anti-virus software installed on the four Linux servers and determined that the software had been configured according to industry best practices.

For the Data Center's non-Linux based servers, we learned from Data Center management that the anti-virus software is still not configured to periodically

scan for virus infections. Data Center staff continue to express concern that actively scanning for viruses will negatively impact server performance. Although we understand the Data Center's argument, active virus scans are an important control for protecting Data Center servers and the systems contained on those servers from infection. Active virus scans are also required by State Cyber Security Policies and industry best practices. It should be noted that the Data Center is organizationally located in the Office of Information Technology, which is responsible for State Cyber Security Policies. We recommend that the Data Center comply with State Cyber Security Policies and configure its anti-virus software to periodically conduct active virus scans on all Data Center servers. To mitigate potential performance problems, the Data Center should configure the anti-virus software to run scans on non-peak days and times and allocate server resources between the anti-virus software and other applications depending upon task priority levels.

Recommendation No. 5:

The Governor's Office of Information Technology should work with Data Center management to protect the computing environment against virus infection by:

a. Establishing project milestones for installing anti-virus software on the remaining Linux servers.

b. Configuring the anti-virus software on Data Center servers to periodically scan for virus infections. Consideration should be given to running the scans during non-peak times.

Governor's Office of Information Technology Response:

a. Agree. Implementation date: December 2008. Staff have completed installing anti-virus software on 95 percent of the Linux servers. The remaining servers will be complete by December 2008.

b. Agree. Implementation date: Implemented. All servers now have virus protection on-demand scanning enabled so that files opened or being added to the machine get scanned immediately.

Version Control Software

Change control is the process of controlling modifications to hardware, software, and documentation to ensure information systems are consistently available to users and the system and data contained are protected against improper use or unintended failure before, during, and after system implementation. The Data Center is required by State Cyber Security Policies to have processes and procedures in place to control changes to the applications it manages and supports. Version control software is an automated tool that assists in overall change management, code and version management, and contributes to management of segregation of duties and testing of changes. If large and complex systems are managed without version control software, unauthorized changes to software could occur, and it becomes difficult to track the source of problems resulting from system changes.

The April 2002 SAS 70 Review of the Data Center recommended that version control software for COFRS be considered. The Data Center reported that it considered the purchase and use of automated version control software for COFRS, but there was not sufficient operating or full-time equivalent (FTE) budget to accomplish this. Data Center management also felt that, for the relatively few code changes that occur on a system as mature as COFRS, the return on investment would be questionable even if the budget were available. Hence, Data Center management decided not to undertake any further actions.

During the 2007 SAS 70, BKD again reviewed the Data Center's change control process and indicated that version control software was necessary due to the large and complex systems managed by the Data Center. BKD recommended that the Data Center reconsider the use of version control software for application changes to all supported systems, not just COFRS (2007 Report Recommendation No. 12). The Data Center partially agreed with the recommendation and responded that although it agreed that using version control software would be beneficial, funds and FTE were still not available to implement the recommendation.

2008 Auditor assessment: *Not Implemented.*

During our 2008 follow-up, Data Center management again reported that funds and FTE do not exist to implement recommendations related to purchasing and using version control software. As discussed earlier, version control software is a tool that helps organizations control and track changes to critical applications like COFRS. In the absence of version control software, the Data Center needs a combination of manual and technical controls to protect the integrity of program source code.

As part of our 2008 follow-up, we reviewed the Data Center's change control procedures related specifically to COFRS. We found that the Data Center's controls adequately limit access to COFRS source code, prevent programmers from making changes in or migrating code to production, require an independent review and testing of programmer changes, and require employees other than programmers to migrate changes into production. However, as part of our testing, we identified one area of weakness that still exists. Specifically, the three Data Center staff that have system access privileges to move the programmers' changes into production could make unauthorized changes to COFRS source code without being detected. To determine if this had occurred, we obtained a list of source code changes that had been moved into production during Fiscal Year 2008 and cross-referenced the changes to those authorized by Data Center management. We did not identify any relevant exceptions. However, to mitigate this risk, we recommend that a Data Center staff person, independent of those staff responsible for migrating changes into production, periodically conduct a review of all COFRS changes to ensure that only authorized code was moved into production. Adequate controls over COFRS are important because all state warrants are issued through the system. Similar procedures should be implemented by the Data Center for the other statewide applications it supports, such as CPPS, the state employee personnel and payroll system. Additionally, we recommend that the Data Center periodically assess its budget and personnel resources to determine if the purchase and installation of version control software is feasible.

Recommendation No. 6:

The Governor's Office of Information Technology should require Data Center management to periodically review changes to all supported statewide applications to ensure that only authorized code is moved into production. Additionally, the Governor's Office of Information Technology should periodically assess budget and personnel resources to determine if the purchase and installation of version control software at the Data Center is feasible.

Governor's Office of Information Technology Response:

Agree. Implementation date: Implemented and ongoing. The Governor's Office of Information Technology will ensure that code changes to statewide applications are periodically reviewed by management. A process has already been developed for COFRS which includes cross-referencing a list

of changes implemented in the production environment with the list of changes authorized by management for implementation. This process will be completed on a quarterly basis. For CPPS, the current mainframe version control software does not work well with the CPPS code and would require extensive modification to CPPS. As an alternative, CPPS Source and Copy libraries are restricted for update to two individuals. One primary and one backup person only are allowed access to the production libraries for Source and Load module migration. The HR system manager reviews the changes that are placed into production monthly.

The Governor's Office of Information Technology will continue to assess whether the purchase of version control software is cost effective.

Reporting of System Outages

Data Center procedures require that significant IT events or failures be reported to senior management. However, all such events or failures, regardless of significance, should be tracked and reported to Data Center management. During 2007 testing of outage reporting, BKD noted that significant IT events and failures are reported to management due to their critical nature. However, BKD also found that some of the Data Center's groups failed to report an outage to the outage administrator because the groups determined the outage was not severe enough to be formally reported. Such selective reporting can distort the effectiveness of current controls and mask significant trends. BKD recommended that the Data Center re-emphasize the outage reporting process and ensure that all outages are reported regardless of their severity. BKD also recommended that outages be included as an agenda item to be discussed at management meetings to ensure that management is made aware of all events regardless of their perceived severity (2007 Report Recommendation No. 8). The Data Center agreed to implement the 2007 recommendation by March 1, 2008.

2008 Auditor Assessment: *Not Implemented.*

The Data Center failed to take appropriate actions to implement this recommendation. All outages, regardless of severity, should be reported to the outage administrator. However, during our 2008 follow-up, we learned that the person serving as the outage administrator was reassigned in September 2007, and a replacement was never designated. In the absence of a designated outage administrator, we found that outage reports were not consistently documented and reported to Data Center management. The lack of adequate controls related to the reporting, documentation, and monitoring of outages could result in failure to prevent significant system downtime and disruption. As such, we reiterate the 2007 Report recommendation and also

recommend that the Data Center immediately designate a staff person as the outage administrator to collect, document, and monitor all Data Center outage reports.

Recommendation No. 7:

The Governor's Office of Information Technology should improve controls over system outages by:

a. Requiring that all outages be reported to management.

b. Discussing outages on a weekly basis with Data Center management.

c. Designating a staff person as the outage administrator.

Governor's Office of Information Technology Response:

Agree. Implementation date: Implemented. OIT made several changes to its system outage process including designating an outage administrator, re-emphasizing to Data Center staff what constitutes an outage, developing an outage report that is provided to the Chief Operations Officer on a monthly basis, and discussing outages at weekly staff meetings. The staff meeting discussions include who the outage impacted, how it was resolved, and lessons learned to help prevent and address future outages.

Review of System Management Facility Information

System Management Facility (SMF) is a component of the IBM z/OS operating system used to generate standardized mainframe performance information, such as input/output activity, network activity, software usage, error conditions, and processor utilization. Data Center procedures require that staff review SMF information regularly and document the review. In 2007, BKD noted that Data Center technical support staff review SMF information on a daily basis to monitor system performance and usage and ensure the system infrastructure is appropriate to need. However, BKD found that the staff do not document their reviews. BKD further noted that there is no backup employee who could perform the review in absence of the technical support manager. In the 2007 Report, BKD recommended that the Data Center implement a procedure to document the review of SMF

information and train another employee as a backup to ensure that the review is performed on a timely basis in case the regular reviewer is not available (2007 Report Recommendation No. 9). The Data Center agreed to implement the recommendation by March 1, 2008.

2008 Auditor Assessment: *Partially Implemented*.

During the 2008 follow-up review we found that the Data Center made significant progress in implementing this recommendation. Specifically, we found that the Data Center has drafted a standard operating procedure, awaiting management approval, detailing how SMF information is to be generated and reviewed. We reviewed the Data Center's current process for generating and reviewing SMF information and found that it meets industry best practices. For the mainframe, SMF information is automatically reviewed and verified by the programs that collect and process the data. If the SMF information fails to process correctly, an error message is automatically sent to a designated technical support staff person. We assessed this recommendation as partially implemented because the Data Center has not designated and trained an employee as back up staff in case the primary staff person receiving the error message is absent. To further test SMF processing, we selected a sample of 15 continuous days and noted that SMF data were processed successfully for all 15 days. Once SMF information is processed, system performance, usage, billing, and tape load reports are automatically placed on the Data Center's shared drive and routinely reviewed by appropriate Data Center staff.

Recommendation No. 8:

The Governor's Office of Information Technology should identify and train a backup person to ensure the Data Center's SMF information is processed correctly and any problems are addressed timely in the absence of the primary staff member.

Governor's Office of Information Technology Response:

Agree. Implementation date: Implemented. The OIT technical support staff are now trained in producing and analyzing System Management Facility reports.

Documentation Requirements

The following two sections discuss the Data Center's responsibilities and practices for maintaining sufficient documentation to comply with its procedures and state requirements.

New Hire and Vendor Documentation

Data Center staff complete new hire checklists and vendor performance reports to ensure compliance with personnel rules and the Data Center's standard operating procedures. During the 2007 SAS 70, BKD noted that the Data Center misfiled two of the new hire checklists tested, making it difficult to locate the checklists. BKD also found that one of the two sampled vendor performance reports was not completed. As such, BKD recommended that the Data Center establish a review process to ensure that new hire checklists are properly filed and vendor performance reports are completed in a timely manner (2007 Report Recommendation No. 4). The Data Center agreed to implement the recommendation by December 31, 2007.

> **2008 Auditor Assessment:** *New Hire checklist - Implemented. Vendor Performance Management - Not Implemented.*
>
> During our 2008 follow-up we determined that the Data Center implemented the prior year recommendation with regard to the completion and filing of new hire checklists. Specifically, we identified the eight employees hired by the Data Center since the December 31, 2007 implementation date and obtained the new hire checklists. All eight of the new hire checklists were completed and filed as required by Data Center procedures.
>
> With regard to vendor performance reports, however, we found that the Data Center has not implemented the 2007 Report recommendation. Data Center procedures require that vendor performance reports, regardless of value, be completed mid-cycle for all contracts less than 13 weeks in duration and quarterly for all contracts greater than 13 weeks long. The vendor performance reports are to be completed by the responsible manager and submitted to the Data Center's financial director. Through interviews and a review of existing documentation, we found that program managers are not completing vendor performance reports as required by Data Center procedures.
>
> Data Center management reports that they have not enforced existing procedures and have delayed implementation of this recommendation with regard to vendor performance until the centralized-contract-management

system required by Senate Bill 07-228 is completed. Senate Bill 07-228 requires that state agencies evaluate the performance of vendors at the conclusion of personal services contracts in excess of $100,000. The evaluation must measure the performance of the vendor in meeting contractual requirements relating to quality, cost, and deadlines. Completed evaluations must be provided to the vendor for comment and then added to the centralized-contract-management system. The centralized-contract-management system is scheduled to be completed by the end of Fiscal Year 2009.

The passage of Senate Bill 07-228 does not remove the Data Center's responsibility for implementing BKD's prior audit recommendation or complying with existing procedures. It is important to note that Senate Bill 07-228 only impacts the Data Center's procedures with regard to personal services contracts in excess of $100,000. As such, the Data Center needs to enforce its existing procedure regarding the completion of vendor performance evaluations and evaluate and modify the procedure to incorporate the additional requirements imposed by Senate Bill 07-228 for personal services contracts in excess of $100,000.

Recommendation No. 9:

The Governor's Office of Information Technology should require Data Center staff to complete vendor performance reports as required by existing procedures and evaluate and modify the Data Center's procedure to incorporate the requirements of Senate Bill 07-228 for personal services contracts in excess of $100,000.

Governor's Office of Information Technology Response:

Agree. Implementation date: June 2009. The Governor's Office of Information Technology is reviewing its contract-related processes and procedures. Through this review, OIT will determine if the current requirements for completing vendor performance reports are appropriate and revise such procedures if determined necessary. This will include incorporating the necessary processes to ensure compliance with SB07-228. Further, OIT will develop a process for monitoring and enforcing completion of vendor performance reporting in accordance with the established protocols.

Document Retention Policies

During the 2007 SAS 70, BKD found that the Data Center did not maintain all of the supporting documents necessary to document its performance of all Data Center control activities for the entire fiscal year. To form a proper conclusion as to the operating effectiveness of a control activity, it is crucial to have adequate data from which to test throughout the audit period (i.e., State Fiscal Year). BKD recommended that the Data Center review its document retention policies and require that documents demonstrating performance of control activities be retained for at least one year (2007 Report Recommendation No. 11). By December 1, 2007, the Data Center agreed to implement the recommendation by reviewing document retention practices against controls and either implementing a minimum 15 to 18 month retention period for all documents or only retaining the documentation required for the next audit.

2008 Auditor Assessment: *Not Implemented.*

During our 2008 follow-up we found that no specific actions were taken by the Data Center to implement this recommendation. Specifically, Data Center management has not identified or standardized the document retention requirements for the different control activities at the Data Center or communicated retention requirements to staff. A proper conclusion of control activity operating effectiveness cannot be reached unless adequate supporting documentation is maintained by the responsible staff members. Additionally, Data Center management should be periodically reviewing documentation of control activities to ensure controls are operating effectively.

Recommendation No. 10:

The Governor's Office of Information Technology should establish a written document retention policy and communicate this policy to all staff.

Governor's Office of Information Technology Response:

Agree. Implementation date: December 2008. OIT will establish a written document retention policy regarding control activities and communicate it to all staff.

Physical and Environmental Controls

Physical and environmental controls are necessary to protect computing resources from threats such as theft, sabotage, fire, corrosion, and unintentional damage. The following two sections discuss improvements the Data Center should make to its physical and environmental controls.

Management of Data Center Visitors

During the 2007 SAS 70, BKD found that procedures for checking visitors in and out of the Data Center were not always followed. Specifically, BKD reviewed the visitor sign-in logs and noted that 4 of 67 visitor entries (6 percent) sampled did not indicate the visitor signed out. BKD recommended that the Data Center implement a process to designate responsibility to the employee host to ensure visitors successfully follow all visitor control procedures, including the return of badges and signing out of the visitor log after hours (2007 Report Recommendation No. 5). BKD also recommended that the Data Center add spaces to the log sheet for employees to sign acceptance of visitor arrival and document departure. The Data Center agreed to implement the recommendation by December 31, 2007, by modifying the visitor control log to capture host employee acknowledgment of visitor sign in and out information and by reinforcing visitor control procedures with Data Center managers.

2008 Auditor Assessment: *Not Implemented.*

The Data Center failed to implement the 2007 Report recommendation. Specifically, Data Center management has not communicated the requirement that Data Center employees are responsible for ensuring visitors follow visitor control procedures. Additionally, the Data Center did not add spaces to the visitor log sheet for employees to sign acceptance of visitor arrival and document departure.

As part of our 2008 follow-up, we again tested the Data Center and building reception staff's compliance with established visitor access control procedures and continued to find non-compliance. Specifically, we selected a sample of 15 days and obtained the visitor log for each day. We noted that approximately 5 percent of visitors (40 of 778 visitor log entries) did not sign out as required by Data Center procedures. We also observed that visitor access control procedures are not consistently followed by reception staff. For example, we observed one instance in which reception staff issued a visitor badge to a non-state employee without retaining photo identification. We observed another instance when reception staff failed to issue a visitor

badge when required, and another instance when a visitor was allowed access to the Data Center's work space without being escorted by Data Center staff.

Physical security is an important component of the Data Center's control framework. Logical access controls are ineffective if unauthorized people can gain physical access to critical systems. Therefore, we reiterate the 2007 Report recommendation and further recommend that the Data Center communicate and reinforce existing visitor control procedures with Data Center employees and building reception staff.

Recommendation No. 11:

The Governor's Office of Information Technology should improve visitor access controls by:

a. Implementing a process to designate responsibility to the employee host to ensure visitors successfully follow all visitor control procedures, including the return of badges and signing out of the visitor log after hours.

b. Including additional space on the log sheet for employees to sign acceptance of visitor arrival and document departure.

c. Communicating and reinforcing visitor control procedures with all Data Center employees and building reception staff.

Governor's Office of Information Technology Response:

Agree. Implementation date: January 2009. The Governor's Office of Information Technology agrees that visitor access controls should be improved. It should be noted, however, that the main entrance to the Data Center is now managed by personnel of the Department of Public Safety. As such, OIT will need to work with Public Safety in the implementation of this recommendation.

Power and Signal Cable Duct Re-Engineering

Industry best practices dictates that data center power and signal cable ducts should be separated. The lack of proper separation could lead to electrical surges, cable breakages, and system outages. In the April 2000 SAS 70 Report, it was

recommended that as equipment changes in the Data Center or major renovations are performed, the Data Center should re-engineer both power and signal cable ducts to provide separation and safety. In 2007 the Data Center reported that previous plans to separate power and network cabling were tabled until current plans for state data center consolidations were completed. As part of the 2007 SAS 70, BKD determined that lack of cable separation continues to be a significant issue and recommended that the Data Center review and address the re-engineering of power and signal cable ducts to provide separation and safety in light of current state data center consolidation planning (2007 Report Recommendation No. 13). The Data Center partially agreed with the recommendation and responded that retro-fitting the data center was not financially sound because plans for state data center consolidations would eventually achieve this recommendation.

2008 Auditor Assessment: *Not Implemented.*

During our 2008 follow-up we again noted that the Data Center's power and signal cable ducts are not properly separated. Although the Data Center agrees that separating power and signal cable ducts is best practice, the Data Center does not believe retrofitting the existing Data Center is financially sound until plans for state data center consolidations are finalized. The Data Center reports that cable separation will be undertaken as part of the three-year data center restructuring process and should be accomplished by 2010.

Recommendation No. 12:

As part of the three-year state data center restructuring process, the Governor's Office of Information Technology should re-engineer the power and signal cable ducts at the Data Center to provide separation and help ensure safety and performance.

Governor's Office of Information Technology Response:

Agree. Implementation date: January 2011. The Governor's Office of Information Technology will re-configure and standardize cabling set up as major renovations to the Data Center occur. Additionally, OIT staff are now trained to certify each cable connection to assure that there is no interference or other electrical problems. This is now a standard practice at the Data Center.

Management Oversight

As previously discussed, the Data Center is responsible for designing and putting in place data processing controls to ensure computer resources and data are protected, transactions are reliably and accurately processed, and customer requirements are met. Data Center management is ultimately responsible for the oversight and implementation of appropriate and timely controls and for the remediation of deficiencies identified in prior audits. As noted throughout this report and discussed below, Data Center management has failed to act on prior audit recommendations and has not established a process to ensure control activities and procedures are updated and designed to achieve management's objectives.

Assessment of Control Activities and Procedures

The Data Center is responsible for establishing and maintaining a control framework to ensure the effectiveness of the services provided and the confidentiality, integrity, and security of systems housed at the Data Center. These services and the support provided by the Data Center are vital to all state agencies' ability to transact business accurately and on a timely basis. Accordingly, regular management attention should be given to the review, evaluation, and implementation of appropriate organizational, technical, and process controls. In the 2007 Report, BKD recommended that the Data Center conduct periodic meetings (at least on a quarterly basis) of the members of management to ensure that control documentation is updated on a regular basis to reflect the actual controls and procedures in place, to evaluate the effectiveness of current or proposed controls, and to review prior year audit suggestions/recommendations to ascertain they are being implemented on a timely basis during the year (2007 Report Recommendation No. 10). The Data Center agreed to implement this recommendation by December 1, 2007, by holding quarterly meetings to review and update controls and activities and to ensure prior audit recommendations are being addressed.

2008 Auditor Assessment: *Not Implemented.*

During the 2008 follow-up we learned that Data Center management has not been periodically assessing control activities and procedures with appropriate staff as recommended in 2007. Additionally, we found that no other mechanisms exist to ensure the Data Center's control descriptions are updated and prior audit recommendations are implemented. During our 2008 follow-up, we again found that the Data Center's control descriptions are outdated and prior audit recommendations were not acted upon. Specifically, the Data Center failed to implement 12 of the 13 recommendations contained in the 2007 Report. Data Center management is ultimately responsible for

the oversight and implementation of appropriate and timely controls and for the remediation of deficiencies identified in prior audits. Therefore, we recommend that the Data Center implement the 2007 recommendation and take immediate steps to ensure that all audit recommendations are implemented in a timely manner.

Recommendation No. 13:

The Governor's Office of Information Technology should ensure the Data Center's controls are accurate and complete and all outstanding audit recommendations are addressed by:

a. Holding periodic meetings with the Data Center's management staff to discuss and update control activities.

b. Periodically evaluating the effectiveness of current and proposed controls.

c. Developing a plan with established milestones for implementing all audit recommendations, including assigning responsibility for each recommendation to a Data Center staff member.

d. Requiring Data Center management to periodically report on the status of all outstanding recommendations to management staff within the Governor's Office of Information Technology.

Governor's Office of Information Technology Response:

Agree. Implementation date: January 2009 and Ongoing. OIT will establish procedures to periodically review, evaluate, and update control activities and monitor progress on implementation of agreed-upon audit recommendations.

The electronic version of this report is available on the website of the
Office of the State Auditor
www.state.co.us/auditor

A bound report may be obtained by calling the
Office of the State Auditor
303.869.2800

Please refer to the Report Control Number below when requesting this report.

Report Control Number 1966