ATTACHMENT D

STATE OF COLORADO

GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

1580 Logan Street, Suite 200
Denver, Colorado 80203
Phone (303) 866-6060
Fax (303) 866-6454
www.colorado.gov/oit

Bill Ritter, Jr.
Governor

Michael Locatis
State Chief Information Officer

March 25, 2009

The Honorable Dianne Primavera, Chair
Legislative Audit Committee
200 East 14th Avenue, Suite 200
Denver, Co 80203

Dear Representative Primavera,

As requested by the Legislative Audit Committee, attached is the Governor's Office of Information Technology implementation status of the Data Center SAS 70 audit recommendations from November 2008. As indicated in the table, the Office has implemented 8 of 13 recommendations and continues to make progress regarding the other 5.

Please contact Todd Olson, Chief Operating Officer, at (303) 866-6060 if you have any questions.

Sincerely,

Michael Locatis
Chief Information Officer

Governor's Office of Information Technology (OIT) SAS 70 follow up
Status tracking

Rec. No.	Page No.	Recommendation Summary	Agency Response	Implementation Date	Status update from OIT Mar-09
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	The Office recently started a project to address strengthening of Top Secret administration. The project will focus on the recommendations from this audit as well as recommendations regarding Top Secret from the FY08 Statewide Financial and Compliance audit. To date, the Office has completed a project plan and charter, drafted TSS procedures, developed an automated report to identify terminated and transferred individuals, worked with agencies in obtaining and utilizing this report for TSS maintenance, and started inputting EID numbers into the Access ID data.
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	The Office continues to review and update its service level agreements. Some of the SLAs currently being worked on include DPA, Treasury, and DNR-Parks. Additionally, the Office created a governance committee to develop service management MOUs which will eventually replace SLAs. The service management MOUs will contain expectations/responsibilities regarding staff consolidation under SB08-155 as well as level of service requirements based on the services procured by each agency.
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	Jan-09	Implemented. A new check off sheet for server builds was created and is now maintained online. The Office has an existing server inventory; however, staff are in the process of revamping the inventory database. The new database is web based and includes server information such as server name, department, function, location, billing code, operating system, date installed, and date removed.
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	Implemented. Anti-virus software was deployed on 41 of the 42 Linux servers. The last server is too old and is scheduled to be retired.
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	Jun-09	The Office has incorporated vendor performance management into its project management process. Project managers are responsible for monitoring vendors to ensure that they are meeting their responsibilities and project milestones. Further, all major projects are overseen by an Executive Governance Committee (EGC). The EGCs serve as advisory boards for making recommendations to OIT regarding changes with project funding, scheduling, release plans, staffing, and other issues which could impact a project. Finally, OIT staff are working with the Department of Personnel and Administration staff in the requirements of SB07-228 and will incorporate the necessary processes once the system is finalized.
10	32	Establish a written document retention policy and communicate this policy to all staff.	Agree	Dec-08	In progress. A draft SOP has been developed and is being reviewed by management. The Office expects this SOP to be formally established by March 2009.
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	Jan-09	Implemented. OIT staff reiterated the access procedures with staff. Additionally, OIT is coordinating revisions to the log sheet with the Department of Public Safety (CDPS) and the new procedures were communicated to OIT and CDPS staff.
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	Jan-11	Complete re-engineering of power and signal cables is a very expensive endevor. As a result OIT has implemented other control & testing procedures to ensure proper performance. As server racks are moved in the future under floor wiring will be addressed.
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	Implemented. The Office established quarterly meetings to discuss and review audit recommendations, implementation status, and control activities. Two meetings have occurred.