Office of the Secretary of State

Kate Brown
Secretary of State

Barry Pack
Deputy Secretary of State

Audits Division

Gary Blackmer
Director

255 Capitol St. NE, Suite 500
Salem, OR 97310

(503) 986-2255
fax (503) 378-6767

March 7, 2012

Michael Jordan, Director and Chief Operating Officer
Department of Administrative Services
155 Cottage St. NE, U20
Salem, OR 97301

Dear Mr. Jordan:

We recently completed an audit of the State Data Center (SDC). The purpose of this audit was to provide internal control information to support our annual financial audits of agencies utilizing the SDC, and to provide DAS management information regarding SDC risks and controls. Our specific audit objectives were to determine whether the SDC provided: (1) a controlled and stable operating environment for agency and enterprise applications, and (2) the necessary security framework to protect agency and enterprise applications and their data. In addition, we evaluated SDC efforts to implement recommendations from prior audits.

This letter communicates our audit results and conclusions relating to the data center operating environment as specified in our first audit objective. Because of the sensitive nature of security, we communicated the results of the second objective in confidential letter No. 107-2012-01-01, according to ORS 192.501 (23).

Results

Managing the complex and extensive inventory of computer operating system platforms, networks, and associated enterprise security infrastructure at the SDC requires competent staff performing the day-to-day activities. In addition, managing these operations efficiently and cost-effectively requires well designed and consistently applied controls.

Based on our audit work, we concluded the SDC provides an operating environment that ensures day-to-day processing occurs for hosted state agency computer applications. Specifically, the SDC physical environment was appropriately protected from environmental and man-made hazards, routine back-ups were taken for agency applications, and production jobs were appropriately monitored. Controls were also in place to ensure significant production problems were analyzed and resolved in a timely manner. However, we noted two important aspects of data center operations that could be improved. Details of these issues are included in the following findings:

Finding #1: Disaster recovery plans were not complete or fully tested.

Restoring SDC operations after a disaster or other serious disruption would require significant advance planning and coordination between all affected parties. Best practices indicate data centers should mitigate the risks associated with serious disruptions in service by developing and periodically testing disaster recovery plans. These plans should be based on agreed-upon customer requirements and regularly updated to reflect changes to the computing environment.

Since 2010, SDC staff expended considerable time and effort to improve disaster recovery capabilities. For example, they performed six separate tests ranging from a tabletop exercise in 2010 to the restoration of a logical partition of the mainframe computer in February of 2011. These accomplishments were noteworthy, but more work is needed to ensure the SDC and its customers will be better prepared to cope with a disaster or other serious incident. Specific weaknesses needing additional work include:

- Detailed instructions to restore infrastructure were not complete. SDC staff indicated they had completed approximately 85% of this task.
- Timelines and priorities for restoring agency applications and data were not established.
- Disaster recovery roles, responsibilities and expectations were not fully defined.
- Infrastructure configurations were not well documented to ensure plans reflected the current or expected state.
- Not all critical disaster recovery processes were tested, including restoring agency applications.

Disaster recovery planning is a resource intensive task that historically has not been given priority when matched with projects having more immediate or certain payback. However, inordinate delays in restoring some computer systems after a disaster could severely impact state agencies' ability to provide mission critical services to Oregon citizens.

We recommend that SDC staff and management complete and test its disaster recovery plans. These efforts should ensure detailed restoration instructions are completed; realistic recovery timelines and priorities are established; recovery roles, responsibilities and expectations are defined; infrastructure configurations are documented and maintained; and all critical disaster recovery processes are tested.

Finding #2: Some media tapes were not properly controlled.

IT control best practices indicate data management procedures should include effective management of the media library, including procedures to maintain an inventory of onsite media such as backup tapes. In addition, procedures should be in place for timely review and follow up on any discrepancies in the inventory.

The SDC tracks the location of tapes used in the backup process in an automated tape library system (ATL). This system documents whether tapes are located in the data center's tape drives or in off-site storage. During our audit, staff indicated they received a number of tapes for storage from agencies during the startup of the SDC. These tapes are stored in the tape room, but since they are not used in the backup rotation, they were not recorded in the ATL. We also noted that staff did not keep any other record of these tapes or reconcile ATL records to physical tapes stored in the tape room.

Maintaining an accurate and complete inventory of removable tapes is imperative for ensuring information stored on the media is safeguarded against unauthorized use, disclosure, modification, damage or loss.

We recommend the SDC maintain an accurate listing of all media tapes in its possession and in authorized offsite locations, and perform regular reviews and timely follow up on any discrepancies.

Scope and Methodology

During our audit, we interviewed various department personnel, reviewed department documentation and conducted various tests of controls. The scope of our audit included controls that were in place during our review, June through December 2011. To determine whether the SDC provided a controlled and stable operating environment, we evaluated processes and procedures for:

- establishing and maintaining customer service level agreements;
- managing infrastructure performance and capacity;
- ensuring continuous service;
- managing problems and incidents;
- controlling infrastructure configurations;
- managing data; and
- monitoring production processes.

To determine whether the SDC had the necessary security framework to protect agency and enterprise applications and their data, we evaluated:

- security plans, policies, procedures, and standards;
- physical and environmental controls;
- selected logical access listings, access policies, and the related system parameters;
- controls in place for governing security testing, surveillance and monitoring;
- procedures for reporting and resolving security violations and incidents;
- processes for managing and protecting operating system configurations; and
- internal and external audit, risk, and vulnerability assessment reports.

We used IT Governance Institute's publication, "Control Objectives for Information and Related Technology," (COBIT) and the United States Government Accountability Office's publication "Federal Information Systems Controls Audit Manual" (FISCAM) to identify generally accepted control objectives and practices for information systems.

We conducted this performance 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 findings and conclusions based on our audit objectives.

Sincerely,
OREGON AUDITS DIVISION

Neal E. Weatherspoon, CPA, CISA, CISSP
ITAudit Manager

Oregon
John A. Kitzhaber, MD, Governor

Department of Administrative Services
Director's Office
155 Cottage Street NE U20
Salem, OR 97301
PHONE: 503-378-3104
FAX: 503-373-7643

March 14, 2012

Gary Blackmer, Director
Audits Division
Office of the Secretary of State
255 Capitol Street NE, Suite 500
Salem, OR 97310

Re: M*anagement letter concerning SDC Audit dated March 7, 2012*

Thank you for the opportunity to respond to the March 7, 2012 letter regarding the State Data Center (SDC). The Department of Administrative Services (DAS) considers the audit a very important safeguard to the integrity of the State's infrastructure and takes these matters very seriously. DAS' response to each Oregon Secretary of State, Division of Audits (OAD) recommendation is outlined in this letter.

You will find below DAS's response to the specific audit recommendations outlined in the March 7, 2012 letter. DAS generally agrees with OAD's recommendations for each finding as phrased in the SDC management letter dated March 7, 2012.

1. Audits Division recommendation:

We recommend that SDC staff and management complete and test its disaster recovery plans. These efforts should ensure detailed restoration instructions are completed; realistic recovery timelines and priorities are established; recovery roles, responsibilities and expectations are defined; infrastructure configurations are documented and maintained; and all critical disaster recovery processes are tested.

DAS' Response:

Management agrees with the recommendation. The SDC has established a Disaster Recovery plan and has performed successful infrastructure recovery tests on all technical platforms and tested the recovery of the identified critical infrastructure applications based on customer business requirements and budget allowances. The SDC has requested funding and position authority for a Disaster Recovery Manager to operate the Disaster Recovery program in a 2013-15 Policy Option Package (POP).

The SDC will test disaster recovery plans and processes for several of the large agencies at the SDC by June 2013 and will continue to partner with customer agencies to further develop and define agency application disaster recovery priorities and with the Executive Leadership Team (ELT) to establish enterprise disaster recovery options based on disaster type and scope.

2. Audits Division recommendation:

We recommend the SDC maintain an accurate listing of all media tapes in its possession and in authorized offsite locations, and perform regular reviews and timely follow up on any discrepancies.

DAS' Response:

Management agrees with the recommendation. The State Data Center will continue to work with the agencies on the tape inventory inherited as part of the initial CNIC consolidation as well as develop an accurate listing of all media tapes and their location by December 2012. The SDC will perform scheduled tape inventories and review the results to determine the accuracy of the tape media control inventory and make process and procedural adjustments as necessary.

Closing

The Department of Administrative Services again thanks the Oregon Audits Division for the opportunity to respond to this audit. We take these findings and recommendations very seriously. Additionally, as the State's Chief Operating Officer, my commitment to you will be to discuss these findings with the Executive Leadership Team (ELT) and provide their input, guidance, and support to the SDC.

We appreciate your audit team's diligent effort over the past year to address concerns and highlight opportunities for improvement at the SDC. Since the team completed its field work in 2011, we have endeavored to implement its recommendations and will continue to make progress as described above.

If you have any questions about this response, please don't hesitate to contact either Julie Bozzi, SDC Administrator at 503-378-4578 or Kurtis Danka, SDC Deputy Administrator at 503-378-6430.

Thank you again for the recommendations and helpful insight your audit has afforded us.

Sincerely,

Michael Jordan
Chief Operating Officer
DAS Director
Oregon Department of Administrative Services

cc: Julie Bozzi, Administrator, State Data Center
Pamela Stroebel, Chief Audit Executive, Department of Administrative Services