LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Angie Grove, Deputy Legislative Auditor

CC: Janet Kelly, Director, Department of Administration
Dick Clark, Chief Information Officer

DATE: October 2011

RE: IS Audit Follow-up (11SP-20): Statewide Disaster Recovery Planning for Information Systems, Department of Administration (orig. 10DP-01)

Introduction

We presented our Information Systems audit on Statewide Disaster Recovery Planning for Information Systems to the Legislative Audit Committee in February 2010. The report contains one recommendation relating to developing policy including criteria for disaster recover planning for State information technology systems.

We requested and received information from Department of Administration personnel regarding progress toward implementation of the report recommendation. This memorandum summarizes the department's responses and our follow-up work.

Background

An important element of business continuity is disaster recovery (DR) planning for information technology (IT) systems. DR planning is a set of steps, communications, and responsibilities that are to be executed in the event of an interruption of services. An effective DR plan is documented and designed to quickly and completely reestablish a system or service following a service interruption or disaster resulting in minimum loss to the organization. Best practices identify the following nine items as critical elements of a complete DR plan:

- Definition of roles and responsibilities of agency staff during and following a disaster or outage
- Detailed information of IT system recovery procedures to be implemented
- Procedures for testing the plan
- Expectations of time for recovery
- Identification and prioritization of critical services
- Usage guidelines (when the plan should be used)
- Communications guidelines (what information should be given to whom and how it should be shared)

- Location of a recovery site
- Inventory of equipment required for recovery

Follow-up discussion

The following sections summarize the report recommendation, and the progress towards implementing the recommendation.

Disaster Recovery Policy

During our audit, we determined state agencies are aware of the need for DR planning for critical IT systems and most have incorporated some elements of a DR plan. However, we noted the level of understanding of DR planning varies between agencies and some are more prepared to deal with extended system outages than others. During the audit, we noted all agencies have considered DR planning, and all have implemented some of the previously identified elements to restore critical systems; however, we also identified disparities in the level of completeness and inconsistent implementation of DR plans. Establishing centralized policy and corresponding guidelines requiring complete and consistent DR planning for critical IT systems will address the situation.

The Statewide Information Technology Services Division (SITSD) provides support for agencies developing business continuity and DR procedures. In addition, SITSD has obtained software to assist in developing business continuity and DR documentation. At the time of our audit, SITSD had not established policies regarding DR planning. Considering our review of critical systems, state policy is needed to ensure agencies are developing complete and consistent procedures for recovering critical systems during a disaster or outage.

RECOMMENDATION #1

We recommend the Department of Administration develop policy including criteria for disaster recovery planning for State information technology systems.

Implementation Status: Being Implemented

DOA is in the process of developing policies to address business continuity throughout state government. As of July 1, 2011, the department had finalized an overall business continuity policy that includes requirements for all agencies to establish capabilities to ensure the continuity of essential government functions and the ongoing operation of services. Policy also requires agencies to develop and implement business continuity plans to support continuity efforts. In reviewing the current policy, there is little mention of the IT component of business continuity other than reference to IT standards from the National Institute of Standards and Technology. However, according to department personnel, this is an ongoing process and the department is still developing additional continuity related policies, including a policy specific to IT Disaster Recovery Planning. The department anticipates this policy will be completed by December 31, 2011.

To support DR policy, the department has taken additional steps to provide guidance and support to agencies. During the audit, we noted the State had purchased software called the Living Disaster Recovery Planning System (LDRPS), which provides users with various templates for continuity of business processes and IT DR. We also determined by completing the templates, the users will have addressed the critical elements of DR planning identified in our audit. Currently, about nine agencies are voluntarily using the LDRPS, with additional agencies projected to use

the system. Additionally, the department has been working with agencies in identifying critical business processes and associated IT systems to assist in the planning process. The processes for implementing LDRPS, identifying critical business processes, and identifying IT systems at the various agencies are ongoing. Because policy development is ongoing, it may be useful for the Committee to continue receiving updates on the status of implementation.

S:\Admin\IS\Follow-up\11SP-20-Statewide-Disaster-Recovery-Planning-for-IS-follow-up-orig-10DP-01.docx\mh