

INFORMATION TECHNOLOGY UPDATE

A Report Prepared for the
Legislative Finance Committee

By
Barbara Smith, Assistant Principle Fiscal Analyst
Kris Wilkinson, Senior Fiscal Analyst

September 27, 2012



INTRODUCTION

The Legislative Finance Committee (LFC) per 5-12-205, MCA is responsible for monitoring information technology with specific attention to issues that are likely to require legislative attention. During the 2013 biennium the LFC monitored and addressed a number of information technology issues, leading to some fundamental changes on how information technology (IT) projects are monitored in the interim. A summary of those items is included in this report.

Since the last LFC meeting, agency information technology strategic plans were completed as required by the Montana Information Technology Act (MITA). MITA directs the Department of Administration (DOA) to prepare a statewide information technology strategic plan and subsequently guide agencies to develop an agency information technology strategic plan that is in alignment with the state strategic plan. The State Information Technology Services Division (SITSD) publishes the guidance, reviews, and approves plans to fulfill this statutory requirement. Subsequent work of SITSD is predicated upon what is included in an approved IT plan. This report includes a synopsis of items found within the agency plans and raises issues regarding the value of the planning process that the LFC may wish to address.

LFC 2013 BIENNIUM IT ACTIVITIES

The LFC receives a report regarding the status of information technology from Dick Clark, Chief Information Officer (COI) for the Department of Administration. The purpose of this report is to keep the LFC apprised of progress of large scale IT projects, IT infrastructure improvements/issues and changes to state IT policies. Three changes occurred within this process:

- criteria for inclusion in the portfolio report
- post-implementation review, and
- readability of state policies.

Portfolio Report

The LFC approved criteria for placing IT projects onto the IT Portfolio Report at its March 2012 meeting. The State Information Technology and Services Division issued a new policy on September 6, 2012 outlining the improvements to report. The policy includes guidance to agencies regarding which costs should be included in the estimate of the IT project. As the formal directive was just issued, the LFC may see additional projects included on the November report as agencies analyze the overall costs of their various IT projects.

Post Implementation

The LFC also approved post implementation reports for completed IT projects. This was the result of reviewing and investigating disruptions in the eligibility process in the Offices of Public Assistance due to the lack of scanning equipment. Review of this project resulted in the LFC seeking post implementation follow up.

The September IT Portfolio Report shows that the CHIMES eligibility system is on schedule and due to be completed by October 2012. Due to the critical nature of the eligibility system the LFC may wish to request a post implementation report at its November 2012 meeting. This would allow the LFC to be apprised of successes and challenges associated with the new system during the first month of operation.

Readability of Policy Reports

The LFC requested that the staff of SITSD submit policy review details in plain language. Over the course of time the policy review document submitted to the LFC had become increasingly technical and difficult to decipher. SITSD has since provided reports in plain language giving the general reader an opportunity to understand changes to statewide IT policy.

LOOKING FORWARD: STRATEGIC PLANS

The strategic plans submitted by agencies and approved by SITSD provide an insight to the information technology issues facing state agencies that could potentially require attention of the Legislature in the 2013 session. The purpose of the strategic plan is to provide the blue print for agency information technology for the time period of 2012 through 2017, with 2012 being an update to the previous plan. The plan includes narrative discussion on security, continuity of operations, goals and objectives, initiatives and potential costs.

This summary focuses on two items gleaned from the strategic plans. First, a summary of security and continuity of operations to provide a systemic examination of the risks associated with poor security or lack of continuity of operations plans. Second, the supplemental initiative documentation process to summarize the identified needs within state agencies, including potential costs. Both summaries are incomplete and provide little if any valuable information due to the wide ranging response from agencies. The value of the strategic plan is controlled by what is provided by the agency and may not accurately represent what the legislature needs to know about IT development within the agencies.

Agency Required Programs

Security is the responsibility of the agency director and not the CIO. Each executive branch agency is required to have an information security management program in compliance with 2-15-114, MCA¹. The CIO and staff is responsible for assuring such a plan exists, but does not have the normally corresponding enforcement capabilities. The strategic plan includes details on agency security programs.

Each agency must also report its continuity of operations program (COOP) is in compliance with DOA operational policies. A COOP is a plan to assure that critical services and process continue during a wide range of emergencies, including acts of nature, accidents and technological or attack-related emergencies. Details of an agency's COOP are to be provided in the strategic plan.

Security

The plan requires that the agency provide a general description of the information security management program being utilized. In review of the strategic plans, three entities (Department of Environmental Quality, Commissioner of Political Practices and the Public Service Commission) did not provide adequate information to determine compliance. In fact the DEQ strategic plan states:

DEQ has worked toward getting resources in place to enable compliance. We are currently optimistic that we will be able to begin the process of building an Information Security Management Program that will bring us into compliance.

The CIO does not have the ability to force DEQ, COPP or the PSC into compliance because security is the responsibility of the agency director. Noncompliance remains noncompliance until such time that the agency begins the development process.

¹ 2-15-114. Security responsibilities of departments for data. Each department head is responsible for ensuring an adequate level of security for all data within that department and shall: data within that department and shall:

(1) develop and maintain written internal policies and procedures to ensure security of data. The internal policies and procedures are confidential information and exempt from public inspection, except that the information must be available to the legislative auditor in performing postauditing duties.

(2) designate an information security manager to administer the department's security program for data;

(3) implement appropriate cost-effective safeguards to reduce, eliminate, or recover from identified threats to data;

(4) ensure that internal evaluations of the security program for data are conducted. The results of the internal evaluations are confidential and exempt from public inspection, except that the information must be available to the legislative auditor in performing postauditing duties.

(5) include appropriate security requirements, as determined by the department, in the written specifications for the department's solicitation of data and information technology resources; and

(6) include a general description of the existing security program and future plans for ensuring security of data in the agency information technology plan as provided for in 2-17-523.

History: En. Sec. 2, Ch. 592, L. 1987; amd. Sec. 22, Ch. 313, L. 2001; amd. Sec. 4, Ch. 114, L. 2003.

However, DEQ was not the only agency to comment on limited resources. In terms of resources most agencies agree, by the inclusion of the following statement, that resources are a constant challenge.

The agency's information security management program is challenged with limited resources; manpower and funding. While alternatives are reviewed and mitigation efforts are implemented the level of acceptable risk is constantly challenged by the ever changing technology and associated risks from growing attacks and social structure changes. Specific vulnerabilities have been identified which require restructure, new equipment, or personnel positions (funds increase).

Yet few agencies used the initiative portion of the plan to address this problem. The discussion of the submitted initiatives below illustrate that requests for resources were not considered at the time the plans were written.

Continuity of Operations

Similar to the plan security requirements, agencies must include a generalized description of the agency Continuity of operations plan (COOP). As with the security requirements not all agencies were able to adequately report a COOP is in place. This includes Arts Council, Historical Society, Livestock, Commissioner of Political Practices, Public Service Commission and the School for the Deaf and Blind.

IT initiatives and future costs

The planning guidance for the strategic plan request that an agency describe significant IT initiatives that will take place during the following biennia (in this case fiscal years 2014 and 2015) by priority. For the purpose of the strategic plan, an initiative is defined as:

- An executive planning process (EPP) item for IT spends
- A budget of \$500,000 or more, whether or not it is an EPP item
- A budget of \$100,000 or more that comprises 25% of more of the agency's IT budget, whether or not it is an EPP item

One would expect to find long range and base budget initiatives within the strategic plans. However, an examination of the ITSD summary document titled "Montana Information Technology Initiatives for FY 14 - 15"² indicates there are 45 initiatives across state government but fails to provide an estimate of those costs. Nor does the summary document identify how much has already been appropriated through the long range information technology bills. This information, if available has to be gleaned from individual plans. A cross walk between the summary document and the actual plans, identified the following initiatives with cost estimates.

Information Technology Initiatives Per Strategic Plans (2015B)		
Agency	Initiative	Cost
Commissioner of Political Practices	Campaign Reporting Services	\$518,000
Administration - General Services	Maintenance Management System	350,000
Livestock	USAHerds Maintenance, Support & Enhancement	398,000
Office of Public Defender	IIS Broker Participation	150,000
State Library	Digitize Legacy State Publications	545,000
	Total	<u>\$1,961,000</u>

There are other items within the reports that indicate other activities are occurring, but appear not to rise to the initiative level. This includes multiple plans to examine electronic records management, migration of disaster and recovery activities to Miles City, replacements of legacy systems and consolidation of agency systems. All of these activities have a cost but the plans do not address the need for any appropriation authority.

² See Appendix.

Value of Strategic Plans

The IT strategic plan can be valuable when appropriate and adequate information is provided to guide agency decision making and resource allocation process. This is not possible with the majority of the plans examined as noted in the IT initiative portion of this report and the lack of information available in the plans. This is similar to the recent findings of the Legislative Audit Division that the planning process lacks completeness and continuity. DOA has agreed with recent legislative audit findings but given the cyclical nature to this process, corrections won't occur for two years. This time lag leaves the legislature without an adequate planning process.

WHAT'S NEXT

While the plans don't provide sufficient details on security, continuity of operations, funding or other identified needs, there still is the ability to scrutinize the plans for other valuable information. This includes utilization of the information in the budget analysis by LFD staff to raise IT related issues; with follow up discussions during agency budget hearings. The combination may allow the legislature to determine what IT activities really are occurring in the agencies. The LFC may wish to consider a global motion for this purpose.

Second, when ISTD begins the process of updating the strategic planning process, the LFC may wish to consider adding this function to the CIO regular report to the LFC. This would allow the LFC to maintain a level of input in the process to assure that strategic planning for information technology is a valuable process.