Computer Systems Planning Council
Potential Issues
February 2010

Below is a list of potential issues the Computer System Planning Council could work on this biennium:

- **Computer System Planning Council Laws** - The Computer System Planning Council law was originally enacted in 1989. Some things have changed over the years, for instance instead of computers the term Information Technology is used more often. Is their any interest in reviewing this law and updating it? Is it working and providing a good outline for governance of IT?

- **IT Governance** - Is their sufficient governance of IT in the Legislative Branch? CobiT (Control Objectives for Information and related Technology) says this about IT governance:

  "IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organizational structures and processes that ensure that the enterprise's IT sustains and extends the organization's strategies and objectives."

  ".... management should understand the status of its enterprise architecture for IT and decide what governance and control it should provide."

  "Value, risk and control constitute the core of IT governance."

- **Social Networking/Social Media** - "Social Media" is an umbrella term that encompass the various activities that integrate technology, social interaction, and content creation. Social media uses many technologies and forms, such as blogs, wikis, photo and video sharing, podcasts, social networking, mashups, and virtual worlds.

  The executive branch has adopted a social media policy. Does the Legislative Branch want or need it's own policy? Are there any issues that need to be discussed with legislator use of social media?

- **Status of Obsolete Systems** - The current computer system plan has defined the following systems as "Declining or Obsolete Technology" (see page 23 of the plan):
  - LAD SABHRS
  - Mainframe TextDBMS System
  - LAWS Web Pages
  - WordPerfect and WordPerfect Macros
  - Lotus Approach
  - Microsoft Office Suite
  - Montana Budgeting Analysis and Reporting System (MBARS)

- Desktop Operating System
- Network Operating System

Staff could prepare a report on the status of each of these systems (and any others that need to be added to the list). This report would talk about the reason these systems are declining or becoming obsolete. The Session Systems Analysis project will address some of the systems and make recommendations.

- **Security** - The branch hired a security officer last biennium. We have struggled to get a security program off the ground. About 6 months ago, our security officer was hired into another position in the legislative branch. Some question the need for an extensive security program and the need for a full time security officer. The security program in the branch is on hold. Directors need to decide what level of security they are comfortable with.

- **Enterprise Architecture** - The branch began to define an Enterprise Architecture last biennium. We hired a part time Architect. The recent IT reorganization defined a full time Architect. We have just scratched the surface of what an Enterprise Architecture would look like. This is another program that we are struggling to get off the ground. We are making some small efforts this biennium toward an Enterprise Architecture. A proposal for next time is do a full fledged Enterprise Architecture project starting from the top of the organization and working our way down. We could identify this as a project to be accomplished in next bienniums computer system plan.

- **Computer System Plan** - Since this is a requirement under the law, the Computer System Planning Council needs to work on this and have a plan to the Legislative Council by it's September meeting.

- **Policy and Policy Education and Awareness** - OLIT would like to see policy developed in the following areas:

  Acceptable Use Policy for information, computer systems and network resources – This policy defines both appropriate and inappropriate use of information, computing, and communication resources and thus provides the user with basic parameters of acceptable use. This policy is necessary to limit the branch's exposure to a variety or risks, including virus attacks and compromise of network systems and services, as well as issues of legal liability such as sexual harassment and discrimination.

  Auditing Software – The branch owns a networking auditing software suite, which enables the directors to monitor (through the IT department) network usage. For instance this software can determine who accessed network resources and what was done with that access. This policy would outline which resource types are being audited and what activity is being monitored. Auditing of resources can be applied to all user levels from the basic user to network administrators and ensures the directors have a complete understanding of how Branch’s resources are being used and a better feel for the security of the Branch’s network. Users gain a better understanding of what network monitoring is being applied.

Software Asset Management – This policy ensures the branch protects itself from the distribution of copyrighted material, by not allowing the use/distribution of unlicensed software. It would detail the way software is obtained/maintained and ensure licensing and distribution is appropriately managed. Through policy, reporting tools, and/or other means the branch ensures staff is not downloading and/or installing unauthorized/unsupported software, which creates a legal liability for the branch and eliminates the threats of unsupported software (system performance and vulnerabilities).

Password Policy – This policy increases the security of our network, by increasing the strength of user/network passwords. Passwords are the front line of defense for network resources and user accounts. A poorly chosen password may result in the compromise of the entire legislative branch network. Increasing the length and complexity of branch passwords will increase the security of branch resources and information.

Creating policy is just the first step. The next step is to make staff aware of the policy. There would need to be an education and awareness component and an enforcement/compliance element to this policy.