

State of Montana Information Technology Managers Council

Council Business Meeting December 3, 2014 - 8:30 – 10:30 DEQ Metcalf Building – Room 111

Welcome and Introductions (8:30 – 9:00)

- Larry Krause, Chair
 - Approval of November Minutes
- Ron Baldwin, State CIO Update (LFC Recap/ECM Pilot)

Business (9:00 -10:25)

- 2015 Information Technology Legislation – Tammy LaVigne (5 minutes)
 - Observations/Concerns/Feedback – Roundtable discussion (2 minutes)
- IT Conference Update –Penne Cross (5 minutes)
 - Observations/Concerns/Feedback – Roundtable discussion (2 minutes)
- Mobile Device Management Update/ Jerry Marks(5 minutes)
 - Observations/Concerns/Feedback – Roundtable discussion (2 minutes)
- Enterprise Risk Assessment/Lynne Pizzini (10 minutes)
 - Observations/Concerns/Feedback – Roundtable discussion (2 minutes)
- Recruitment and Retention Phase I – Mike Bousliman (5 minutes)
 - Observations/Concerns/Feedback – Roundtable discussion (2 minutes)
- ITMC Security Task Force Update – Joe Chapman (2 minutes)
 - Observations/Concerns/Feedback – Roundtable discussion (2 minutes)
- FIM/SPLUNK– Jerry Marks (5 minutes)
 - Observations/Concerns/Feedback – Roundtable discussion (2 minutes)
- Business Checklist – Audrey Hinman (2 minutes)
 - Observations/Concerns/Feedback – Roundtable discussion (2 minutes)

Posted Reports

- Apprenticeship Program
- Legislation Template
- MITA Bill
- Enterprise Risk Assessment

Adjournment (10:27-10:30)

- Next Meeting January 7, 2015
- Member Forum

State of Montana Information Technology Managers Council

- **Public Comment**
- **Adjourn**

Notice: The Department of Administration will make reasonable accommodations for persons with disabilities who wish to participate in the ITMC's public meetings or need an alternative accessible format of this notice. If you require an accommodation, contact the Department of Administration no later than six business days prior to the meeting of interest, to advise us of the nature of the accommodation that you need. Please contact Tammy LaVigne at 406.444.2589 or TLaVigne@mt.gov.

**ITMC Council Business Meeting
November 6, 2014**

Attendees

State CIO	Ron Baldwin
Department of Revenue	Tim Bottenfield
Department of Justice	Joe Chapman
Department of Environmental Quality	Dan Chelini
Department of Agriculture	John Dayton
DNRC	Kreh Germaine
Department of Public Health and Human Services	Chris Gleason
State Library	Evan Hammer
Department of Commerce	Larry Krause
Montana Supreme Court	Lisa Mader
Department of Labor and Industry	Kim Moog
Department of Higher Education	Edwina Morrison (online)
Department of Fish, Wildlife & Parks	Dustin Temple (online)
Office of Public Instruction	Jody Troupe

Guests

DOR – Christie McDowell, DOA – Chris Bacon, Supreme Court – Tammy Peterson, DOA – Cheryl Grey, TRS - Rick Bush, MDT- Mike Bousliman, Northrop Grumman-Veronica Lanka, Legislative Audit - Amber Nuxoll, Dell-Armie Vacenzuela, Dell-Paul Erickson, Dell-Karen Farley, MPERA- David Swenson, Andrea Keno-SHI

Real Time Communication (online)

Kyle Belcher – DOA OPD, ART-Kristin Burgoyne, DEQ - Jerry Steinmetz, DOA – Matt Pugh, MACO- Joe Frohlich, SITSD – Dave Johnson, , SITSD-Kyle Hilmer, SITSD – Anne Kane, Central Office – Jon Straughn,- SITSD – Teresa Enger, SITSD – Ty Weingartner, DPHHS – Dan Forbes, SITSD-Doug Volesky, SITSD – Maris Cundith, SITSD-Wes Old Coyote, FWP-Jessica Plunkett, SITSD-Ed Sivils, STF-Stacy Ripple, DOC-Terry Meagher, SABHRS-Ed Glenn

SITSD Attendees

Tammy LaVigne, Warren Dupuis, Scott Lockwood, Steve Haynes, Jerry Marks, Audrey Hinman, Tom Murphy, Lesli Brassfield, Lynne Pizzini, Sean Rivera, Irv Vavruska, Cheryl Pesta, Carol Schopfer

I. Welcome and Introductions – Larry Krause, Chair

- Approval of October minutes.

II. State CIO Update – Ron Baldwin

- **ECM RFP Cancelled:** cost section being addressed. Will be starting a pilot with DLI, specifically George Parisot and Judy Kelly that will match funding from House Bill through pilot effort. Enterprise pilot policy will be put in use. Scope of project is expanding throughout

the agency. Choice of software is perceptive and is in use throughout the State. Pilot constructed in 4 phases, each phase being about two weeks.

- **Follow-up:** Ron will share a report and plan with the group and is expecting a report generated within the first month of this pilot.

III. E-procurement – Ron Baldwin

DOA is working on an enterprise e-procurement system. Details are still being developed.

- Contract Management Component: online and outward facing
- Key Stakeholders: Cheryl Grey, Sheila Hogan (Executive Sponsor)
- Executive Scope: in formation and will be formally addressed soon.
- Request to Agency's: please hold off on development of any agency e-procurement systems. SITSD would like agencies to be able to make use of this tool.
- Asset Lifespan: Expressed from group request for the new tool to cover the entire cycle of asset lifespan in addition to contract management.
 - *Inquiry*:
 - Is this tool going to be used for all procurement, not just IT Procurement? Would it include asset management? Will there be integration between IT asset purchasing, tracking through receiving, to install, to disposal at the end of lifecycle? It would be ideal for new system to run cradle to grave.
 - *Response*:
 - The hope is all agencies will make use of this system. Main focus is the e-marketplace, vendor and contract management. Asset management component already in SABHRS. Interface with SABHRS. The functionality of tracking procurement through the entire lifespan will be taken into consideration.

IV. IT Inventory Report – Ron Baldwin

- Response to report from Governor Bullock: meeting with Ron Baldwin and Lynne Pizzini resulted in direction from Governor Bullock to set a meeting with Department Directors and IT Managers. The context of this meeting is to share report information initially presented to the Governor. Some topics covered in the report include number of server rooms, state data centers, physical servers etc.
- Security: Some of the details generated from the report will not be discussed in this forum due to security risks. CIO's are encouraged to meet with Ron individually to discuss details pertaining to their agencies.
- Virtualization: report substantiated progress/benefits of virtualization in the State, including cost efficiency.

V. MITA Legislation– Ron Baldwin

- MITA Legislation Approved: will be carried forward into Legislative session. The conclusion of the current Bill’s assessment by Warren Dupuis, examining the Bill as written ten years ago, was it’s a good Bill. Goal of this Bill is clean the law up, making IT as effective and helpful as possible to workers in State Government.

- Primary Changes:

1. Revision of outdated terminology to modern definitions, e.g. “data”

Definition of data by statute:

“Any information stored on IT resources”

Proposed update for definition of data:

“Digital assets stored on IT resources, may refer to any electronic files, no matter what the format, including (but not limited to) database, data text, images, audio and video”

2. Clarify/quantify State CIO authority, assignment, governance and duties

VI. Re-organization of SITSD – Ron Baldwin

- Lynne Pizzini designated Deputy CIO. She will continue with her duties as CISO and will carry out a more internal-facing role. Lynne will also take on NTSB and those responsibilities to align them with security and technical responsibilities of the division.
- Ron Baldwin will continue taking on a more outward facing role. This translates to increased communication with IT holders, agency directors and work with other stakeholders including private companies and the legislative session.
- Warren Dupuis is taking on the significant business responsibilities of the division including oversight of bureaus and offices, business services, project management and acquisition management. He will be creating a matrix management approach applicable to alignment of business functions, ultimately increasing ability of SITSD to provide services and effective, clear service catalog.

VII. ITMC Security Task Force – Joe Chapman and Lynne Pizzini

- Goal: to recommend a structure that will enhance Montana information security posture. Group contains different people from different agencies, split into two main groups.
- Definition of problem: information security for the state needs to be improved, we are only as strong as our weakest link. There is a lack of resources, mostly human resources, not every agency has or needs a full time security person. There is a lack of standardized security across

the state. We need to improve communications on high-level and day to day threats and incidents.

- Primary Recommendations:

1. Security Task Force: to examine strategic direction.
2. Security Assistance Team: due to lack of human resources, implement a security assistance team that would make rounds across the agencies looking at different aspects of security. In addition, the team would help them establish policies and procedures and provide assistance as needed.
3. Enhancement of Information Security Communication: there are a number of security issues. One of which is addressing access to the different security levels. Outside security consultants were incorporated. Work needs to be done on immediate communication from threats and incidents.

- Enterprise Security Program/Executive Order: Ron and Lynne met with the Governor and Chief of Staff and proposed an enterprise security program. Based on Security Task Force recommendations, they requested the establishment of an Information Security Advisory Council. The Governor is contemplating an executive order. IT Security will be a major topic this legislative session; Ron anticipates a decision on the order from the Governor prior to the session. Governor showed support of what ITMC Task Force has done and is in approval of moving forward with implementation.

Inquiry (Tammy):

- Who will be on this board? Will they be formal appointments?

Response (Lynne):

- Recommendation is to have 8-12 members that will come from the IT area. Group will also include the State CIO, local government representation, legislative representation and representation of the general public. Yes, they will be formal appointments.

VIII. Master Contract/CEP Procedures- Steve Haynes

- Link 1: Master contract for IT services. Currently 125 companies listed in 14 different service categories. (Attachment 1) In June of 2016 these contracts will expire. Steve wants to be able to add companies to the master contract list as they contact him, instead of being locked down with the list for 10 year periods. Requesting agency feedback.

- *Inquiries:*

- **1.1** Is there a way to pre-qualify vendors for projects in particular categories?

- **1.2** Is there an opportunity to have vendors provide a synopsis of service areas/products and company overview when they are added to master contract list.
 - **1.3** When do the 18-24 days on the RFP timeline begin?
 - *Responses:*
 - **1.1** The CEP process should screen out vendors that are not qualified for projects in most cases.
 - **1.2** Yes. Steve felt it would be beneficial.
 - **1.3** 18-24 day timeline begins when Steve receives statement of work and job description from agencies.
- Link 2: Tier 2/CEP Procedure. Recently revised. CEP Procedures include a requisition form and estimated timeline. Generally process takes 18-24 business days. Steve will contact agencies per request with estimated quotes for projects. (Attachment 2)
- Contractor Assessment Program:
 - Agencies often request to either use a certain company or not use a certain company for projects. According to current RFP, CEP policy agency preference cannot be taken into account when considering contracts.
 - To address this, Steve is trying to incorporate the Contractor Assessment Program. The program will take into account the companies past performance (based off of agency assessment on the company's past performance) by either adding or deducting five percent from the CEP evaluation criteria.

IX. Recruitment and Retention Phase I – Tim Bottenfield

- First Meeting: Group met two weeks ago to discuss improving recruitment and retention within IT shops. There was a good representation from DOR, DLI, SITSD, AG, and FSWP in attendance. Conversation involved agency representatives sharing how their IT shops are organized and identifying what is and isn't working.
- Goals: review organizational structures, develop a strategy for external recruitment and create a plan for retention. May involve agencies learning from each other, sharing ideas, pooling resources, providing better training opportunities for staff and some discussion on career ladders.
- Next Meeting: Organizational structuring for IT shops and apprentice program Helena College will be discussed at today's 10:30 a.m. meeting. Meeting will be held at DLI located at 2550 Prospect Ave. Tim invited IT/HR agency representatives to attend.

X. Customer Service Catalog Project – Carol Schopfer

- Service Catalog Update: Business Services Management Bureau looking at full-scale revamp of the service catalog. Looking at integrating with current point of business tool. Kicking off the requirements gathering phase.

✉ Please participate in the survey located on SITSD homepage. [Ctrl+click here to complete survey](#). Business Services Management Bureau wants feedback, thoughts and suggestions on how this should work. If you would like to participate in the group, let Carol know.

- *Comments*:
 - Currently it's hard to understand what the options in the catalog are. It's not always straight forward and user friendly.
 - It would be helpful to include access to services that are separate from standard IT services. For example, phone lines for new employees.
- *Inquiry*:
 - Will this tool include procurement services?
- *Response*:
 - Focused on just SITSD services for now, although it's certainly an option to consider as we continue to develop program.

XI. IT Conference Update – Dan Chelini

- Conference Details: conference is December 8-10 at the Red Lion Hotel. Registration is \$75 until November 21, 2014 after which it will increase to \$100. Tentative conference agenda will be available this afternoon. Tracks will include security, network, tech, project management, computing, business management, and hands on lab. Friday morning will potentially include cyber incident table-top exercise, encouraging all agencies to participate. Friday morning presentation will be done by the Office of Homeland Security.
- ITMC Meeting at Conference: Tammy sent inquiry if people wanted to have ITMC meeting at the conference and the response was yes. Dan said at this point there is not a spot for the ITMC meeting to occur.
- Next ITMC Meeting Date: Tammy asked to move into another week. Response from Chair of ITMC, Larry Krause was to keep the ITMC meeting separated from the conference and keep the date set for December 3, 2014.
- Annual Incident Table-top Response CEU Requirement: Lynne commented this year there will be an outstanding security speaker at the IT Conference and if you need Continuing Education Units, you obtain that at the conference. I encourage you to participate in the table top exercise on Friday. This will provide the opportunity to fulfill the annual incident table-top response requirement.

XII. Enterprise Risk Assessment – Lynne Pizzini

- Background: Last session through HB10 we were given funding to complete an Enterprise Risk Assessment. Five agencies participated including DOJ, DOA, DOR, DLI, and DPHHS. Cerium contracted to complete risk assessment. Yesterday we were provided with an overview of the risk assessment results.

Brief overview of report as follows:

- Contributing Factors to a Successful Risk Management Program:
 1. **Support/sponsorship from top management.** Montana is doing well in this area. Governor Bullock has made this one of his priorities.
 2. **Comprehensive Plan:** involving governance and good policies and procedures. A review indicates a need for improvement in this area. One of those improvements is the recommendation of putting together a Governance Committee and updating policy.
 3. **Full Participation:** of all employees, from administrators down to end users. Enterprise Security Training Program now in place, last year's participation rate was at 75%. Goal is 100% participation this year.
 4. **Recourses:** currently limited resources for security personnel, being addressed in proposal to Governor.
 5. **Up to date tools:** state has multitude of security tools in place. The State is continuing to develop and add to this arsenal of tools.
 6. **Ongoing Vulnerability Assessments:** conducted quarterly on web servers. Lynne encouraged assessments completed for all servers; this can be done by opening a case with SITSD.
- Additional Recommendations:
 1. **Incident response:** rates lacking across the board. With the exception of SITSD, agencies were not properly documenting incidents. SITSD is happy to share incident response plan to any agencies that are interested.
 2. **Lack of updated policies/procedures:** Good enterprise security policies, but they are lacking within the individual agencies. Hopeful enterprise security program will help produce a template all agencies can use to develop their own security policies.

3. **Log review:** was identified as needing additional implementation. Lynne's group collects 100GB of information per day to identify areas of concern. Lynne's group reviewing from an agency perspective, reviews need to be conducted on by individual agencies.
4. **Continuous monitoring:** identified as an issue. The federal government recommends vulnerability scanning daily. Lynne encouraging this monthly or quarterly, with an effort to work towards daily scanning. Make sure no configuration changes have been made and nothing is going that is security relevant.
5. **Encryption for data at rest:** was identified across the board. Data that is sensitive in nature and/or has personally identifiable information.
6. **Patches:** go back to the basics. Examine basic security items and that they are in place. Check to make sure automated patching is working as it should.
7. **Updated anti-virus**
8. **Legacy software** – a lot of things in state government rely on Legacy software. We need to have a plan to move from outdated and unsupported software. XP no longer supported by Microsoft and Windows Server 2003 as of June 2015. Systems require review in order to upgrade and remain current. Outdated systems are susceptible to vulnerabilities.
9. **Phishing:** several phishing attempts sent via e-mail to a number of our employees and our response on our first scenario was very good. Only 17% of our employees went out to click on the link. This was due to our Service Desk blocking the link as they were not notified. The other three scenarios there was almost a 50% failure rate. We need to emphasize to our employees not to click on links. We will see more training as we move forward with our security training.

- Status on Moving Forward: Review of progress taking place in January. Summary of information will be available to agencies. Information provided in report will be sent to the IT Board, eGovernment Council, Legislative Finance Committee and Cabinet. Each agency that participated received recommendations/mitigations from contractors. Recommendation/request that agencies not share reports on security and vulnerabilities. Sharing could create additional security risks.

XIII. Customer Satisfaction Survey – Warren Dupuis

- Marketing Concept: being used by SITSD with product, placement, price, performance and customer at the center. Warren feels we can do a better job serving the customers. Offering proposition for quarterly customer satisfaction review of SITSD. Review of feedback will examine trends and business processes. Would like customers (agency's) to be involved in designing survey for SITSD. Warren would like agency feedback in designing the survey. Goal is to improve customer service to agencies.
 - Warren posed the question of what the best method is to provide agency feedback.

- **Follow-up:** Larry putting together a meeting with an open invite in the near future to discuss method (e.g. electronic, verbal feedback etc.) that will be used to evaluate customer service of SITSD.

XIV. Member Forum

- File Sharing: Larry brought up concern over file sharing with new web filtering products. Dave Carlson's team working on a secure file sharing service, still in the process of being built.
- **Follow-up:** Dave will provide update at next ITMC meeting

XV. Public Comment: none

Attachments:

Attachment 1: Master Contract for IT Services

Attachment 2: Master Contract for IT Services Tier II Procedure

Attachment 3: Enterprise Information Security Program Proposal

Next Meeting: December 3, 2014

Location: TBD

8:30 a.m. – 10:30 a.m.

Adjournment: 10:23 a.m.

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM
6101_07_006_Technology_Act_FINAL-1

*** Bill No. ***

Introduced By *****

By Request of the Department of Administration

A Bill for an Act entitled: "An Act clarifying provisions of the Montana Information Technology Act; amending sections 2-17-505, 2-17-506, 2-17-511, 2-17-512, 2-17-516, 2-17-521, 2-17-524, and 2-17-546, MCA."

Be it enacted by the Legislature of the State of Montana:

Section 1. Section 2-17-505, MCA, is amended to read:

"2-17-505. Policy. (1) It is the policy of the state that information technology be used to improve the quality of life of Montana citizens by providing educational opportunities, creating quality jobs and a favorable business climate, improving government, and protecting individual privacy and the privacy of the information contained within state information technology systems.

(2) It is the policy of the state that the development of information technology ~~resources in~~ for the state must be conducted in an organized, deliberative, and cost-effective manner.

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

(3) It is the policy of the state that information technology is essential and vital to the people of the state of Montana, and the services, systems, and infrastructure are therefore considered to be an asset of the state.

(4) The following principles must guide the development of state information technology resources:

(a) ~~There are statewide~~ Statewide information technology policies, standards, procedures, and guidelines are applicable to all state agencies and other entities using the state telecommunications network.

(b) Mitigation of risks is a priority ~~in order~~ to protect individual privacy and the privacy of information contained within information technology systems as ~~they~~ these systems become more interconnected and as the liabilities stemming from the risk to information technology, also known as cyber risk, have increased.

(c) Whenever feasible and not an undue cyber risk, common data is entered once and shared among government entities at any level or political subdivision.

(d) Third-party providers of data, such as citizens, businesses, and other government entities, are responsible

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

for the accuracy and integrity of the data provided to government entities.

(e) Government entities are required to conduct business through open, transparent processes to ensure:

(i) accountability to the citizenry, Montana citizens; and

(ii) information technology provides access to information through simple and expeditious procedures.

(f) ~~In order to~~ To minimize unwarranted duplication, similar information technology systems and data management applications are implemented and managed in a coordinated manner.

(g) Planning and development of information technology resources are conducted in conjunction with budget development and approval.

(h) Information technology systems are ~~deployed aggressively whenever it can be shown that it will provide improved services to Montana citizens~~ in an effective and efficient manner.

(i) Public-private partnerships are used to deploy information technology systems when practical and cost-effective.

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

(j) State information technology systems are developed in cooperation with ~~the~~ federal government, tribal, and local governments with the objective of providing seamless access to information and services to the greatest degree possible.

(k) State information technology systems are able to accommodate electronic transmissions between the state and its citizens, businesses, and other government entities, including providing financial incentives for citizens and businesses to use electronic government services.

(l) State information technology systems are able to ~~embrace the economics~~ maximize the use of digitized records to avoid duplication and transport costs.

(m) Electronic record creation, management, storage, and retrieval processes and procedures are used to create and deliver professional records management ~~experiences~~ for the benefit of Montana citizens ~~of Montana~~.

(n) State information technology systems are ~~able to embrace continuous process improvement initiatives in order~~ designed to keep pace with new and emerging technologies and delivery channels ~~in order~~ to allow Montana citizens to determine when, where, and how they interact with government agencies.

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

~~(5) It is the policy of the state that the department must be accountable to the governor, the legislature, and the citizens of Montana."~~

{Internal References to 2-17-505:
2-17-521X }

Section 2. Section 2-17-506, MCA, is amended to read:

"2-17-506. Definitions. In this part, unless the context requires otherwise, the following definitions apply:

(1) "Board" means the information technology board established in 2-15-1021.

(2) "Central computer center" means any ~~stand-alone or shared computer and associated equipment, software, facilities, and services~~ state data center facility administered by the department ~~for use by state agencies.~~

(3) "Chief information officer" means a person appointed by the department director ~~of the department~~ to carry out the department's duties and responsibilities relating to information technology.

(4) "Data" means any ~~information stored on information technology resources~~ asset information stored on information technology resources, and may refer to any

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

electronic file regardless of the format including, but not limited to, databases, text, images, audio, and video.

(5) "Department" means the department of administration established in 2-15-1001.

(6) "Electronic access system" means a ~~system capable of making data accessible by means of an information technology facility~~ telecommunications network that allows information technology to exchange data in a voice, video, or electronic data form, including but not limited, to the internet.

(7) "Information technology" means hardware, software, and associated services and infrastructure used to store or transmit ~~information in any form, including voice, video, and electronic data.~~

(8) "State agency" means, for purposes of this part, any entity of the executive branch listed in 2-15-104 and includes, including the university system and the office of public information.

(9) "Statewide telecommunications network" means any telecommunications facilities, circuits, equipment, software, and associated contracted services administered by the department for the transmission of voice, video, or ~~electronic data~~ from one device to another."

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

{Internal References to 2-17-506:

17-5-807X 90-1-405X }

Section 3. Section 2-17-511, MCA, is amended to read:

"2-17-511. Chief information officer -- duties. The

duties of the chief information officer include, but are not limited to:

(1) carrying out all powers and duties of the department ~~as assigned by the director of the department;~~ provided in 2-17-512 and 2-17-534 and assigned by the department director;

(2) serving as the chief policy advisor to the director ~~of the department~~ on statewide information technology issues; ~~and~~

(3) ~~assisting and advising the director of the department on~~ carrying out the enforcement responsibilities provided in 2-17-514; ~~and~~

(4) advising the governor and the cabinet on matters concerning information technology and information security."

{Internal References to 2-17-511:

2-6-503X 2-15-1021X }

Section 4. Section 2-17-512, MCA, is amended to read:

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

"2-17-512. Powers and duties of department. (1) The department is responsible for carrying out the planning and program responsibilities for information technology for state government, except the national guard as defined in 10-1-101. The department shall:

(a) ~~shall~~ encourage and foster the development of new and innovative information technology within state government;

(b) ~~shall~~ promote, coordinate, and approve the development and sharing of shared information technology application software, management systems, and information that provide similar functions for multiple state agencies;

(c) ~~shall~~ cooperate with the office of economic development to promote economic development initiatives based on information technology;

(d) ~~shall~~ establish and enforce a state strategic information technology plan as provided for in 2-17-521;

(e) ~~shall~~ establish and enforce statewide information technology policies and standards;

(f) ~~shall~~ review and approve state agency information technology plans provided for in 2-17-523;

(g) ~~shall~~ coordinate with the office of budget and program planning to evaluate budget requests that include

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

information technology resources. The department shall make recommendations to the office of budget and program planning for the approval or disapproval of information technology budget requests, including an estimate of the useful life of the asset proposed for purchase and whether the amount should be expensed or capitalized, based on state accounting policy established by the department. An unfavorable recommendation must be based on a determination that the request is not provided for in the approved agency information technology plan provided for in 2-17-523.

(h) ~~shall~~ staff the information technology board provided for in 2-15-1021;

(i) ~~shall~~ fund the administrative costs of the information technology board provided for in 2-15-1021;

(j) ~~shall~~ review the use of information technology resources for all state agencies;

(k) ~~shall~~ review and approve state agency specifications and procurement methods for the acquisition of information technology resources;

(l) ~~shall~~ review, approve, and sign all state agency contracts and shall review and approve other formal agreements for information technology resources provided by the private sector and other government entities;

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

(m) ~~shall~~ operate and maintain a central computer center for the use of state government, political subdivisions, and other participating entities under terms and conditions established by the department;

(n) ~~shall~~ operate and maintain a statewide telecommunications network for the use of state government, political subdivisions, and other participating entities under terms and conditions established by the department;

(o) ~~shall~~ ensure that the statewide telecommunications network is properly maintained. The department may establish a centralized maintenance program for the statewide telecommunications network.

(p) ~~shall~~ coordinate public safety communications on behalf of all state agencies as provided for in 2-17-541 through 2-17-543;

(q) ~~shall~~ manage the state 9-1-1 program as provided for in Title 10, chapter 4, part 3;

(r) ~~shall~~ provide electronic access to information and services of the state as provided for in 2-17-532;

(s) ~~shall~~ provide assistance to the legislature, the judiciary, the governor, and state agencies relative to state and interstate information technology matters;

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

(t) ~~shall~~ establish rates and other charges for services provided by the department;

(u) ~~must~~shall accept federal funds granted by congress or by executive order and gifts, grants, and donations for any purpose of this section;

(v) ~~shall~~ dispose of personal property owned by it in a manner provided by law when, in the judgment of the department, the disposal best promotes the purposes for which the department is established;

(w) ~~shall~~ implement this part and all other laws for the use of information technology in state government;

(x) ~~shall~~ report to the appropriate interim committee on a regular basis and to the legislature as provided in 5-11-210 on the information technology activities of the department; and

(y) ~~shall~~ represent the state with public and private entities on matters of information technology.

(2) If it is in the state's best interest, the department may contract with qualified private organizations, foundations, or individuals to carry out the purposes of this section.

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

(3) The director of the department shall appoint the chief information officer to ~~assist in carrying~~ carry out the department's information technology duties."

{*Internal References to 2-17-512:*

2-15-40X 2-17-513X 2-17-514X 2-17-516X
2-17-516X 2-17-516X 2-17-516X 2-17-516X
2-17-516X 2-17-516X 2-17-531X 17-5-807X }

Section 5. Section 2-17-516, MCA, is amended to read:

"2-17-516. Exemptions -- university system -- office of public instruction -- national guard. (1) Unless the proposed activities would detrimentally affect the operation of ~~the~~ a central computer center or the statewide telecommunications network, the office of public instruction is exempt from 2-17-512(1)(k) and (1)(l).

(2) Unless the proposed activities would detrimentally affect the operation of ~~the~~ a central computer center or the statewide telecommunications network, the university system is exempt from:

(a) the enforcement provisions of 2-17-512(1)(d) and (1)(e) and 2-17-514;

(b) the approval provisions of 2-17-512(1)(f), 2-17-523, and 2-17-527;

(c) the budget approval provisions of 2-17-512(1)(g);

(d) the provisions of 2-17-512(1)(k) and (1)(l); and

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

(e) the transfer provisions of 2-17-531.

(3) The department, ~~upon notification of~~ shall review proposed activities by the university system or the office of public instruction, ~~shall and~~ determine if whether the a central computer center or the statewide telecommunications network would be detrimentally affected by the proposed ~~activity~~ activities.

(4) For purposes of this section, a proposed activity affects the operation of ~~the a~~ a central computer center or the statewide telecommunications network if it detrimentally affects the processing workload, reliability, cost of providing service, or support service requirements of ~~the a~~ a central computer center or the statewide telecommunications network.

(5) When reviewing proposed activities of the university system, the department shall consider and make reasonable allowances for the unique educational needs and characteristics and the welfare of the university system as determined by the board of regents.

(6) When reviewing proposed activities of the office of public instruction, the department shall consider and make reasonable allowances for the unique educational needs

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

and characteristics of the office of public instruction to communicate and share data with school districts.

(7) Section 2-17-512(1)(u) may not be construed to prohibit the university system from accepting federal funds or gifts, grants, or donations related to information technology or telecommunications.

(8) The national guard, as defined in 10-1-101(3), is exempt from 2-17-512."

{*Internal References to 2-17-516:*
2-17-513A 2-17-515X }

Section 6. Section 2-17-521, MCA, is amended to read:

"2-17-521. State strategic information technology plan -- biennial report. (1) The department shall prepare a state strategic information technology plan. The department shall seek the advice of the board in the development of the plan.

(2) The plan must:

(a) reflect the policies ~~as~~ set forth in 2-17-505 and be in accordance with statewide standards and policies established by the department;

(b) establish the statewide mission, goals, and objectives for the use of information technology, including

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

goals for electronic access to government records,
information, and services; and

(c) establish the strategic direction for how state agencies will develop and use information technology resources to provide state government services.

(3) The department shall update the plan as necessary. The plan and any updates must be distributed as provided in 2-17-522.

(4) The department shall prepare a biennial report on information technology based on agency information technology plans and performance reports required under 2-17-524 and other information considered appropriate by the department. The biennial report must include:

(a) an analysis of the state's information technology infrastructure, including its replacement value, condition, and capacity;

(b) an evaluation of performance relating to information technology;

(c) an assessment of progress made toward implementing the state strategic information technology plan;

(d) an inventory of state information services, equipment, and proprietary software;

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

(e) state agency budget requests for major projects;

and

(f) other information as determined by the department or requested by the governor or the legislature."

{*Internal References to 2-17-521:*

2-17-512X 2-17-514X 2-17-524 X 2-17-527X

3-1-702X }

Section 7. Section 2-17-524, MCA, is amended to read:

"2-17-524. State agency information technology

plans -- form and content -- performance reports. (1)

Each state agency's information technology plan must include but is not limited to the following:

(a) a statement of the agency's mission, goals, and objectives for information technology, including a discussion of how the state agency uses or plans to use information technology to provide mission-critical services to Montana citizens and businesses;

(b) an explanation of how the state agency's mission, goals, and objectives for information technology support and conform to the state strategic information technology plan required in 2-17-521;

(c) a baseline profile of the state agency's current information technology resources and capabilities that:

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

(i) includes sufficient information to fully support state-level review and approval activities; and

(ii) will serve as the basis for subsequent planning and performance measures;

(d) an evaluation of the baseline profile that identifies real or potential deficiencies or obsolescence of the agency's information technology resources and capabilities;

(e) a list of new projects and resources required to meet the objectives of the agency's information technology plan. The investment required for the new projects and resources must be developed using life-cycle cost analysis, including the initial investment, maintenance, and replacement costs, and must fulfill or support ~~an~~ a state agency's business requirements.

(f) when feasible, estimated schedules and funding required to implement identified projects; and

(g) any other information required by law or requested by the department, the governor, or the legislature.

(2) Each state agency's information technology plan must project activities and costs over a ~~6-year~~ 4-year time

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

period, consisting of the biennium during which the plan is written or updated and the ~~2~~ subsequent ~~bienniums~~ biennium.

(3) Each state agency shall prepare and submit to the department a biennial performance report that evaluates progress toward the objectives articulated in its information technology plan. The report must include:

(a) an evaluation of the state agency's performance relating to information technology;

(b) an assessment of progress made toward implementing the agency information technology plan; and

(c) an inventory of agency information services, equipment, and proprietary software.

(4) State agencies shall prepare agency information technology plans and biennial performance reports using standards, elements, forms, and formats specified by the department."

{*Internal References to 2-17-524:*

2-17-521X 2-17-523X 2-17-527X }

Section 8. Section 2-17-546, MCA, is amended to read:

"2-17-546. Exemption of law enforcement telecommunications system -- exception. The provisions of this part do not apply to the law enforcement telecommunications system or its successor except for the

CD-ROM Draft Copy

Last printed 1/6/2015 10:27:00 AM

6101_07_006_Technology_Act_FINAL-1

provisions dealing with the purchase, maintenance, and allocation of telecommunication facilities and information technology using the statewide telecommunications network. ~~However, the~~ The department of justice shall cooperate with the department to coordinate the telecommunications networks of the state."

{*Internal References to 2-17-546: None* }

-END-

Apprentice Program Discussion

Montana State Government

Why an Apprenticeship Program?

- Improve recruitment and retention efforts in hard to fill positions
- Can “shape” the employee to Agency specific needs
- Fills the skill gap of the employer by training to the occupation both on the job and through classroom instruction
- Addresses succession planning by providing a pipeline of skilled workers

How does an Apprentice Program work?

- Must meet Federal and State standards
- Competitive recruitment process
- Employee receives a nationally recognized certification
- May also receive a degree (depending upon program design)
- Customizable to the Agency’s needs
- Employee becomes permanent employee and is guaranteed a job upon successful completion
- Must follow apprentice requirements set forth in contract
- Successful completion is a condition of employment
- Graduated pay scale. Apprentice starts below existing employees - and at completion, employee should be at low end of pay scale for occupation with room to continue growing
- Pay is set by the hiring Agency’s pay plan – graduated over term of apprenticeship
- Requires existing employees to commit time to OTJ training and close supervision
- Typically requires a financial commitment by the Agency to pay for classroom instruction. Can be done on a reimbursement-at-completion model if desired.
- The coursework can be waived in part or totally if comparable ‘previous education’ is documented and applicable to the occupation
- In return for OTJ training and certification, employee may be required to stay on job for X years
- NOT an internship

Enterprise-wide “issues” to consider

- Centralized committee review of apprentice standards and progress evaluation
- Standard union contract language – condition of employment
- Standard non-union contract language – condition of employment
- Consistent application of FLSA – paid time, classroom time, and study time
- Standardization of pay as a % of Agencies pay scales
- Consistent classification of occupations between agencies
- Interagency competition for same talent

Enterprise Security Risk Assessment

November, 2014

Presented by:

Lynne Pizzini, CISSP, CISM, CIPP
Deputy Chief Information Officer and
Chief Information Security Officer
State Information Technology Services Division
444-9127
lpizzini@mt.gov



-----*State Information Technology Services Division*-----



Overview

Funded by HB10 - 2013 Legislative Session

Five participating agencies:

- Department of Administration
- Department of Justice
- Department of Labor
- Department of Revenue
- Department of Public Health and Human Services

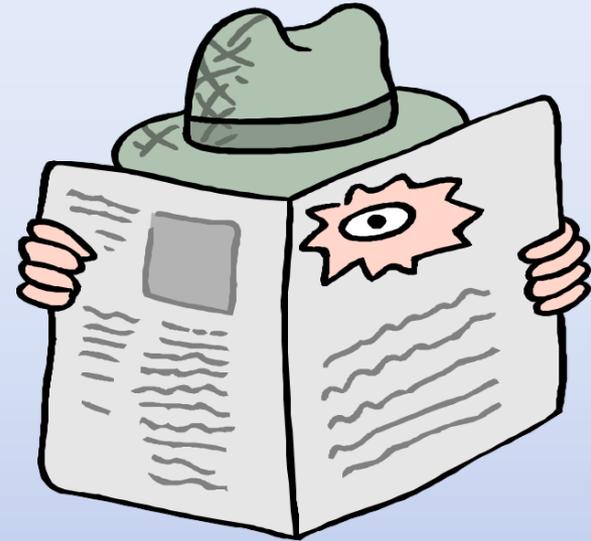


Enterprise Risk Assessment Project Description

To evaluate the security of enterprise as well as high-profile, high-value information systems at a limited number of agencies, and identify vulnerabilities discovered during the evaluation.



Overview Continued



- Request for Proposal (RFP) was completed in the spring of 2014 and a vendor was chosen to conduct the work.
- The project kickoff meeting was held June 9, 2014.
- The Final reports were provided to participating agencies on October 17, 2014.
- The presentation of the reports was completed on November 5, 2014.

General Comments – Important Factors for Successful Risk Management

- Support and Sponsorship by top level management
- A comprehensive plan
 - Enterprise Approach
 - Governance
 - Standard (NIST)
 - Policies
- Full participation – Management to end-users
- Up-to-date Tools
- Good information security behavior
- Ongoing vulnerability assessments



Overall Recommendations

- Conduct periodic risk assessments
- Create or update policies and procedures based on the risk assessment recommendations
- Evaluate effectiveness of policies and procedures
- Provide for:
 - Security planning
 - Security training
 - Continuity of Operations
 - Independent and periodic evaluation of controls



Findings - Categories

- Managerial – Controls that address the management of risk within the organization
- Operational – Controls that are put into place to improve the security of certain systems that are implemented by people
- Technical – Controls that are dependent up on the proper functioning of an information system
- Physical – Controls that address physical access to an information system
- Social Engineering – The practice of obtaining confidential information by manipulating and/or deceiving people.

Managerial Findings

- Incident Response
- Configuration Management
- Ongoing Assessments
- Interconnection Security Agreements



Operational Findings

- Log Review
- Continuous Monitoring
- Accreditation boundaries – network compartmentalization



Technical Findings



- Encryption for data at rest
- Patching
- Application Hardening
- Legacy and Unsupported software
- Various Web application vulnerabilities

Physical Findings

- Secured areas need doors with good locks
- Security of computer equipment
- Security of shred bins
- Viewable records



Social Engineering Findings

- Four scenarios
- Did not notify service desk or security personnel for first scenario – 18% fail rate
- Other scenarios – 50% fail rate



Conclusion

- Lots of work to do
- Collaboration is needed
- Enterprise Security Program Implementation
- Top 5



ANY QUESTIONS?

