

**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.