

CNIC Governing Board Meeting Minutes – July 10, 2006

Approved 8/14/06

Attendees:

Agency:	Board Representative:	CIO or Representative:
DAS	Lindsay Ball/Kris Kautz	Mike Zanon
DCBS	Greg Malkasian	Dan Adelman
Corrections	Max Williams	John Koreski
Education	Doug Kosty	Baron Rodriguez
Employment	Bill Fink	Curt Amo
Forestry	Clark Seely	Sandy Jefferson
Housing & Community Services	Rick Crager	
Human Services	Fariborz Pakseresht	Bill Crowell
State Police	Greg Willeford	David Yandell
Revenue	Elizabeth Harchenko	Stan McClain
ODOT	Mike Marsh	Ben Berry
Veterans' Affairs		Herb Riley

State Data Center: Mark Reyer

Project Office: Sarah Miller

Accenture: Mike Dawson, Kari Ensminger

Others: Kate Coffey, Ken Disbrow, Raelynn Henson, Keith Kohan, Jerry Korson, Merrilyn Nixon, Theresa Masse

1. Opening Comments

Lindsay Ball reaffirmed his intention that directors rather than delegates attend this meeting as much as possible.

It was moved and seconded to approve the June 12 minutes as written. The motion passed.

Lindsay noted that the JLCIMT has requested information regarding agencies' intentions related to potential requests for new IT positions.

ACTION: All directors need to send Lindsay a brief statement respective to whether or not they will be requesting additional FTE for functions that were sent to the SDC. House Bill 5156 identifies the positions that are being phased out. Note specifically whether or not any of the FTE functions being transferred to the SDC will be backfilled. These statements will be forwarded to Dallas Weyand to provide to the JLCIMT. This is due to Lindsay no later than August 15.

2. Quarterly QA Report

Ken Disbrow distributed his report to the board. There are some small risks associated with moving the remainder of the servers. The only remaining high risk pertains to the size and complexity of the project and this cannot be helped. During the last report agencies were concerned about internal projects being neglected due to the resource strain associated with the project. This has since been resolved. During the upcoming lessons learned initiative, Ken will be contacting the directors to ask about desired participation. This is not an audit of the project but a compilation of feelings and lessons learned amongst the stakeholders.

3. Project Management Report

Sarah Miller introduced herself and distributed the report in Julie Bozzi's absence. The transition of the three largest data centers is complete in addition to the migration of Housing and Community Services. There is an opportunity to accelerate the schedule if agencies are willing.

Everything from an infrastructure perspective is on schedule. Security infrastructure is listed as "pending" due to staffing issues which are being addressed. An interim change management and

incident management process has been implemented. Transition agreements have been written for the stabilization period. This covers the time after each agency has moved until the SDC takes over operations. Processes and communications for the remaining migrations is the next focus of the SDC. Stabilization scorecards are also being built.

Some training will have to be done to ensure that rotational staff supporting SDC functions can continue to do so until permanent staff members are hired. Mark Reyer continues to address software licensing and will be reporting back as soon as possible. Agency account managers will be assigned as staff is hired. These individuals will work directly with each agency. A service desk and escalation protocols will be established at the SDC. Once stabilization is complete, a formal service level agreement will be negotiated with each agency. And the Steering Committee is working on clarifying its new role as an advisory board.

Though the agency account managers will provide a direct line of contact to the agencies from a relationship perspective, technicians will also have contacts and a service desk will be available.

4. Administrator's Report

Mark Reyer distributed an extract of the SDC two-year strategic plan. Completing the migration of the equipment and the hiring of the SDC staff is only the first step. There are three components of the SDC strategic plan:

1. Migration
2. Standardization-consolidation
3. Optimization.

The first thing to address is accounting. Hardware, software, maintenance and people will need to be properly placed in the accounting system. This will include the delineation of software as it pertains to each agency. Where the software is running will influence this process. This will be addressed from the ground up for invoicing purposes.

Quality controls and reporting will be addressed. Benchmarks will be identified for areas such as performance and availability. This is true for capacity and asset utilization. There will be an effort to ensure that assets are being used to their fullest efficiency. Business process in general will be addressed.

The Information Technology Infrastructure Library (ITIL) will be used as a framework with a comprehensive set of processes and policies to use in managing operations. Customer service will be addressed to ensure that it is easy for customers to communicate expectations, issues, etc. There is a large initiative underway to set standards and define the architecture of the SDC. Implementation of security is part of this. Smaller agencies will want to separate storage from the computer platform. This is a much better way to utilize expensive assets and to ensure back-up. On the server side, there are many options including virtualization and blade servers. This also addresses a great deal of savings in power usage. One of the first actions will be to migrate from servers that are quite old to new equipment. There are also some servers that are not up to liability standards and this will need to be addressed quickly. The goal is to achieve enterprise class computing throughout the data center. An enterprise management system will also be put in place in the command center. This will enable 24 hour monitoring of all systems at all times so that any issues or failures will be identified, addressed and communicated immediately.

A service catalog exists that defines functions but will be of little use to anyone who is not a technician. Mark has also put together a diagram to explain the IT infrastructure that is within scope of the SDC and includes those things that are not managed by the SDC. This was used in presentations with legislators and it was well received. This may be a useful tool for the directors.

The Finance Committee is working very closely with Mark. Lindsay reiterated that those who have a chance to visit the SDC should do so. Mark has noted to Lindsay many times that there is an extraordinary amount of talent amongst the state workers involved in this project.

5. Human Resources Report

Jerry Korson noted that the administrative team at the SDC is finalizing their decisions based on the candidates first ("A") choice for the first round of hiring. Before they can be notified, the team wants to ensure that everyone has been fully considered. Directors and CIOs will be notified of the status of each applicant as formal offer letters are about to go out. Salary information will be included in offer letters. Once these letters go out, the management team will reevaluate to understand what the second round of hiring looks like. The goal is to know where each applicant stands by the end of this week. Then letters will be drafted and will go out no later than the middle of next week. HR departments in each agency will be notified a couple days before letters go out. They will be instructed to share this information with CIOs and directors.

6. Finance Committee Report

Elizabeth Harchenko reported as chair of the committee. They have been meeting with agency representatives to verify what agency dollars are attributed to data center activities. The committee will be working with Mark on his budget for the next biennium and to develop a services charge back model. A very expensive fixed asset belonging to all of the agencies will need to be addressed. Any major change to the way any agency does business such as contracting out work to a third party vendor should be communicated to the finance committee as it will likely have impact on the other agencies. There are discussions around creating a formal policy or protocol to address this issue. Once this issue has been vetted within the committee, some sort of communication will go out to the directors to prompt a conversation at their level. Lindsay noted that any agency with a current program housed in the data center that will be pulled out of the SDC later will cause everyone else's fees to go up. A full report of status for the rest of the biennium will be available by the board's August 14 meeting. Lindsay thanked Elizabeth for her many hours of additional work associated with this committee.

7. Budget Status Report

Kate Coffey distributed a statement of operations as of May 2006. June does not close until this Friday and therefore could not be communicated today. All but one agency has paid their assessment. The June assessments include the previously discussed refund so everyone's bill was less. The next debt service is due around the end of October.

8. Other Business

Theresa Masse presented on security breaches that have occurred recently. She noted that this is not exclusive to CNIC agencies. A survey was done of many national organizations that showed 84 percent had experienced security breaches in the last year. A number of the most recent issues are related to stolen laptops. Most of the breaches in general are due to employees not following security policy. 75 percent of security breaches are internal. There is no way to ensure that breaches will not happen. A number of security policies including appropriate use will be distributed by the Enterprise Security Office (ESO). Agencies should do everything they can to communicate these policies to employees and monitor enforcement.

Laptop security:

- Businesses need to know exactly who has laptops
- Business reasons for having laptops need to be identified
- Confidential information stored on laptops must be identified as well as a business requirement for doing so. (If no business requirement exists, these laptops should be purged of all such information. If a business requirement does exist, these laptops need to be properly protected.)

A lot of work can be done to address these issues but it must be recognized that there is nothing that can be done to completely stop it. Knowing this, we need to always be able to report to the Legislature that everything that could be done to protect information was done. Education will be extremely important moving forward. Addressing access to the Internet and to confidential information to assess the actual business need can be one easy way to quickly reduce risk. All technology must be considered including smaller items such as cell phones.

Addressing agency leadership is the first step as agency leadership is ultimately responsible for the security of their information. The security office will be surveying each agency to find a baseline of current security and to address those things that can be done immediately to better security. A commitment will be needed from leadership to ensure that this is done properly. There are some legislative responsibilities that must be met regarding assessments. Every agency is at risk and every agency will experience a breach at some point. This is why we must be extremely prepared and doing our due diligence to prevent as much interference as possible. Any agency doing its own assessments should feed this information back to the ESO so that it can become part of the assessment prepared for the Legislature.

Elizabeth shared some Department of Revenue lessons learned after their recent breach. Employees had been given permission to use the Internet on their breaks and personal time and that privilege has since been revoked. It cannot be conveyed in too many ways or too often how easy it is for one employee to cause a breach in security. Conversely, there needs to be a balance between instructing employees about what not to do and giving them comfort in reporting anything strange without too much threat based on a mistake they made. Managers have also been asked to monitor their employees. Have a plan in place for how to handle this when it happens to your agency. As noted, it is not a matter of if but when and the best way to be prepared is to have a plan for dealing with the situation and communicating the issue internally and externally.

The ESO is developing a security standard for agencies to create consistency. Lindsay reiterated the need for a contingency plan and posed the question, "how would you respond if the Legislature suddenly directed that there would be no more personal use of computers or use of laptops." Forestry is doing a review of their own laptops and Internet accessible computers to understand the actual business needs versus actual current usage. Lindsay noted that it is important to illustrate to the Legislature and the citizens of Oregon that everything that can be done to protect information is being done. Lindsay asked directors to bring their comments on security to the agency heads meetings.

It was noted that the use of the Internet itself is likely not the real issue so much as the nature of the use, i.e. downloads.

Governance Model: The Secretary of State Audit report will come out in the next week or week and a half. A plan on how this board will function going forward is already in place but some discussion needs to be had before anyone takes action. It was noted that the report will likely have some clear recommendations. Lindsay talked about the Secretary of State's desire to have one person accountable for the project. It was suggested that the board wait for the audit report and then discuss the results and how to move forward with ongoing governance. It is not inappropriate that this board would want to readdress the previously decided upon governing model because of the length of time since its development.

Governance model considerations:

- The director of DAS as the SDC administrator's boss
- SDC administrator is accessible to the agency directors
- Extent to which the Governing Board is an advisory board
- The role and authority of the CIO advisory board
- Whether or not an interagency agreement will be necessary.

The Legislature's quality assurance request for proposals was discussed. It was noted that approximately \$200,000 is being spent to review three projects including CNIC. Timeframe of the RFP:

- Proposals are due July 19 (selection process begins)
- The final contract is to be signed around August 3
- An interim report will be made to JLCIMT in September
- A final report will go to the JLCIMT in November.

CNIC Governing Board Meeting
July 10, 2006

Approved 8/14/06

Next Regularly Scheduled Meeting

Monday, August 14, 2006

3 - 4:30 p.m.

DAS West ~ Conference Room A