

## MINUTES

### JOINT COMMITTEE ON INFORMATION TECHNOLOGY

September 23-24, 2009  
Room 535-N—Statehouse

#### Members Present

Representative Joe McLeland, Chairperson  
Senator Tim Huelskamp, Vice-chairperson  
Senator Tom Holland  
Senator Mike Petersen  
Senator Vicki Schmidt  
Senator Chris Steineger  
Representative Mike Burgess  
Representative Harold Lane  
Representative Jim Morrison

#### Staff

Julian Efird, Kansas Legislative Research Department  
Aaron Klaassen, Kansas Legislative Research Department  
Dennis Hodgins, Kansas Legislative Research Department  
Jonathan Tang, Kansas Legislative Research Department  
Norm Furse, Office of the Revisor of Statutes  
Daniel Yoza, Office of the Revisor of Statutes  
Don Heiman, Legislative Chief Information Technology Officer  
Gary Deeter, Committee Secretary

#### Conferees

Alan Weiss, Project Manager (Application), Kansas Legislative Information Systems and Services  
Terri Clark, Project Manager (Infrastructure), Kansas Legislative Information Systems and Services  
Joe Hennes, Executive Chief Information Technology Officer  
Peggy Hanna, Deputy Project Director, Division of Accounts and Reports, Kansas Department of Administration  
Kent Olson, Director, Division of Accounts and Reports, Kansas Department of Administration  
Dr. James Lyall, Associate Vice Provost, Information Technology Services, Kansas State University

Michael Erickson, Associate Vice President for Technology and Computing Services/Chief Information Officer, Emporia State University  
Denise Stephens, Vice Provost for Information Technology, University of Kansas  
Alan Foster, Auditor, Legislative Division of Post Audit  
Duncan Friend, Director, Enterprise Technology Initiatives, Kansas Partnership for Accessible Technology  
Robert Waller, Executive Director, Kansas Board of Emergency Medical Services  
Joe Morland, Project Manager, Kansas Board of Emergency Medical Services  
Susan Duffy, Executive Director, Kansas Corporation Commission  
Tom Ryan, Chief Information Officer, Kansas Corporation Commission  
Marty Wiltse, Chief Information Officer, Kansas Turnpike Authority  
David Kerr, Secretary, Kansas Department of Commerce  
Anthony Schlinsog, Chief Information Officer, Kansas Department of Transportation

### **Others Attending**

See attached list.

### **Wednesday, September 23 Morning Session**

The Chairperson called the meeting to order at 10:10 a.m. and welcomed Don Heiman, Legislative Chief Information Technology Officer (CITO), who introduced Bill Roth, Kansas Chief Information Architect; Mr. Roth announced that the Kansas Department of Corrections had received a national Best Practices award for its preparatory infrastructure project before launching two enterprise-wide projects.

The Chairperson recognized Dave Larson, Director, Legislative Computer Services, Legislative Administrative Services (LAS), who announced two staff changes: Terri Clark promoted to Assistant Director/Infrastructure, and Mike Baker, recently hired as a Data Center Technician.

Mr. Heiman updated the Committee on the Kansas Legislative Information Systems and Services (KLISS) project. The project, begun in 2004, includes 21 sub-systems and offers comprehensive infrastructure and application initiatives for all phases of legislative activity (Attachment 1). Mr. Heiman presented details of the various systems to show their seamless functionality through the various legislative processes. He stated that both the application and infrastructure aspects of the project are on time and on budget (application with vendor Propylon, \$6 million; infrastructure with VMWare and Avamar, \$1.1 million), and the completed system will have interfaces with the Internet, intranet users, the State Printer, KanWIN, and the KAN-Ed network. He acknowledged the tight schedule for completion of the first sub-system, Law-Making Base System, by November 30, 2009, but said the deadline would be met. KLISS is scheduled to go live in January 2011, and the project will be completed by July 31, 2011.

Answering questions, Mr. Heiman said the backup system to Wichita will have ten gigabytes-per-second bandwidth. He responded that the methodology for the project was established by 1997 SB 5, that the Information Technology Executive Council (ITEC) will certify the project, and that he will provide project plans to Committee members. He distributed Attachment 2 to show the acceptance criteria used with vendor Propylon.

Alan Weiss, Project Manager for KLISS Applications, reviewed the application information provided by Mr. Heiman. Answering a question regarding deadlines, Pat Saville, Secretary for the Kansas Senate, said the work can be done on schedule by using legislative staff added during the legislative session.

Terri Clark, Project Manager and Assistant Director, KLISS Infrastructure, commented that the choice of VMWare has proved beneficial. Answering a question regarding a possible simultaneous power failure at both the Topeka and Wichita sites, she replied that the only loss of data would be in the pipeline; none at either site would be lost. Mr. Heiman replied that the project can be completed even with past budget cuts; if there are further cuts, it will complicate meeting project requirements.

Joe Hennes, newly appointed Executive CITO, commented on his work history, introduced Morey Sullivan, Chief Financial Officer, Division of Information Systems and Communications (DISC), and Mary Grace, Manager, Kansas Information Technology Office, and reviewed the agency quarterly reports for April-June 2009 (Attachment 3). He stated that of 27 active projects totaling \$159 million, 20 are in good standing, three are in caution status, and three have been recast. He noted one planned project, the Kansas Department of Education's (KSDE's) Kansas Statewide Electronic Transcript System (estimated cost, \$1.8 million) and commented on 12 approved projects, including the Kansas State Historical Society's Kansas Enterprise Electronic Preservation Project (KEEP) and deployment of the Kansas Department of Labor's (KDOL's) Unemployment Insurance Modernization Project. He listed the completed projects, among which are the Kansas Department of Correction's Enterprise Architecture Plan mentioned earlier, the Kansas Department of Revenue's Division of Motor Vehicles Modernization-Mobilization Request for Proposal (RFP), the data warehouse of the KSDE, the third phase of the Vital Statistics Integrated Information System/Electronic Death Registration System (Kansas Department of Health and Environment), and the collaborative Traffic Record System Development and Implementation Program created by the Traffic Records Coordination Committee under the auspices of the Kansas Department of Transportation (KDOT).

A member requested total cost and number of bidders for the KSDE Enterprise Data System. Mr. Hennes said the project was begun March 2006, and was completed in May 2009. Mr. Roth, replying to a question about the Kansas Department of Commerce Regional Education and Workforce Access Remote Delivery, said the completion date was extended to address bandwidth problems.

Mr. Hennes, continuing his comments on active projects, said KDOL, after several problems with vendors, was beginning to build and deploy the Unemployment Insurance Modernization project. Replying to a question, he said an extensive review was done to correct earlier errors. Members urged Mr. Hennes to monitor the project more closely.

Mr. Hennes noted that the lack of a report from the Kansas Lottery was caused by a misunderstanding between the agency and the vendor. Answering a question, Ed Van Petten, Executive Director, Kansas Lottery, said the casino at Dodge City will be ready for its scheduled opening in mid-December. Mr. Hennes made special note that the Kansas Historical Society's KEEP project, initially funded by an Information Network of Kansas grant, was approved by all three branches of CITOs; it will preserve documents in electronic form and make available to the public a certified copy of a document. Regarding DISC's KanWIN (Kansas Wide-Area Information Network) upgrade, Mr. Hennes said the completed project will prepare Kansas for a future technology, Unified Communications.

### Afternoon Session

Peggy Hanna, Deputy Project Director, Division of Accounts and Reports, Kansas Department of Administration, gave a status report on the State-wide Financial Management System, now called the Sunflower Project (Attachments 4 and 5). She noted the benefits of the new system and commented on the scope of the project; it replaces STARS (State-wide Accounting and Reporting System), de-commissions over 60 agency systems, interfaces with 50 current agency systems, including the seven state universities, and enhances SHaRP (State-wide Human Resources, Reports and Payroll). She listed the project's current accomplishments and noted that the new system will be more adaptable and provide greater transparency.

Answering questions, Ms. Hanna replied that:

- The Regents and the KSDE will continue to maintain their current financial systems.;
- Inclusion of the Regents' student managements systems would add too much complexity to the system;
- The University of Kansas Medical Center is using PeopleSoft 9.0; and
- The project is still on time and on budget.

Kent Olson, Director, Division of Accounts and Reports, Kansas Department of Administration, replied to a question that the Regents and KSDE will include the proper data to participate in the KanView transparency initiative. He responded that the data warehouse will enable a person to search state-wide to determine how much a vendor is receiving from various state agencies or how much a given agency is paying a vendor.

When Ms. Hanna replied that fewer than 50 modifications were being made to the new system, members expressed concern that the modifications could complicate upgrades; the Committee requested a list of the modifications.

Dr. James Lyall, Associate Vice Provost, Information Technology Services, Kansas State University, testified before the Committee in response to a Legislative Post Audit report on IT security. He said that the University has addressed 18 of the Post Audit's 26 recommendations, and the remaining eight are in the final stages of review (Attachment 6).

Michael Erickson, Associate Vice-President, Technology and Computing Services/Chief Information Officer, Emporia State University, also testified in response to the Post Audit report (Attachment 7). He stated that a formal project security plan was developed and is being implemented, with two progress reports already submitted to Post Audit. A final report will be submitted to the Legislative Division of Post Audit by January 1, 2010.

Denise Stephens, Vice-Provost for Information Technology Services, University of Kansas, also responding to the Post Audit recommendations, commented that the University is nearing full implementation of the recommendations (Attachment 8). 28 of the 35 recommendations have been addressed, and the remaining eight are nearing implementation.

*Following presentations in response to Post Audit's public report, Senator Vicki Schmidt made the following motions:*

*I move that the open meeting of the Joint Committee on Information Technology in Room 535-N of the Kansas Statehouse be recessed for a closed, executive meeting to commence immediately in Room 535-N of the Statehouse pursuant to subsection (b)(13) of K.S.A. 2008 Supp. 75-4319 for a discussion of the security of the information systems of the State Board of Regents for Emporia State University, the University of Kansas, and Kansas State University, that are under the supervision and control of the State Board of Regents. The subject of security is under consideration by the Joint Committee on Information Technology, because open discussion would jeopardize the security of the information systems. The Joint Committee on Information Technology will resume the open meeting in Room 535-N of the Statehouse at 3:45 p.m., and that this motion, if adopted, be recorded in the minutes of the Joint Committee on Information Technology and be maintained as a part of the permanent records of the Committee.*

*The motion was seconded by Representative Morrison and was unanimously passed.*

The Chairperson announced that Alan Foster from Legislative Post Audit was necessary to aid the Committee in the closed meeting. The Committee went into executive session at 3:15 p.m. The open meeting resumed at 3:45 p.m.

Duncan Friend, Director, Enterprise Technology Initiatives, Kansas Partnership for Accessible Technology (KPAT), reviewed progress in providing online information for those with visual or auditory limitations (Attachment 9). He illustrated advances in technology to enhance communication, referenced Information Technology (ITEC) Policy 1210, and noted lawsuits for entities that failed to address accessibility concerns. He stated that Governor's Executive Order 08-12 established KPAT, which will serve as a resource for various stakeholder communities.

### **Thursday, September 24 Morning Session**

Robert Waller, Executive Director, Kansas Board of Emergency Medical Services (KBEMS), introduced Joe Morland, Project Manager, Kansas Emergency Medical Information System, who by remote phone gave a visual demonstration to the Committee of how information is gathered and communicated on a typical EMS call. He said that the system, built by vendor Image Trend, provides web access, so that data can be input in real-time during patient transport and can be transferred to the destination hospital by the time the patient arrives. The system also creates required reports for other agencies and for the federal government.

Answering questions, Mr. Waller replied:

- 42 services currently have signed on to use the system, and 63 other services will be added as training is completed;
- Data transmission for reports to other agencies is seamless, including reports to the Trauma Registry at the Kansas Department of Health and Environment;
- Since the annual cost for the system is only \$65,000, KBEMS is able to offer the service free to all stakeholders. All that is needed is a computer and web access;

- Hospitals like the service. Patient-care reports can be transmitted immediately; billing reports require additional time;
- By 2012, KBEMS hopes to have all 170 services active with the new system. Some services have their own system, which they are currently reluctant to relinquish; and
- Initially KBEMS provided free Panasonic hardened laptops when a service signed on to the system; however, at \$3,500-plus per laptop, that practice has been suspended unless federal stimulus monies become available.

Susan Duffy, Executive Director, Kansas Corporation Commission (KCC), commented on agency's 2010 Business Process Innovation and Improvement Project (BPI<sup>2</sup>), which, in spite of budget cuts, is progressing. She introduced Tom Ryan, Information Technology Director, KCC, who provided an update on the project (Attachment 10). An RFP was issued in December 2008 to automate e-filing, document and case management, and work flow. Of the eight bids submitted, ACO Information Services of Mobile, Alabama, was selected; the final bid was \$550,000 for software and implementation support services. After selecting an experienced project manager and an independent validation service and receiving CITO approval for Phase I, the KCC held an implementation kick-off meeting on August 11, 2009. BPI<sup>2</sup> will be implemented in a series of seven iterations. Mr. Ryan listed the project goals and the iteration sequence.

Alan Foster, an auditor for Legislative Post Audit, briefed the Committee on an audit of state agency network passwords and security updates (Attachment 11). Of the five agencies reviewed, three agencies had weak password policies, two had weak password settings; the auditors were able to crack up to 58 percent of the passwords. He stated the reviewed agencies did well installing security patches on operating systems, but less well installing patches on applications. Mr. Foster said that Post Audit's recommendations include:

- Each agency addressing shortfalls in its password protection;
- Regularly updating applications with security patches; and
- Education of all state agencies by the State's Enterprise Security Office regarding vulnerability scanning.

Mr. Foster suggested mandatory vulnerability scans from the Enterprise Security Office. Answering questions, Mr. Foster replied that some agencies do vulnerability scans, but the practice is not widespread. He responded that a state-wide password policy has been discussed by the ITEC Security Council. He replied that biometric passwords have not yet proved reliable.

Marty Wiltse, Chief Information Officer, Kansas Turnpike Authority (KTA), testified before the JCIT in response to previous Committee concerns. He identified common computer projects between KDOT and KTA (800 MHz radio system, KANROAD 511, SCAN weather systems) and noted a cooperative venture to implement KDOT's Intelligent Transportation System on I-70 from Topeka to Kansas City and on I-35 south of Wichita (Attachment 12). In response to a question about sharing road design software, Mr. Wiltse replied that the software is licensed per computer unit. He noted the joint effort between KDOT and KTA on the East Topeka interchange, the Emporia interchange, and the automated toll station being built at Leavenworth. A member commended the text message service. Mr. Wiltse said the lower power of the 1610 AM broadcast service leaves gaps in coverage. He will consider putting the 511 information on the KTA website.

David Kerr, Secretary, Kansas Department of Commerce, presented information on the State Broadband Project (Attachment 13). He explained that the project is being funded by two federal agencies (the U.S. Department of Commerce and the U.S. Department of Agriculture) in coordination with the Federal Communications Commission using American Recovery and Reinvestment Act grants, a partnership that complicates the process. Further, he said each federal agency has its own program (Commerce, the National Telecommunications and Information Administration's Broadband Technology Opportunities Program [BTOP], and Agriculture, Rural Utilities Service's Broadband Initiatives Program [BIP]). Thirty to forty applications have been submitted from Kansas entities requesting more than \$216 million in grants and \$152 million in loans. Also, 30-40 national companies have made requests in relation to Kansas broadband services. The Governor has designated the Kansas Department of Commerce to be the lead agency in planning and administration; a planning committee from Commerce, DISC, KCC, State Library, KAN-Ed, Kansas Hospital Association, Kansas departments of Agriculture, Aging, Health and Environment, and others has been formed to determine state priorities. After visiting with industry leaders, the Committee developed an infrastructure scoring model and a public interest projects scoring model. To initiate mapping of available broadband services and to continue planning, the Committee received grants from the Information Network of Kansas (\$185,000) and the Kansas Farm Bureau (\$15,000); the Committee, through vendor Connected Nation, has submitted a mapping-and-planning request for over \$5 million. Mr. Kerr stated that receipt of the funds will enable the Committee to create a broadband task force and establish ongoing administration for deploying broadband services across the state. A member requested e-mail updates on the project for Committee members.

Brad Harrelson, State Policy Director, Kansas Farm Bureau Governmental Relations, submitted written testimony commenting on the state-wide deployment of broadband services (Attachment 14).

Anthony Schlinsog, Chief Information Officer, KDOT, testified before the Committee to respond to questions from a previous meeting (Attachment 15). He said the Comprehensive Program Management System Replacement fully participates in KanView, but the operational requirements of the system are not compatible with KTA requirements. He reiterated Mr. Wiltse's comments that KDOT participates with KTA in utilizing the 800 MHz radio system and the KANROAD 511 system. KDOT will include a consumable inventory module in the state-wide financial management system at a future date; adding that initially it will create too many complications with other KDOT systems. Responding to a question, he said the KDOT text message service is free, but a person must subscribe in order to receive the service.

A Committee member suggested that the JCIT Annual Report include recommendations regarding agency password and security-scan policies. Another member requested that, in order to identify the status of the Department of Labor's Unemployment Insurance Modernization Project, the agency submit a set of deliverables. The Chairperson agreed that the Committee needs to closely monitor the project. Finally, a member requested that the KDOL presentation scheduled for the next meeting be e-mailed to members before the meeting.

The Chairperson announced that, subject to Legislative Coordinating Committee approval, the Committee will meet for three days—December 14, 15, and 16. If approval is not granted, the meetings will be held December 14 and 15. The meeting was adjourned at 11:15 a.m.

Submitted by Gary Deeter  
Edited by Aaron Klaassen, Julian Efird, and Dennis  
Hodgins

Approved by Committee on:

December 15, 2009

(Date)

# JOINT COMMITTEE ON INFORMATION TECHNOLOGY

## GUEST LIST

DATE: SEPTEMBER 23, 2009

NAME	REPRESENTING
Chad Champney	KLISS
Alan Weis	KLISS
Mike Beck	LAS
Nick Byrnes	LAS
Don Gosselin	LAS
Mary Grace	EPMD
JAVIER Zaragoza	EPMD
Terri Clark	LAS
BILL ROTH	CITA
JEFF LEWIS	SRS
BRYAN DREILING	KITO
Jim Hollingsworth	INK
Ed Van Petten	Kansas Lottery
Keith Kocher	KS Lottery
Bill Cavaliere	Kansas Lottery
Berend Koops	Hein Law Firm
Sean Miller	Capital Strategies
Cheryl O'Dell	Emporia State Univ
Michael D. Erickson	Emporia State Univ.





# JOINT COMMITTEE ON INFORMATION TECHNOLOGY

## GUEST LIST

DATE: SEPTEMBER 24, 2009

NAME	REPRESENTING
Berend Koops	Hein Law Firm
John Oliver	KPIERS
Susan Duffy	KCC
Bryan Dreiling	KITD
Matt Casey	GBA
Michelle Bellus	Cap. Strategies
Tom Ryan	KCC
Marty R. Wilke	KTA
Anthony Schlinsoy	KDOT
Bill Roth	CITA
Mary Corace	EPMD
Linda Eagan	EPMD
JAVIER ZARAZUA	EPMD
Robert W	
PHIL STEVENSON	OFFICE OF STATE TREASURER
Joe Hennes	DISC
Paul Brady	Capitol Strategies

# **KLISS Status Report**

## **Joint Committee on Information Technology**

September 23, 2009

Conferees:

Don Heiman Legislative CITO

Alan Weis Assistant Director Application Development

Terri Clark Assistant Director Infrastructure

Attachment 1  
JCIT 9-23-09

# KLISS Status

1-2

Kansas Legislative Information Systems & Services = KLISS

-- Strategic Plan Approved October 2004

-- Includes Building 21 Subsystems

Law Making            5 systems

Chamber                6 Systems

Decision Support    9 Systems

Leg Interface        1 Systems

Total                    21

# KLISS Status

1-3

## Law Making

Resolutions

Bill Draft

Bill Amendment

Engrossing

Statute Creation/  
Publications

## Chamber

Bill Status

Calendars

Journals

Messages

Vote Mgmt Sys

Flagging

## Decision Support

Bill Explainer

Supplemental Notes

Fiscal Notes (Division of Budget)

Interim Committee Rpts

Appropriations

Conference Com Rpt Brief  
Claims

Confirmations

Committee Agenda &  
Minutes

Future Legislative systems include Constituent Services and Redistricting

# KLISS Status

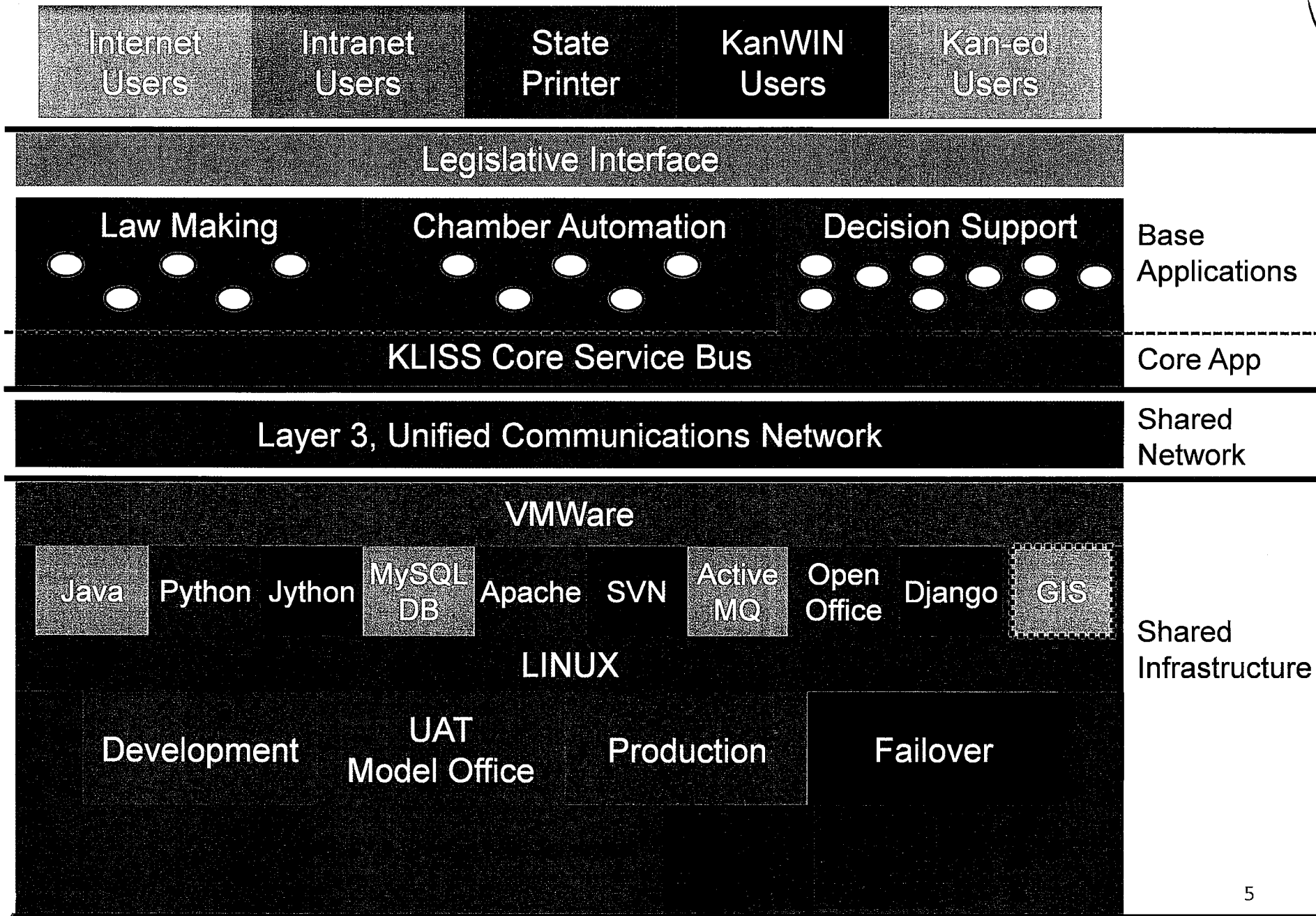
1-4

## Infrastructure and Application Initiatives

- Server and Software Consolidation
- Integrated Security
- Centrally Managed Infrastructure for operations and technical support under Terri Clark
- Centrally managed application development projects under Alan Weis

# KLISS Systems and Infrastructure

1-5



# KLISS Status

1-6

## Application is on time and on budget

- Build Propylon contract \$ 6,000,000
- Spent with vendor to date \$ 1,414,000
- Project Completes July 2011

## Infrastructure is on time and on budget

- Sub Project 1 (Vendor costs)
  - 4 Environments budget \$ 850,000
  - Spent to date (balance to sub project 2) \$ 732,000
- Sub Project 2 (Vendor costs)
  - Avamar Backup Sub Project 2 \$ 248,000
  - Spent to date \$ 248,000



# KLISS Status

- Application Risks

- Law Making acceptance due on 11/30/09

- Test scripts (scenarios) are not complete

- Propylon is on a very tight schedule for having the Law Making base system ready for testing

- Infrastructure Risks

- Tight timeline for bringing up Wichita fail over

- Current KLISS infrastructure budget must carry us through 2011 session. Savings in the Divisions from using the KLISS infrastructure should be leveraged for the good of all.

# KLISS Software Application Build Project

8-1

## Timeline:

Build contract signed (Vendor: Propylon, Inc.)	Jan 7, 2009
Project duration	Jan 2009 to July 2011
Project Initiation Document (PID) (Complete)	Mar 31, 2009
Construction Strategy and Conversion Plan (Complete)	May 31, 2009
KLISS Core System (Complete)	Aug 31, 2009
Law Making Base System	Nov 30, 2009
Vote Management System API	Mar 16, 2010
Chamber Base System	Mar 31, 2010
Chamber Journals & Messaging Base System	May 31, 2010
Legislative Interface	July 31, 2010
Chamber Calendar and Remaining Base Systems	Sept 30, 2010
Decision Support Base System	Dec 31, 2010
Conference Committee Report Briefs Base System	Feb 28, 2011
KLISS begins production during 2011 session	Jan 2011
Project closeout	July 31, 2011

# KLISS Software Application Build Project

1-9

## Budget:

Event	Date	Deliverable	Paid	Payment
Contract Signed	01/07/2009		Yes	\$454,000
Conversion Plan	05/31/2009	Deliverable 1	Yes	\$384,000
Core System	08/31/2009	Deliverable 2	Yes	\$576,000
Law Making	11/30/2009	Deliverable 3		\$576,000
Vote System API	03/16/2010	Deliverable 4		\$384,000
Chamber Base System	03/31/2010	Deliverable 5		\$384,000
Chamber Journal and Messaging Base System	05/31/2010	Deliverable 6		\$384,000
Legislative Interface	07/31/2010	Deliverable 7		\$192,000
Chamber Calendar Base System	09/30/2010	Deliverable 8		\$288,000
Chamber Remaining Base System	09/30/2010	Deliverable 9		\$288,000
Decision Support Base System	12/31/2010	Deliverable 10		\$768,000
Conference Committee Report Briefs Base System	02/28/2011	Deliverable 11		\$100,000
2011 Session Support	05/31/2011			\$668,000
Project Close Out	07/31/2011			\$554,000
<b>Total Payments (without \$600,000 contingency)</b>				<b>\$6,000,000</b>

# KLISS Software Application Build Project

1-10

## Application Risk Mitigation:

1) Law Making test scenarios not complete.

– Mitigation:

- Applying more resources to scenario development.
- Fill open positions (funded in 2010 budget)
- Documentation – Tracks scenario testing, system functionality, and output production during Model Office iterations. This will provide a weekly status leading up to delivery and acceptance.

2) Propylon is on a very tight schedule to have Law Making components ready for Model Office testing.

– Mitigation:

- The KLISS Core System is in place which provides much of the underlying functionality.
- Part of Law Making integrates with Chamber Automation and Decision Support which will be completed after November 2009.

# KLISS Infrastructure Project

11-1

## Timeline:

Sun Computers equipment evaluated	December, 2008
Server and SAN Quote Process	Jan 2009 to March 2009
Topeka Data Ctr Servers and SAN Installed	May, 2009
Project Initiation Document (PID) (Complete)	July 24, 2009
Red Hat Enterprise Linux Virtual vs VMWare Evaluation	June, 2009
VMWare Environment Installed	July, 2009
Propylon Acceptance of KLISS Infrastructure	Aug 26, 2009
Kansas Legislative acceptance of KLISS Infrastructure	Aug 31, 2009
Avamar Grid Backup System Installed	Sept 22, 2009
Wichita Data Center Installed (Servers, SAN, VMWare, Avamar, Exchange Server 2007)	October 19, 2009
KLISS begins production during 2011 session	Jan 2011
Project closeout	July 31, 2011

# KLISS Infrastructure Project

## KLISS Core System Acceptance

1-12

Testing of the Core System involved Propylon running test scripts simulating 25, 50, 100 and more connections continuously loading documents into the system. Metadata for each document was stored in the MySQL database, and corresponding folders were created automatically for the documents.

Assuming an attorney saves a document on average every 2 minutes, 25 connections in the test script simulates 2,000 attorneys. The high-end load test of 100 connections simulates approximately 8,000 drafting attorneys. The tests used the Kansas Statutes for test data. The tests created up to 1,700,000 revisions each day. Up to 38 GB of new storage was created in a daily test.

---

The testing was useful in identifying and resolving issues, such as:  
Memory Leak – Apache server configuration resolved this  
I/O Waits, CPU utilization high – MySQL database configuration resolved this

---

Testing continues throughout each iteration of the application development cycle. Tools such as egnInnovations monitoring, eHealth from DISC and VMWare allow the KLISS-I team to identify issues quickly and report them to the developers for resolution within the 2 week iteration cycle.

---

# KLISS Infrastructure Project

1-13

## Budget:

<b>Event</b>	<b>Payment</b>
Hewlett-Packard ProLiant 785 DL servers & EMC Clariion SAN	\$575,000
VMWare	\$117,500
egInnovations Monitoring	\$ 27,000
Red Hat Enterprise Linux	\$ 12,500
<b>Subtotal</b>	<b>\$732,000</b>
.....	
Avamar Grid Backup	\$248,000
<b>Total Payments</b>	<b>\$980,000</b>

\*\*\* The Avamar Grid solution was filed on a separate project plan and will be fully implemented by October 31, 2009. It is a replacement for the legislative CommVault tape backup system. The balance of the project funding is from the operations budget.

The KLISS application architecture identifies 200 virtual servers across the 4 environments – Development, Model Office, Production and Failover – to be backed up. CommVault tape backup required a software license for each server, in addition to the hardware costs of tape libraries and consumable tapes. The Avamar Grid project has a break even point of 2 months.

Avamar Grid also implements increased security, disaster recovery capabilities in Wichita, and data deduplication. Data deduplication technology will greatly reduce the amount of time our backup jobs run.

# KLISS Software Infrastructure Build Project

1-14

## Infrastructure Risk Mitigation:

1) Wichita Data Center installation is on a very tight schedule.

– Mitigation:

- Wichita Data Center installation week of October 19<sup>th</sup>
- Installed failover SAN and Proliant Server in Topeka.
- Loaded all failover software and tested the system using load and soak testing scripts
- Purchased and installed racks in Wichita
- When failover server is fully tested, it will be moved to Wichita
- From Topeka we will perform two end to end test scenarios producing bills from Law Making test scripts and conduct a demonstration test on November 15 and 16<sup>th</sup> in the Wichita site from Topeka
- We will use egInnovations software to benchmark the tests and post the results in the development offices.
- We will conduct test from Topeka directly to Wichita and repeat tests from Topeka through UAT environment and recover in Wichita



# KLISS Software Infrastructure Build Project

1-15

## Infrastructure Risk Mitigation:

2) Current KLISS infrastructure budget must carry us through 2011 session.

– Mitigation:

- Full architecture configuration and sizing report prepared by Propylon in November 2008 and updated in March 2009
- Demonstration data center established and soak test by Propylon demonstrating the architecture
- Four environments established and operating in the SW vault KLISS data center
- eglInnovations software used to produce benchmark reports for core system. Benchmarks highly favorable
- Layer 3 network installed with Cisco 3560 AND 6500 switches providing one gig of bandwidth to the desk top
- Two SAN 48 terabytes storage EMC devices installed –one for Topeka data center and the other for Wichita failover
- All technologies operating on open source OS's and third party software scaled and configured for 99.999% uptime.

Category	Functionality	Use Cases	Outputs	Scenarios	Scenario Data	Iteration	MO RAG
Request	Request #	KS0001 KSLM1002 KSLM1004	LMD-304 LMD-302	0061 0062 0063 0045	HB 2352 HB 2576 SB 418 SB 147		
	Meta Data	KS0002		0061 0063	HB 2352 HB 2576		
	Steno Sheet	KSLM1003	LMD-301	0061 0062 0045 0046	HB 2352 HB 2576 SB 147 SB 195		
	Resource Documents attached	KSLM1001	LMD-409	0062 0061 0063	SB 418 HB 2352 HB 2537 HB 2576		
	Yellow Sheet	KSLM1006	LMD-304	0061 0046	HB 2352 SB 195		
Bill Draft	Create Draft Bill	KS0003 KSLM0001 KSLM2008 KSLM2024 KSLM2025	LMD-200 LMD-308 LMD-410 LMD-408	0060 0062 0061 0046 0011	HB 2537 HB 2576 HB 2352 SB 195 Amended statute with an effective date of July 1 is not available for drafting, a copy of the engrossed bill needs to be cleaned up for usage		
	Bill Title	KSLM2020	LMD-200	0061 0046	HB 2352 HB 2537		
	Retrieve Statute	KS0005	LMD-200	0061 0046	HB 2352 HB 2537		
	Mark Changes	KS0004 KSLM2016	LMD-200	0061 0062 0045	HB 2352 HB 2537 SB 147		
	New Text	KSLM2006	LMD-200	0061 0062 0046	HB 2352 HB 2576 SB 195		
	Repealer	KSLM2021	LMD-200	0061 0046	HB 2352 HB 2537		
	Resource Documents attached	KSLM0008	LMD-409	0061 0062 0063	HB 2352 SB 418 HB 2576		
	Drafter Notes	KSLM2012		0061 0062	HB 2352 HB 2576		
	Boilerplate	KSLM2004		0061	HB 2352		
	Reference	KSLM2005		0061 0062	HB 2352 SB 418		
	Prefiled Bill	KSLM2023	LMD-200 LMD-303 LMD-307	0062	HB 2576		
	Renumbering (Sec and Para)	KSLM2011	LMD-200 LMD-001 LMD-003 LMD-005	0061	HB 2352		
	Tables (appropriations bill)	KSLM0007 KSLM2003	LMD-202 LMD-203 LMD-204 LMD-206	0222 0223 0224 0230	2006 HB 2958 Supplemental bill – House 2006 HB 2869 Mega bill – House 2006 HB 3021 Omnibus bill – House 2006 Senate Substitute for HB 2968 Omnibus bill – Conference		
	Find and Replace	KSLM2009		0061	HB 2352		
	Split and Compile bill	KSLM2001 KSLM2002	LMD-200	0061	HB 2352		
	Override markup rules	KSLM2014		0061	Correct KSA database errors		
	Override style	KSLM2015		0061 0062 0063 0045	HB 2352 HB 2576 SB 418 SB 147		
	Macros	KS00013					
Resolution							

Attachment 2  
 JCIT 9-23-09

Category	Functionality	Use Cases	Outputs	Scenarios	Scenario Data	Iterations
	Amending KS Constitution – Concurrent	KSLM0001	LMD-003 LMD-007 LMD-012 LMD-014e LMD-102 LMD-414 LMD-103	0001	2005 SCR 1601 to amend KS Constitution	
	Creating Joint Rules – Concurrent	KSLM0001	LMD-002 LMD-007 LMD-102 LMD-413 LMD-014	0001	2005 SCR 1603 Joint Rules	
	Creating Senate Rules	KSLM0001	LMD-006 LMD-011 LMD-100a-b LMD-413 LMD-014a-d	0001	2005 SR 1803 Senate Rules	
	Creating House Rules	KSLM0001	LMD-006 LMD-011 LMD-100a-b LMD-413 LMD-014a-d LMD-411 LMD-412	0001	2005 HR 6004 House Rules	
Amendment	Resource Documents attached	KSLM0008		0008	SB 418	
	Amendment Instructions	KSLM4001 KSLM4002		0008	HB 2576	
	Floor Amendment	KSLM0002a KSLM4004 KSLM4005	LMD-005	0001	HB 2352	
	Committee Report	KSLM0002b KSLM4008 KSLM4009	LMD-001	0008 0046	HB 2576 SB 195	
	Balloon	KSLM0009 KSLM4006 KSLM4007	LMD-010	0008	SB 418	
	CCR	KSLM0003 KSLM4008 KSLM4009	LMD-003	0008	HB 2576	
	Group Amendment Instructions	KSLM4010				
	Confirmation Committee Report	KSLM4013	LMD-310	0008	SB 418	
Proofing	Proofer Tools	KS0007 KS0008 KS0009 KS0010 KSLM0005 KSLM2010 KSLM3001 KSLM3002 KSLM3004 KSLM3005 KSLM3007 KSLM3008 KSLM3010 KSLM3011 KSLM3012 KSLM3013		0001 0002 0003 0004	Proofing of SB 418 Proofing of HB 2352 Proofing of HB 2576 Proofing of HB 2537	
	Proofer Checklist	KSLM3014	LMD-309	0001 0002 0003 0004	Proofing of SB 418 Proofing of HB 2352 Proofing of HB 2576 Proofing of HB 2537	
Engrossing	Engrossed Bill (Flagged)	KSLM0006 KSLM5001 KSLM5001a KSLM5002	LMD-201	0008 0001	HB 2576 HB 2537	
	Parallel Engrossing (w/Chambers)	KSLM0006 KSLM5001 KSLM5001a KSLM5002	LMD-201	0008 0001	HB 2576 HB 2537	
	Trial Engrossing	KSLM5004		0008	HB 2537	

Category	Functionality	Use Cases	Outputs	Scenarios	Scenario Data	Iteration
	Clean Engrossed (Net Engrossing)	KSLM5003	LMD-201	0061 0063 0065 0045 0046	HB 2352 HB 2576 SB 418 SB 147 SB 195	
	Manual Engross	KSLM5005	LMD-201	0063	HB 2576	
	Transmit Bill Packet	KSLM5006		0063	HB 2576	
Update Bill Index						
	Suggest Bill Index	KSLM2022		0061	HB 2352	
	Approve Bill Index	KSLM2022a		0275 0176 0277 0178	Review and approve bill index entries for SB 418 Review and approve bill index entries for HB 2352 Review and approve bill index entries for HB 2576 Review and approve bill index entries for HB 2537	
	Index Report		LMD-306 LMD-421	029	Create 2006 bill index report	
Update KSA						
	Retrieve Statute Text	KS0005		0061	HB 2352	
	Import Text into Workbench	KSLM2006		0061	HB 2352	
	Split Bill for Post Session Processing.	KSLM0102a		0211 0252 0254	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Update K.S.A. Processing Table	KSLM0102b		0251 0252 0254	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Filter K.S.A. Processing Table	KSLM0104		0251 0262 0254	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Re-Order K.S.A. Processing Table Entries	KSLM0105		0251 0262 0254	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Remove K.S.A. Table Entry	KSLM0106		0262	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Assign Split Bill Sections to Drafter	KSLM0107		0262	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Reassign Split Section	KSLM0107a		0262	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Drafter Process Assigned Section	KSLM0108		0262 0254	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Suggest Reserved Statute Section Number(s)	KSLM0109		0262	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Publications Editor Approval and Clean Up	KSLM0112		0262	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Approve/Edit Reserved Statute Section Number(s)	KSLM0114		0279	Create 2005 KSA reserved sections	
	Update Retrieval Database	KSLM0126			Update Retrieval Database	
	Update Statute Database	KSLM0127			Update Statute Database	
	Process Bills from Previous Sessions with Delayed Effective Dates	KSLM0139		0266	Process delayed eff. date sections from prior session (using 2004 SB 141 and 2004 HB 2347)	
Update Annotations						
	Create Annotation:	KSLM0101	LMD-401	0267 0268 0269 0270 0271 0272	Asterisk Note Source of prior law Revisor's Note Kansas Comments Cross Reference to Related Sections Research and Practice Aids Law Review & Bar Journal References Governmental Ethics Commission opinion Attorney General's Opinions CASE ANNOTATIONS	

Category	Functionality	Use Cases	Outputs	Scenarios	Scenario Data	Iterati
	Update Annotation	KSLM0101a	LMD-401	0307 0308 0309 0310 0311 0312	Asterisk Note Source of prior law Revisor's Note Kansas Comments Cross Reference to Related Sections Research and Practice Aids Law Review & Bar Journal References Governmental Ethics Commission opinion Attorney General's Opinions CASE ANNOTATIONS	
Publish KSA						
	Print	KS0006		0066	HB 2576	
	Create Volume Item List	KSLM0120		0307	Create KSA volume or chapter item list for bound or supp book	
	Create Supplementary Chapter	KSLM0121a	LMD-404 LMD-417 LMD-418 LMD-419	0308	Create and format chapter for supp to KSA	
	Create Supplementary Volume	KSLM0121b	LMD-404 LMD-417 LMD-418 LMD-419	0309	Create and format volume for supp to KSA	
	Create Bound Chapter	KSLM0124a	LMD-207 LMD-417 LMD-418 LMD-419	0308	Create and format chapter for bound KSA	
	Create Bound Volume	KSLM0124b	LMD-207 LMD-417 LMD-418 LMD-419	0309	Create and format volume for bound KSA	
	Create Valid Section Number List Report	KSLM0111	LMD-400	0309	Create Valid Section Number List Report	
	Publication Content Corrections	KSLM0125		0308	Correct KSA database errors	
	Transmit Data to External Customers	KSLM0130	LMD-405 LMD-406	0310	Transmit data to external customers	
Update KSA Index						
	Update KSA Index [FOCAL]	KSLM0010	LMD-403	0304 0305 0306	Drafter process index entries for assigned passed bill sections Editor approve changes and edits to index Compile single letter of index entries Make changes after compilation	
	Drafter Process Assigned Section	KSLM0108		0304	Drafter process index entries for assigned passed bill sections	
	Publications Editor Approve and Clean Up	KSLM0112		0305	Editor approve changes and edits to index	
	Suggest Removal/Edit of Index Entry Not in K.S.A. Processing Table	KSLM0133		0304	Drafter process index entries for assigned passed bill sections	
	Approve Removal/Edit of Index Entry Not in K.S.A. Processing Table.	KSLM0134		0306	Editor approve changes and edits to index	
	Process Each Alphabetic Letter Component for Index Volume	KSLM0135a		0305	Compile single letter of index entries	
	Create K.S.A. Index	KSLM0135	LMD-403	0305	Compile single letter of index entries	
	Edit K.S.A. Index	KSLM0136	LMD-403	0306	Make changes after compilation	
Reports						
	Create A&R Report	KSLM0103	LMD-314	0261 0262 0264	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Create Valid Section Number List Report	KSLM0111	LMD-400	0261 0262 0264	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Create Composite Report	KSLM0116	LMD-316 LMD-315	0261 0262 0264	Publish KSA for 2005 SB 147 Publish KSA for 2005 SB 195 Publish KSA for 2005 HB 2352	
	Create K.S.A. Reverse Index Report	KSLM0132	LMD-402	0303	Create reverse index for editor actions	
	Conflict Report	KSLM8001	LMD-313	0066	HB 2537	
Proof KSA						
	Proof and Correct	KS0007		0274 0275 0276 0277	Proofing of SB 418 Proofing of HB 2352 Proofing of HB 2576 Proofing of HB 2537	
	Document Compare (Diff)	KS0010		0274 0275 0276 0277	Proofing of SB 418 Proofing of HB 2352 Proofing of HB 2576 Proofing of HB 2537	
	Correct and Flag Statute	KSLM0128		0276	Correct KSA database errors	

Category	Functionality	Use Cases	Outputs	Scenarios	Scenario Data	Iterati
	Double Space Check	KSLM3002		0171 0172 0173 0174	Proofing of SB 418 Proofing of HB 2352 Proofing of HB 2576 Proofing of HB 2537	
	Check References	KSLM3004		0171 0172 0173 0174	Proofing of SB 418 Proofing of HB 2352 Proofing of HB 2576 Proofing of HB 2537	
	Check Form and Grammar	KSLM3010		0171 0172 0173 0174	Proofing of SB 418 Proofing of HB 2352 Proofing of HB 2576 Proofing of HB 2537	
Research						
	Search Navigation-Windows	KSLM7001		0171 0172 0173 0174 0175 0176	Search words by proximity to other words in document Search for documents with date limiters Search for documents with session limiters Search for single or multiple KSA sections by chapter, article, or range limiters Build search expression View and manage searches and results	
	Search Navigation-Keyboard or Mouse	KSLM7002		0171 0172 0173 0174 0175 0176	Search words by proximity to other words in document Search for documents with date limiters Search for documents with session limiters Search for single or multiple KSA sections by chapter, article, or range limiters Build search expression View and manage searches and results	
	Trigger Search from within a Request	KSLM7003		0171 0172 0173 0174 0175 0176	Search words by proximity to other words in document Search for documents with date limiters Search for documents with session limiters Search for single or multiple KSA sections by chapter, article, or range limiters Build search expression View and manage searches and results	
	Limit Searches	KSLM7004		0171 0172 0173 0174 0175 0176	Search words by proximity to other words in document Search for documents with date limiters Search for documents with session limiters Search for single or multiple KSA sections by chapter, article, or range limiters Build search expression View and manage searches and results	
	Sample Search-Proximity	KSLM7005		0171 0172 0173 0174 0175 0176	Search words by proximity to other words in document	
	Sample Search-Date Limiters	KSLM7006		0171 0172 0173 0174 0175 0176	Search for documents with date limiters	
	Sample Search - Session Limiters	KSLM7007		0171 0172 0173 0174 0175 0176	Search for documents with session limiters	
	Sample Search - Search Note	KSLM7008		0171 0172 0173 0174 0175 0176	Search words by proximity to other words in document Search for documents with date limiters Search for documents with session limiters Search for single or multiple KSA sections by chapter, article, or range limiters Build search expression	
	Work In Progress Search	KSLM7009		0171 0172 0173 0174 0175 0176	Search words by proximity to other words in document Search for documents with date limiters Search for documents with session limiters Build search expression	
	Search for Synonyms	KSLM7010		0171 0172 0173 0174 0175 0176	Build search expression	
	Change Sort Order in Search Results	KSLM7011		0171 0172 0173 0174 0175 0176	View and manage searches and results	
	Save List of Search Results	KSLM7012		0171 0172 0173 0174 0175 0176	View and manage searches and results	
	Recall Saved List of Search Results	KSLM7014		0171 0172 0173 0174 0175 0176	View and manage searches and results	
	Print List of Search Results	KSLM7015		0171 0172 0173 0174 0175 0176	View and manage searches and results	
	Navigate Through Search Results	KSLM7018		0171 0172 0173 0174 0175 0176	View and manage searches and results	
	Save Search Criteria	KSLM7019		0171 0172 0173 0174 0175 0176	View and manage searches and results	
	Recall Search Query	KSLM7021		0171 0172 0173 0174 0175 0176	View and manage searches and results	
	Search by Citation	KSLM7024		0171 0172 0173 0174 0175 0176	Search for single or multiple KSA sections by chapter, article, or range limiters	
	Constrain Search by Search Area	KSLM7023		0171 0172 0173 0174 0175 0176	Build search expression	
	Build Search Expression	KSLM7025		0171 0172 0173 0174 0175 0176	Build search expression	
	Constrain Search by Document Element	KSLM7026		0171 0172 0173 0174 0175 0176	Build search expression	
Administration						
	Dictionaries	KSLM6005		0171 0172 0173 0174 0175 0176	Add or Remove dictionary words and define hyphenation	
	Word Lists	KSLM6008		0171 0172 0173 0174 0175 0176	Add or Remove words from the word lists	

2-5

Category	Functionality	Use Cases	Outputs	Scenarios	Scenario Data	Iteration
	Boilerplate	KSLM6009			Add or Remove boilerplate	
	Hyphen library	KSLM6010			Add or Remove dictionary words and define hyphenation	
	Stop Words	KSLM6012			Add or Remove stop words	
	User Preferences	KSLM6004			Add, Edit and Remove user preferences	
	Revisor Personnel	KSLM6002			Add/update staff data for 2005 session Add/update staff data for 2006 session	
	Search Synonyms	KSLM6020			Add, Edit and Remove search synonyms	
	Placeholder	KSLM6015			Add, Edit and Remove placeholder	
	Maintain Volume Hierarchy	KSLM0131			Create KSA volume or chapter item list for bound or supp book	
<b>Appropriations Bills</b>						
	Prepare Appropriations Bill	KSLM0007	LMD-202 LMD-203 LMD-204 LMD-206 LMD-205		2006 HB 2958 Supplemental bill – House 2006 HB 2869 Mega bill – House 2006 HB 3021 Omnibus bill – House 2006 Senate Substitute for HB 2968 Omnibus bill – Conference	



# JOINT COMMITTEE ON INFORMATION TECHNOLOGY

SEPTEMBER 23 – 24, 2009

Joe Hennes – DISC Director

Executive Chief Information  
Technology Officer



## JCIT Quarterly Report April-June 2009 Executive Summary

### Active Projects:

27 Projects totaling \$159,323,101

- 16 Projects are in Good Standing
- 4 Projects are in Good Standing – Infrastructure
- 3 Projects are in Caution Status
  - Attorney General – Case Management System
  - Social and Rehabilitation Services – Host Access Transformation Services
  - Kansas Department of Transportation – Workflow Conversion Project





## **Executive Summary Active Projects: (Continued)**

- **0 Projects are in Alert Status**
- **1 Project Recast**
  - **KHPA – Data Analytic Interface**
- **2 Infrastructure Projects Recast**
  - **Department of Administration - KANWIN Infrastructure Upgrade**
  - **Department of Administration – Mainframe Tape Modernization**

3



## **Executive Summary Active Projects: (Continued)**

- **1 Project Reporting Insufficient**
  - **KS Lottery – Expanded Gaming Central System**
- **25 Executive Branch Projects**
- **2 Legislative Branch Projects**
- **20 Projects managed by Kansas Certified Project Managers**

4



## **Executive Summary Planned Projects**

### **Kansas Department of Education**

- **Kansas Statewide Electronic Transcript System**  
– **Projected Total Cost - \$1,833,912**

5



## **Executive Summary Approved Projects**

**Estimated Cost \$19,676,182**

### **Kansas State Historical Society**

- **Enterprise Electronic Preservation (KEEP) – High Level Plan Approved 5/14/2009**

### **Kansas Department of Labor**

- **UI Modernization Build and Deploy – Detailed Plan Approved 6/22/2009**

6



## **Executive Summary Completed Projects**

**Estimated Cost \$3,186,033**

### **Kansas Department of Corrections (KDOC)**

- KDOC Enterprise Architecture Plan

### **Kansas Department of Education**

- Enterprise Decision Support and Reporting System

### **Legislature**

- Conversion to Exchange Server 2007

**Plus 7 more since June 30th**

7



## **COMPLETED PROJECTS**

8



## Completed Projects Department of Administration

### Mainframe Tape Modernization

- Data Center space utilization reduced by 10 fold  
- Approximately 632 square feet down to 120
- Recast - 6 week delay in getting electrical installation completed.
- Completed 9/11/2009

9



## Completed Projects: Continued Kansas Department of Corrections

### Enterprise Architecture Plan

This project created an Enterprise Architecture by conducting a thorough Business Process Analysis that included process reengineering, conceptual data models, core specifications, and technical architecture.

- Formed base for 10 yr roadmap
- Documented approach, methodology, processes for sharing
- Reflects how business works today - in the future.
- PIER submitted 7/10/2009
- National Recognition
  - Leadership in Enterprise Results Award
  - September 10<sup>th</sup> - Washington D.C. -Federal Enterprise Architecture Conference

10



## Completed Projects: Continued Kansas Department of Revenue (KDOR)

### Division of Motor Vehicle Modernization – Mobilization/ RFP

Replacement of Vehicle Information Processing System (VIPS), Kansas Driver License System (KDLS), Kansas Vehicle Inventory System (KVIS). This first piece of the project utilized professional services to assist with initial mobilization activities and contract award.

- Feasibility Study in 5/2007
- Organizational analysis and design completed in 10/2007
- Seeks professional services to assist with
  - Initial project mobilization through contract award
  - Implementation phase preparation
- Contract award to 3M
- Negotiations in June, Contract Signed 7/1/2009

11



## Completed Projects: Continued Education, Kansas Department of (KSDE)

### Enterprise Data System to Support Decision Making and Reporting

Creation of Enterprise Data Warehouse to integrated 80 separate databases.

- Reduced redundancy within collections
- Streamlined reporting
- Supports research
- Student level statewide longitudinal data linked to other education data

12



## Completed Projects: Continued

Kansas Department of Health and Environment (KDHE)

### Vital Statistics Integrated Information System Phase III: Electronic Death Registration System

Submission of all death certificates to Office of Vital Records electronically.

- Stores over 8 Million records, Adds 100,000 each year
- Includes:
  - Fact of death
  - Cause/underlying causes
  - Manner of death

13



## Completed Projects: Continued

Kansas Department of Transportation (KDOT)

### Traffic Record System Development and Implementation Program

- Traffic Records Coordination Committee (TRCC)
  - Established to coordinate traffic records programs across state and local agencies
  - Collaborative effort KDOT, KHP, KBI, KCJIS and local agencies
- Strategic plan identified 51 potential projects
  - Dependent on available funding
  - Over next 10 years
- Contractor to coordinate long term, multi-agency effort

14



## Completed Projects: Continued

Kansas Department of Transportation(KDOT)

### TRCC Program Administration Project

- Preparatory work for Traffic Record System (TRS)
  - Coordination of ongoing cross-agency efforts
  - Also seeks technical assistance for the first release of TRS
  - Assist in reviewing TRS design



## Completed Projects: Continued

### Other Completed Projects

- KPERS – KPERS Plan Design Change Project -  
Estimated Cost \$237,300
- SRS – Host Access Transformation Services  
Estimated Cost \$402,148
- KDOT – Enhanced Priority Formula System  
Estimated Cost \$996,332
- Legislature – Conversion to Exchange Server 2007  
Estimated Cost \$281,332



# ACTIVE PROJECTS

17



## Active Projects Department of Administration

### KanWIN Infrastructure Upgrade II

- Replaces old Nortel switching equipment with Cisco switching gear
- New core switches in Landon, Eisenhower, and Off-Site Data Center
- Redundant distribution switches in 7 campus buildings and Capitol
- Edge Switches in all these buildings plus off-campus (WAN) buildings
- Establishes a single environment for switching and routing.

18





## Active Projects

### Department of Administration

#### KanWIN Infrastructure Upgrade II: Continued

- KanWIN Internet access, Wide Area Networking, Wireless Networking all functionally separate
  - Increased reliability and efficiency in networked operations
- Project was recast on 6/30/2009
- Numerous high priority projects interrupted work
- All project cost incurred before recast

19



## Active Projects: Continued

### Attorney General's Office

#### Case Management System

Provides a new Enterprise Case Management System to replace numerous individual systems.

- Web based filings, requests for services and follow-up
- In Caution status
  - Subproject I - 7/31/2009 to 8/21/2009
  - Data migration issues
- Finalizing project plan for Subproject II
- Data migration lessons learned during Subproject I allow Subproject II to meet planned execution end date of 5/17/2010

20



## Active Projects: Continued Department of Commerce

### Regional Education & Workforce Access Remote Delivery (REWARD)

This project provides High Definition Videoconferencing capabilities in 9 cities across the state.

- Provide training to dislocated workers
- Employment services for business and jobseekers
- Use off the shelf equipment
- Connectivity via KanED, KanWIN, and commercial vendors
- Computer connected to each videoconferencing unit
  - Allows KansasWorks and other Job Search tools during conference

21



## Active Projects: Continued Department of Commerce

### Regional Education & Workforce Access Remote Delivery (REWARD): Continued

- On hold from 3/17/2009 to 5/11/2009
- New Anticipated End 12/31/2009
- KCCC install delayed waiting on KANED
- New demands from UI Workforce and Services
- Will expand coverage by 6 locations

22



## **Active Projects: Continued**

### **Kansas Health Policy Authority (KHPA)**

#### **Data Analytic Interface II**

Creates a repository of all health related data to fulfill statute requiring KHPA to provide data to all stakeholders

- Provides to stakeholders
  - Cost information
  - Health services information
  - Information to make decisions on management of benefits for Medicaid, State Children's Health Insurance Program (SCHIP), state employees

23



## **Active Projects: Continued**

### **Kansas Health Policy Authority (KHPA)**

#### **Data Analytic Interface II (Continued)**

- Recast 6/11/2009
  - Delays in receipt of data from fiscal agent
  - Need to do more extensive research
  - Project scope Changed
    - Added State Employee Health Plan files
    - Added License Diagnostic Cost Groups for State Employee Health Plan
    - Expanded database from housing 5 years to 6 years
- Execution end moved to 5/18/2010
- Project costs increased to \$3,495,745

24



## Active Projects: Continued

### Kansas Department of Labor (KDOL)

#### UIM Build and Deploy

This project is one piece of the Kansas Department of Labor's efforts to modernize their technical and operational model

- Prior project completed Feasibility Study, requirements, design and part of build
- Replaces applications developed in late 60's and 70's

25



## Active Projects: Continued

### Kansas Department of Labor (KDOL)

#### UIM Build and Deploy

Incorporates the following principles

- Incorporates Customer Relationship Mgt.
- Incorporates Case management
- Incorporates Self Service options
- The project includes several subprojects
  - Infrastructure of core technologies
  - Deploy first priority functionality, data migration and interfaces
  - Wrap-up and secondary functionality

26



## Active Projects: Continued

Kansas Department of Labor (KDOL)

### UIM Build and Deploy

- **Current Status**
  - Genesys completing pre-install activities
  - Siebel has completed upgrade to 8.1.1
  - Performing additional design validation and deployment planning
  - RPP's for contract labor and project management services on street

27



## Active Projects: Continued

Kansas Lottery

### Expanded Gaming Central System

This project provides for a centrally managed application that would provide Lottery Security staff access to alerts and other information about the gaming machines .

- **Reporting insufficient due to missing CITO reporting requirements**
  - Contracted with Spielo last year
  - Execution start - 4/29/2009
  - Execution end - 12/14/2009
  - CITO Detailed Plan approval - 8/20/2009

28



## Active Projects: Continued

### Kansas Lottery: Continued

#### Expanded Gaming Central System: Continued

- **Stop and go effort**
  - Original plan for pari-mutuel racetracks to be first gaming operations
  - Negotiations broke off
  - Central system implementation stifled
  - 3 of 4 casino managers withdrew due of economic meltdown
  - Resulted in Central system not needed until later this year
  - Project appears in good health

29



## Active Projects: Continued

### Kansas Department of Transportation (KDOT)

#### Workflow Conversion Project II

The current software is obsolete and no longer supported. This project will replace 38 automated workflows and associated forms. In addition, conversion of 207 Fill and Print forms will occur. All KDOT employees will be impacted

- Execution began - 8/28/2008
- Recast on 5/12/2009
  - Realignment of business priorities based on budget constraints
- Currently in Caution Status
  - Realignment of business priorities related to KDOT's Comprehensive Program Management System Project
  - 5 deliverables delayed and 15 will be completed early

30



## Summary of Active Projects

- D of A – Financial Management System - \$44,777,322
- KHPA – KHPA Document Imaging Project - \$419,378
- KHP – Digital Video - \$2,717,604
- KHP – Kansas Law Enforcement Reporting System - \$583,303
- KDOR – Drivers License Photo First Model Office - \$933,154
- KDOR – PVD Computer Assisted Mass Appraisal Replacement II - \$4,766,431

31



## Summary of Active Projects: Continued

- SRS – Statewide Protection Report Center System - \$1,064,284
- KDOT – Communication System Interoperability - \$54,186,870
- KDOT – Comprehensive Program Mgmt System Replacement II - \$6,939,517
- KDOT – KDOT Financial Mgmt System Integration with SMART - \$779,707
- KDOT – KDOT Traffic Records System Release 1 Deployment - \$920,815

Questions?

32



## APPROVED PROJECTS

33



## Approved Projects Kansas State Historical Society (KSHS)

### Kansas Enterprise Electronic Preservation (KEEP)

This effort will produce a Trusted Digital Repository to preserve and access electronic government documents.

- KSHS doing preliminary work toward a digital archive
  - In 2008, the legislature appropriated \$150,000 to begin
  - In 2009, INK awarded a \$175,000 grant to build the archive
- Agencies to archive material under the expertise of State Archivist
- Eliminate need for agencies to have own digital archivist
- 3 CITO collaboration and sharing of resources
- All 3 CITOs agree to provide oversight and report individual projects
  - Authentication of legislative meeting minutes
  - Judicial Supreme Court Opinions
  - Executive branch projects
- High Level Plan approved - 5/14/2009
- RFP released

34





## Approved Projects: Continued Kansas Department of Revenue (KDOR)

### DMV Modernization

Implementation of Integrated Titles and Registrations, Inventory and Driver Control, and Driver's Licensing

- Completed Request for Proposal evaluation and contract negotiation process
- Contract with 3M signed - 7/1/2009
- Configurable off-the shelf product
- Require modifications of product, business processes
  - ADA compliance
  - Interfaces to existing systems
- No other product in marketplace
- 3M has implemented this system in 2 states

35



## PLANNED PROJECTS

36



## Planned Projects

Education, Kansas Department of (KSDE)

### Kansas Statewide Electronic Transcript System Implementation

This project will implement Electronic transcripts for all K-12 districts in the state. The system will include electronic exchange of transcript as students move between K-12 districts. Also to post secondary schools.

- Annual upload to KSDE
- 3 year project
- 100% Funding from National Institute of Education Sciences Grant
- Service provided free of charge,
  - Parents
  - Students
  - Post-secondary institutions

37



## JCIT Quarterly Report April-June 2009

### Questions?



## **JCIT Quarterly Report April-June 2009**

**Joe Hennes – DISC Director  
Executive Chief Information Technology Officer  
900 SW Jackson, 751-South  
Topeka, Kansas 66612**

**<http://www.da.ks.gov/kito/projstatusreport.htm>**

**Joint Committee on Information Technology**  
**September 23, 2009**  
**Testimony from Peggy Hanna, Deputy Project Director**

Thank you for the opportunity to give an update on the Sunflower Kansas Financial Management System Implementation Project. Listed below is a brief update of activities that have already occurred as well as how we measure success.

**Project Rationale and Benefits**

- Current state of central systems vs. agency systems
- Future state of integrated systems
- Benefits Kansas citizens seeking information as well as allowing state agencies to create efficiencies in their operation

**Scope and Timeline**

- Implementing 19 modules of PeopleSoft Financials, including a data warehouse -new system is called Statewide Management, Accounting Reporting Tool (SMART)
- Decommissioning approximately 60 agency financial systems
- Interfacing over 50 agency programmatic systems
- Enhancing SHARP with full interfacing between SHARP and SMART
- All agencies involved in implementation, especially if they are interfacing
- Timeline – analyze and design phases completed on time; build stage and unit testing on target; ‘Go-live date’ is still July 1, 2010 as in the original plan

**Accomplishments**

- Adhering to strong Governance structure put into place early in pre-implementation phase
- Strong State/Accenture teams built
- On time and within budget
- Provided assurance to agencies regarding this central system meeting their needs
- Prudent review of this out of the box software to keep modifications to a minimum,
- Statewide change management plan – 4 liaisons working with agencies
- Training for trainers and end-user – State agencies have volunteered trainers to conduct instructor led courses
- All environments have been ready in time for the phase they are needed – have a good partnership with DISC to ensure planning is common knowledge
- Receiving good reviews from KITO and our IV&V contractor

**Success Factors**

- Maintain Key Scope Elements – 23 modules purchased, 19 being implemented at this time

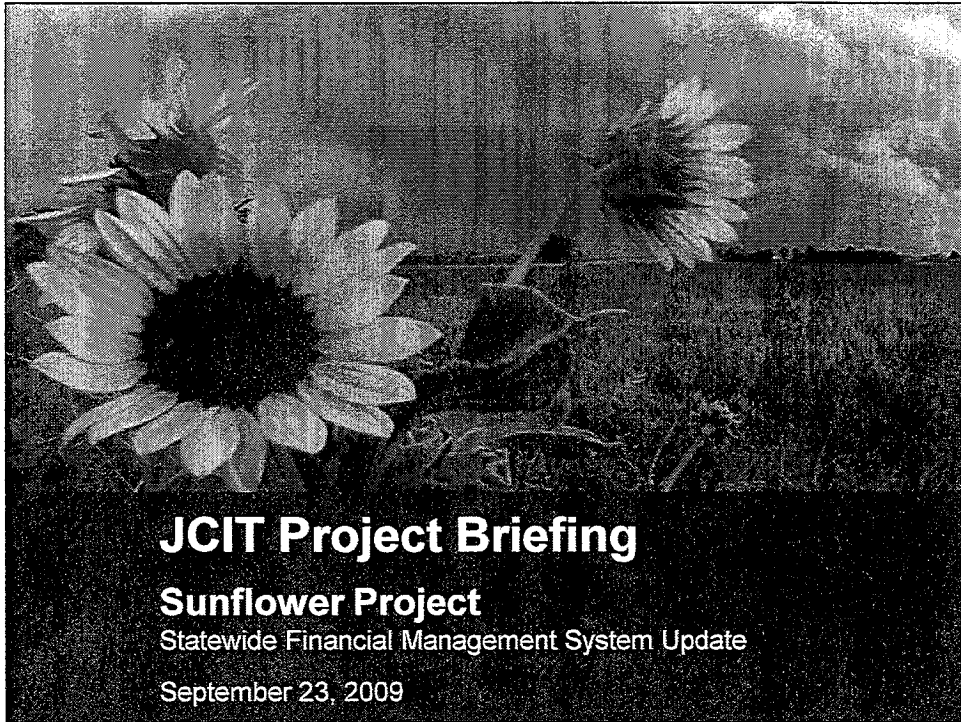
Attachment 4  
JLIT 9-23-09

- Balance Diverse Agency Needs – each agency as its own general ledger business unit
- Consolidate systems – Treasurer’s Office systems (unredeemed warrant tracking and SOKI) become a part of SMART
- Gain efficiencies – Opportunity for agencies to build in best practices to their processes
- Improved Decision Making – Reporting is the number one goal
- Support Taxpayer Transparency Act – More frequent updates to the KanView website as well as better detail reporting
- Minimize Software customizations – Part of the governance process
- Invest in our State workforce – On-going communication, Training, both system and basic accounting
- Extensibility – additional functionality to be added in future years

### **Governance and Oversight**

- Sponsors – weekly meeting to bring forward important updates and issues
- Steering committee – monthly meetings with all three branches of government represented
- FMS team – State team made up of state employees from various agencies, “experts” from private industry and experienced consultants; Accenture brought their ‘A’ team to this project
- KITO – Sunflower Project continues to meet quarterly performance goals
- IV&V – First 3 quarterly reviews indicate either an ‘excellent or very good’ project status

Thank you very much for your support of the FMS. I would be happy to answer any questions.



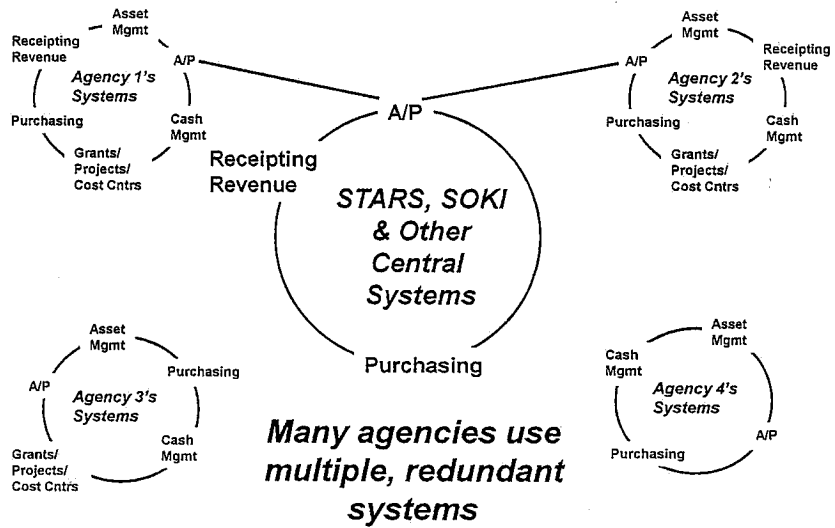
## Today's Briefing



- Project Rationale and Benefits
- Project Scope and Timeline
- Project Accomplishments
- Project Success Factors
- Project Governance and Oversight

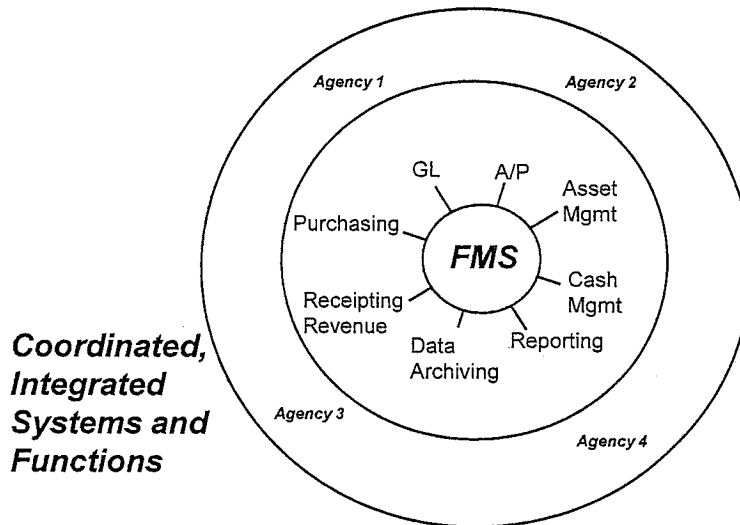
Attachment 5  
JCIT 9-23-09

## Current State



3

## Future State



4

## Project Benefits



- Streamlines and automates business processes
- Better integrates Payroll (SHARP) and core financials
- Modular application allows functionality to be easily extended (e.g. integrated budget development, e-commerce)
- Web-based architecture
- State-of-the-art data warehouse archives 10 years of transactional data
- Supports the Taxpayer Transparency Act
- Core Financials System will allow for future development of State initiatives

5

## High-Level Scope



- Implement 19 modules of PeopleSoft Financials including a data warehouse and ad-hoc reporting tools
- Replace STARS, SOKI, Procurement Manager Plus and STO's Warrant Tracking System
- De-commission over 60 agency systems and countless spreadsheets and stand-alone databases
- Interface with over 50 agency systems that are used for agency programs (e.g. eligibility, transportation, etc.)
- Enhance SHARP (State HR/Payroll system)
  - Modify chart of accounts to match the financial system
  - Integrate HR/Payroll application with the financial system application
  - Implement Time and Labor with employee self-service
- Impacts all agencies including the seven universities

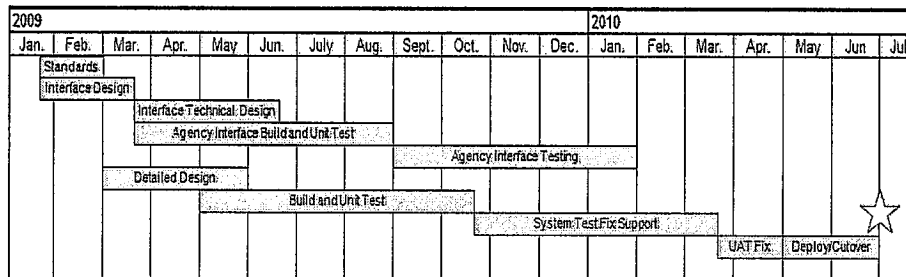
6



## High-Level Timeline

Agency interface testing is underway

On-schedule to begin system testing in mid-October and cutover in mid-June



7

## Accomplishments

- Established a strong governance structure to provide guidance and help make strategic and policy decisions
- Built a high-performing project team comprised of State and Accenture personnel
- Completed the *Analysis* and *Design* phases on-time and within budget
- Provided agencies assurance that system will meet their business needs enabling them to move forward de-commissioning agency fiscal systems
- Identified, scrutinized and prioritized modifications to the out-of-the-box software such that a relatively small number of software modifications will be needed

8

5-4

## Accomplishments

- Developed and implemented a statewide change management plan to help agencies manage the impact of moving to a new system
- Created an extensive training program comprised of approximately 40 courses to train over 3,000 employees
- Built-out several hardware/software environments for configuration, development and testing activities
- Received positive reviews on progress and project structure from oversight organizations

9

## Success Factors – Maintain Key Scope Elements

<u>Success Factor</u>	<u>Actions</u>	<u>On-Target</u>
Implement purchasing, accounting, asset management, data warehousing and reporting functions using a single integrated Statewide platform that will streamline core administrative functions.	Purchased 23 PeopleSoft modules to support original statement of work; removed 3-4 modules that didn't add marginal value	Yes

10

5-5

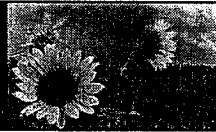
## Success Factors – Balance Diverse Agency Needs



<u>Success Factor</u>	<u>Actions</u>	<u>On-Target</u>
Strike a balance between central policies, business process standardization, best practices and decentralization – enabling agencies to configure some elements of the system specifically for their agencies (e.g. workflow routing, budget thresholds) and attempt to address the concerns and needs of large and small agencies alike.	Configured each agency as a separate business unit to provide future flexibility to agencies	Yes
	Established Set IDs so that agencies only see their chartfield values	
	Allowing intelligent (agency) numbering	
	Permitting agencies to store & manage any asset regardless of cost	
	Providing a data warehouse for agencies to perform ad-hoc queries and reporting	

11

## Success Factors – Consolidate Systems



<u>Success Factor</u>	<u>Actions</u>	<u>On-Target</u>
Move as many financial and administrative functions onto a single software platform and de-commission legacy systems, as appropriate, so that agencies can focus resources on the specialized systems and business processes that are germane to agencies' missions.	STARS, SOKI and unredeemed warrant systems will be de-commissioned	Yes
	Over 60 agency systems will be retired	
	Countless databases and spreadsheet and paper-based system will be retired	
	Extensive efforts made to demonstrate PeopleSoft to agencies so they can make informed decision regarding system de-commissioning	

12

## Success Factors – Gain Efficiencies



<u>Success Factor</u>	<u>Actions</u>	<u>On-Target</u>
Gain efficiencies in central and programmatic agencies by eliminating dual entry of data and the need for manual reconciliation	Implementing Labor distribution and project costing	Yes
	Providing agencies the means to interface or upload datasets to or from SMART, e.g. receipts interface for State Hospitals	
	Integrating centralized purchasing with Accounts Payables and Asset Management	
	Working closely with agencies to ensure interfacing needs are met	

13

## Success Factors – Gain Efficiencies



<u>Success Factor</u>	<u>Actions</u>	<u>On-Target</u>
Gain efficiencies in central and programmatic agencies by re-designing and automating business processes as appropriate.	Redesigning and automating business processes	Yes
	Incorporating best practices into business process workshops so that agencies can realize efficiencies by re-engineering processes and reorganizing accordingly	
	Provide agencies with tools in the workshops to help them re-engineer their processes and re-organize accordingly	

14

5-7

## Success Factors – Improved Decision Making



### Success Factor

Provide the data and analysis tools for agencies to measure and improve internal performance, to improve management decision-making and to improve customer service.

### Actions

Provide agencies with an extensive set of agency reports at "go-live"

Implement the data warehouse to enable agencies to answer their own questions by providing them query and reporting tools to access data

### On-Target

Yes

15

## Success Factors – Support Taxpayer Transparency Act



### Success Factor

Support transparency by providing the public more comprehensive and timely reporting of State finances than currently provided by KANVIEW

### Actions

After "go-live" a revised set of KANVIEW requirements will be developed based on data available in the DW. At a high level KANVIEW can include:

1. more granular transactional data
2. total cost of projects including capital expenditures
3. aggregation of expenditures by vendor, county, agency, program, etc.
4. revenues received from federal grants and use of these monies
5. bond debt payments
6. agency assets

Increase frequency of posting to KANVIEW

### On-Target

Yes

16

## Success Factors – Software Customizations



### Success Factor

Minimize customizations to the software to reduce software lifecycle costs.

### Actions

Scrutinize requests for software modifications by applying best business practices and other solutions whenever possible

Established a well-structured and disciplined change control process

Managing all software modifications within the project budget

### On-Target

Yes

17

## Success Factors – Workforce



### Success Factor

Invest in the workforce by ensuring adequate training and two-way communication to generate acceptance of change in the workplace resulting from the Sunflower project.

### Actions

Develop an extensive training program consisting of instructor lead training, web-based training and on-line help

Train all agencies' key staff prior to go-live

Require that attendees receive passing scores on End User Training assessments

Hold meetings and workshops (e.g. Change Agent Network, Knowledge Transfer, Business Process Workshops and Interface & Data Conversion Workshops)

Publish monthly newsletters

### On-Target

Yes

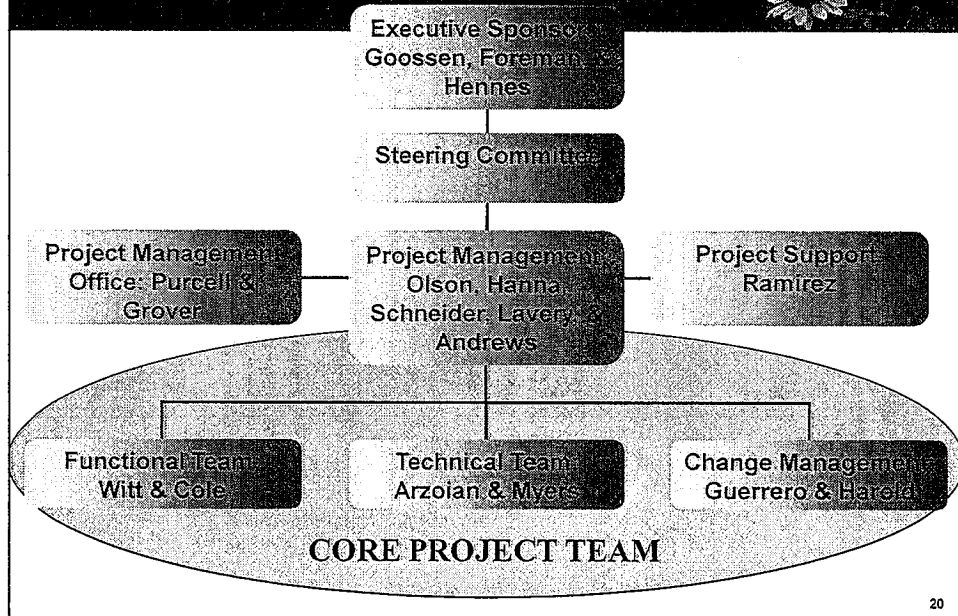
18

## Success Factors – Extensibility

<u>Success Factor</u>	<u>Actions</u>	<u>On-Target</u>
Build upon the core financial system, in future phases, to integrate budget development, labor distribution, AR/billing, travel and other functionality as needed to support agencies' missions.	<p>Added AR/billing, travel and labor distribution to support agency business processes</p> <p>Compiling a list of agency needs for adding functionality in the future</p>	Yes

19

## Project Organization



20

5-10

## Project Governance

### Executive Sponsors

- Secure budget
- Resolve inter-agency issues
- Assist with changes to statutes and policies

### Steering Committee

- Define and control high-level project scope
- Provide guidance on cross-agency issues
- Champion the Sunflower project

### FMS Management Team

- Secure project resources
- Address agency issues
- Propose changes to statutes & policies
- Identify and manage strategic issues (3-6 months out)
- Assist managers and Team Leads in problem resolution (tactical or strategic)
- Resolve cross-team issues, when necessary
- Control scope, schedule, cost and quality
- Manage contractual issues with Accenture

21

## Project Governance

- Weekly meetings with project Sponsors to review status and address policy and strategic agency issues
- Monthly meetings with project Steering Committee to review project progress, budget and to approve changes over \$50K and to address agency issues
- Strict change control procedures with specific thresholds for authorizing change orders
- Change control process is well-documented to ensure accountability

22

5-11



## Oversight – KITO



- Based on KITO metrics the project continues to meet quarterly performance goals
- All deliverables on-schedule
- Task completion rate within 90% of planned
- Actual costs and estimate at completion below projections
- No major scope changes

23

## Oversight – Quarterly Independent Verification and Validation Audits



- 3 of 5 scheduled IV&V project reviews (completed by Sys Test Labs of Denver)
- Typical reviews include one week prep, one week on-site, one week to draft report
- Interview 25 – 30+ project and non-project personnel
- Review 20 – 35 documents (deliverables, risk log, issue log, project plan, status reports, requirements matrix, test scripts, etc.)
- Overall project health rated as “excellent” or “very good” on each review
- Several recommendations provided after each visit which are followed up at each subsequent review
- Major concerns continue to be the broad scope and aggressive schedule of the Sunflower project

24

5-12

## Questions and Answers



For additional information on the project, please see the project website: <http://da.ks.gov/smart>

25

## Authority for Change Requests

Change Request	Authority	Cost Impact	Scope Impact	Impact on PS Code Base	Schedule Impact	Agency Impact	Law, Reg, Policy Impact
Level 1	Executive Sponsors	TBD	TBD		Any change affecting the "Go-live" date	TBD	Any changes affecting laws, regulations or other non-A&R policies
Level 2	Steering Committee	Changes over \$50K	"Significant" impact on project scope (+/-)			TBD	Recommends changes to Executive Sponsors
Level 3	FMS Mgmt Team (CCB)	Changes under \$50K	"Moderate" impact on project scope (+/-)	All mods approved by FMS Mgmt Team	Any change affecting KITO milestones or other key (internal management) milestones	Any decisions/changes "adversely" affecting agencies	Any changes affecting A&R policies and procedures
Level 4	Managers	All changes affecting cost (+/-) approved by FMS Mgmt Team	"Minor" impact on project scope (+/-)		"Minor" impact on project activities that do not adversely impact a milestone	Configuration decisions benefiting agencies that do not impact cost or do not impact a milestone	

26

5-13

## Universities Use of SMART



- All universities will be interfacing into SMART or entering data directly into SMART for payments, receipts as well as purchases which exceed their statutory authority
- Universities have their own well-established financial management systems tailored to meet their unique business processes
- These systems link tightly to universities' student information management systems
- The additional number of users and required modifications would require a much larger support organization

Testimony

Joint Committee on Information Technology

Lynn Carlin, Interim Vice-Provost for Information Technology Services

Kansas State University

September 23, 2009

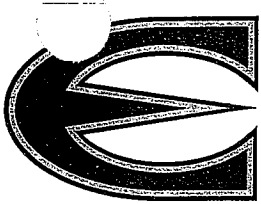
Chairman McLeland, and Members of the Joint Committee on Information Technology,  
My name is James Lyall and I am the Associate Vice Provost for Information Technology Services. I am here representing Lynn Carlin, the Interim Vice Provost for Information Technology Services. I am pleased to have the opportunity to talk with you today about the critically important issue of information and computer security and to report that we are have nearly completed implementing the recommendations of the February 2009 follow-up IT security performance audit titled *Regents' Information Systems: Following Up on Computer Security Issues at Various Universities*. University policies have been approved for eighteen of the twenty-six recommendations. Policies addressing the remaining eight recommendations are in the final stage of review.

Since the completion of the 2005 security audit, Kansas State University has improved its information and computer security postures in a number of areas. For example, we replaced the social security number with the "Wildcat ID" as the primary identifier of our employees and students. We increased collaboration between central IT and departmental IT staffs and significantly expanded campus awareness and user training in IT security. These efforts include

Attachment 6  
JCIT 9-23-09

weekly articles in our IT newsletter, monthly roundtable discussions, an annual training workshop open to all students and employees, an enhanced IT security website and a security threats blog, guest lectures, seminars, and campus TV segments. Last summer, we created the position of University Chief Information Security Officer and reallocated several positions to information security, creating an IT security team with three full-time positions. The creation of the IT security team has allowed Kansas State University to accelerate progress improving our security posture in the past year.

Kansas State University is committed to protecting the security of its information and technology resources in an extremely complex environment. I appreciate the interest of this Committee and the work of the Legislative Post Audit in highlighting the importance of information and technology security for our state and its public institutions. I'm happy to take any questions.



Testimony to Joint Committee on Information Technology (JCIT); September 23, 2009

Good afternoon,

At the request of the committee, I am here today to provide an update on progress made in response to the Legislative Division of Post Audit's report on Regents' information security issues from February, 2009.

In response to both the public and confidential findings of the report and the subsequent Recommendations for Executive Action, ESU took immediate steps to address the identified concerns and has made significant progress in implementing those recommendations. We established a formal project plan, outlining both the steps and a timeline necessary to meet all recommendations with which we concur. We are currently in the implementation phase of that plan and are on target for timely completion and compliance with those recommendations.

As directed by the Recommendations, we have submitted two written progress reports to the Legislative Division of Post Audit, including details of specific actions we have taken to comply with policy recommendations from the confidential report. We also continue to make progress with regards to the non-policy recommendations of the report.

Information Security has, and continues to be, a priority at Emporia State University. Independent of LPA recommendations, we have increased personnel resources assigned to information security and invested in additional technology resources to assist in those efforts – despite hiring freezes and other significant impacts of the current financial environment. We continue to work on a comprehensive Information Security program and actively collaborate with other Regents Institutions through the Regents Information Technology Council (RITC) and the Regents Information Security Council (RISC). Our common goal is to increase the Information Security at each of our institutions through the sharing of policy development, implementation and best practices which address the unique nature of higher education.

I am confident that the focused efforts in response to the LPA report, as well as broader, ongoing efforts continue to improve the information security posture at ESU. As recommended, we will submit a final report to the Legislative Division of Post Audit by January 1, 2010. I am confident that we will have met all of the recommendations as we indicated in our response to the confidential report.

I appreciate the committee's time today and would be happy to answer any questions that they might have at this time.

Submitted by:

Michael D. Erickson  
Associate Vice President, Technology and Computing Services  
Chief Information Officer

cc: Dr. Michael R. Lane, President  
cc: Dr. Tes Mehring, Provost & Vice President for Academic Affairs and Student Life

**Information Security at the University of Kansas-Lawrence**  
**Status of Action and Timeline Regarding the 2005 Legislative Post Audit Findings**

Submitted to

The Joint Committee on Information Technology

September 23, 2009

By

Denise Stephens

Vice Provost for Information Services and Chief Information Officer

**Introduction**

→ The University of Kansas (KU) considers the articulation and full implementation of the LPA recommendations an essential component of its comprehensive approach to securing information. We are very near completion of this important work. In addition to the specific LPA recommendations, the University has undertaken an aggressive strategy of technical intervention, industry-recognized practices, and institutional awareness/education programming to promote systematic and sustainable change. This approach reflects our strategy for securing information at KU since 2002. The environment we seek to create is one that recognizes institutional and individual responsibility for safeguarding the information entrusted to KU by the people of Kansas. We have transformed our environment to meet and exceed the Post Audit standards. Our transformation involves both technological and policy-based approaches. This brief summary of our activities – including those devoted to achieving LPA recommendations – outlines the University's strategy.

**Strategy for Fulfilling LPA Recommendations and Extended Security Improvements**

Our strategy is based on the goal of effectively managing risk in a complex and diverse community of more than 33,000 users. The recommendations resulting from the *2005 Computer Security Audit Report* reinforced our ongoing challenge of implementing campus-wide controls in a highly decentralized computing environment. Recognizing that significant time and effort was necessary to address all of the recommendations, we decided to move simultaneously on several levels, understanding that progress would be uneven - but certain. Our approach is *Defense in Depth* and includes the following actions:

- First, Protect from the Outside. KU pursued the most immediate impact by hardening the campus' virtual perimeter using the technologies available to the central organization. This was essential to minimize the risk of external attack.
- Second, Protect from the Inside. KU began work to change the culture regarding information security and to address our greatest vulnerability – individual handling of information assets. We launched a comprehensive Information Management Initiative to serve as a sustainable framework for campus-wide awareness/education and policy development. The Initiative created a permanent Policy Group charged with ongoing responsibility for the articulation of information policy.

Our goal of protecting the external and internal environments required significant assessment and programmatic work to understand our over-all information risk profile, to identify and institute effective practices, and to develop a security-conscious information culture. KU has worked steadily to achieve these objectives with the following:

- • KU embarked on the development of practices considered best in the information security field. Developing a network of distributed campus IT professionals, the central IT organization began to encourage the adoption of common practices to promote consistency in managing computing assets connected to the network. In addition to the critical 2005 Audit and subsequent findings, KU has had its central IT security practices audited by outside industry bodies to assess our practices compared to industry standards. We have passed those audits.
- KU began the analysis of risk regarding the handling of information throughout its 400-plus departments. This step informed the development of *policies and practices*, including 17 drafted or approved policies resulting from the 2005 Audit as of December 2008. Further, the comprehensive analysis of department information and technology informed the extent of awareness/education necessary to encourage secure information handling among the University's many information custodians.
- • Initiative One. KU's fragmented computing architecture is being reconfigured under Initiative One – a program of efficiency and cost-saving changes to maximize and secure the University's technology resources through improved technical and policy coordination.

### **Regarding Standards and Practices**

The University of Kansas-Lawrence is serious about all aspects of information security. We apply aggressive and comprehensive industry best practices in the development and



implementation of security controls – among which are policies. Third party assessors have contributed guidance and validation to our security management plan – which encourages responsible user behavior in handling information assets. Since 2007, our PCI (payment card industry) environment has been scanned by a certified PCI assessor. We have successfully passed each of these scans. Our environment has undergone continuous security improvement since 2002. We believe the application of practices such as those articulated by the information security industry and those articulated by the LPA findings contribute to the secure environment we seek to create.

## **Response to LPA Findings and Status of Action**

### **Status of Action (September 2009)**

Building upon KU's actions since December 2008, the campus has drafted new policy relevant to the Audit's System Development recommendations. The System Development Policy for the Lawrence Campus and the accompanying Standard addresses the noted issues. This development leaves one category of Audit pending action. New policy on Data Center/Server Room Management is in development with implementation expected in October 2009. This policy addresses the remaining recommendations relevant to Physical Security. Upon implementation this fall, the policy will complete work to address all recommendations resulting from the *2005 Findings*.

### **Updating the June 2009 quarterly Status of Action:**

Completed Recommendations. As of September 4, 2009, 28 of 35 recommendations have been addressed. Of the remaining 8 recommendations, 5 are at policy approval stage and 3 in policy development.

### Status of Outstanding Recommendations from the February 2009 Report of Findings.

- *Access Controls* – 6 of 6 recommendations have been addressed in the Data Classification and Handling Policy approved January 2009 and in the Information Access Control Policy approved April 2009.
- *Data Controls* – 5 of 5 recommendations have been addressed in the Data Classification and Handling Policy approved January 2009.
- *General* – 1 of 1 recommendations have been addressed in the Data Classification and Handling Policy approved January 2009.
- *Operations* – 5 of 5 have been addressed in the Data Classification and Handling Policy approved January 2009.

- *Physical Security* :
  - 1 of 5 recommendations has been addressed by modifying the existing Network Policy.
  - 1 of 5 recommendations has been addressed in data-relevant sections of the Data Classification and Handling Policy approved January 2009.
  - 3 of 5 recommendations are pending approval and implementation of the new draft Data Center/Server Room Management Policy (expected completion October 2009).
- *System Development* – 5 of 5 recommendations have been addressed in the draft Systems Development Policy for the Lawrence Campus and the accompanying Standards. Revised following stakeholder review. Implementation October 2009.
- *Security Management* – 2 of 2 recommendations have been addressed in the Data Classification and Handling Policy approved January 2009.

### **Conclusion**

The University is in the final stages of implementing all of the LPA recommendations. These important measures must be fully articulated, implemented, and enforced. To accomplish these objectives, we are introducing substantial technological and cultural change. In some cases, significant financial costs are involved. Given the critical nature of this work, KU is proceeding with due caution to ensure sustainable outcomes and conscientious stewardship of taxpayer and university resources. We have worked steadily to build the institutional framework for addressing these and other essential steps to secure our computing and information environment. The foundation is in place. We are weeks away from fully achieving the outcomes specified in the LPA Findings. Finally, we are positioned to further expand upon an already significant effort to ensure information security into the future.

# **Kansas Partnership for Accessible Technology**

Presentation to the Joint Committee on  
Information Technology  
September 23, 2009

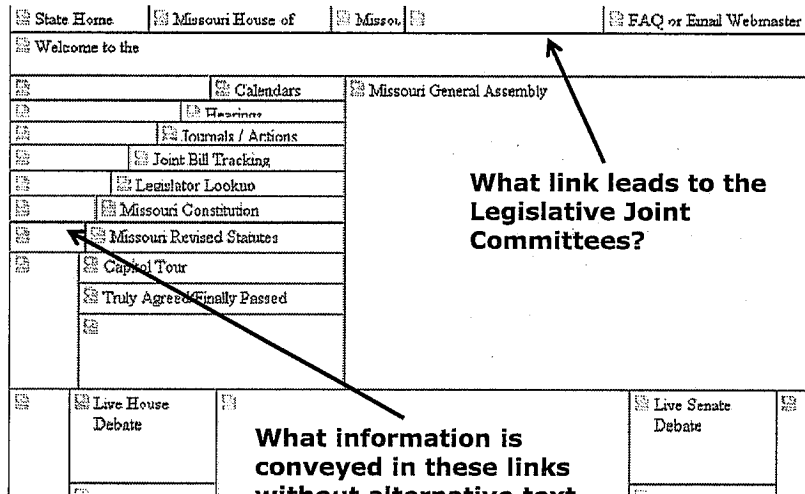
## **Presentation Outline**

- Accessible Technology: Scope & Impact
- Legal and Policy Framework
- Kansas Efforts: 1999-2008
- KPAT Overview
- Emerging Accessibility Issues
- Questions

# Accessible Technology: Scope & Impact



# Accessible Technology: Scope & Impact





## Accessible Technology: Scope & Impact

- Impacts access to government services and information (Accessibility = Usability)
- Accessible technology can improve productivity for all users, lower costs
- Benefits not always obvious – e.g. aging population, color-blindness, search engines
- Applies to websites, telecommunications, hardware, software, and a variety of other technologies

## Legal and Policy Framework

Requirement for Accessible IT rests on both law and policy

- ADA of 1990 and amendments of 2008, Section 504 of Rehab Act of 1973, K.S.A. 39-1101, 1105; K.S.A. 44-1001 et seq.), others.
- Section 508 of Rehab Act of 1973 establishes requirements for electronic and information technology.
- ITEC Policy 1210 – State of Kansas Web Accessibility Requirements

## Legal and Policy Framework ITEC Policy 1210

- Information Technology Policy 1210:  
State of Kansas Web Accessibility Requirements
  - establishes "a State of Kansas policy regarding accessibility requirements for all State of Kansas internet, intranet, and extranet websites, web services, and web applications, including those that are developed internally, developed via contract, provided by third parties on behalf of state Entities, or purchased products"

## Legal and Policy Framework Potential Financial Risk

- A recent high-profile lawsuit brought against Target by the National Federation for the Blind was settled for \$6M
- SAP settled a complaint filed against it by the State of Arkansas regarding their state financial system, after Arkansas was sued by the NFB.
- Web accessibility lawsuits have also been brought against:
  - State of Texas
  - Connecticut Attorney General's Office
  - City of San Rafael
  - Southwest Airlines
  - American Airlines
  - Ramada and Priceline
  - Bank of America
  - H&R Block

## Kansas Efforts: 1999-2008

- **1999:** Web Accessibility Subcommittee (WAS) formed to address urgent need for state response to web accessibility issues. Focus limited to Web only.
- **2000-2001:** ITEC Policy 1210 on Web Accessibility approved, guidelines rolled out over an 18-month period, supported by training
- **2002-2005:** Continue to provide training, surveys, presentations to publicize effort, update guidelines and address emerging issues.
- **2005-2007:** Strategic planning effort to determine how to approach growing need for resources and sponsorship
- **2008:** Director hired, Partnership founded by Executive Order of the Governor

## Kansas Efforts: 1999-2008 Lessons Learned

- Staff turnover and changing technologies drive a continuous need for awareness-building and training
- Assessment needed to understand levels of compliance, training needs, as well as emerging issues
- Emphasize accessibility early in the procurement process to ensure products and services meet requirements
- Central resources needed to research/address issues, support agencies, implement training & assessment
- Executive-level sponsorship required to focus resources and priority on the issue
- IT Accessibility more than just the Web



## Kansas Partnership for Accessible Technology

Established by Governor's Executive Order 08-12 on December 22, 2008. Primary objectives are to:

- Provide recommendations on IT accessibility issues, standards and policy to ITEC and other committees, boards, commissions, as appropriate.
- Develop and support programs for assessing and monitoring IT accessibility compliance
- Develop, coordinate delivery of training
- Establish a leadership role in the national effort to improve access to information and services by individuals with disabilities.

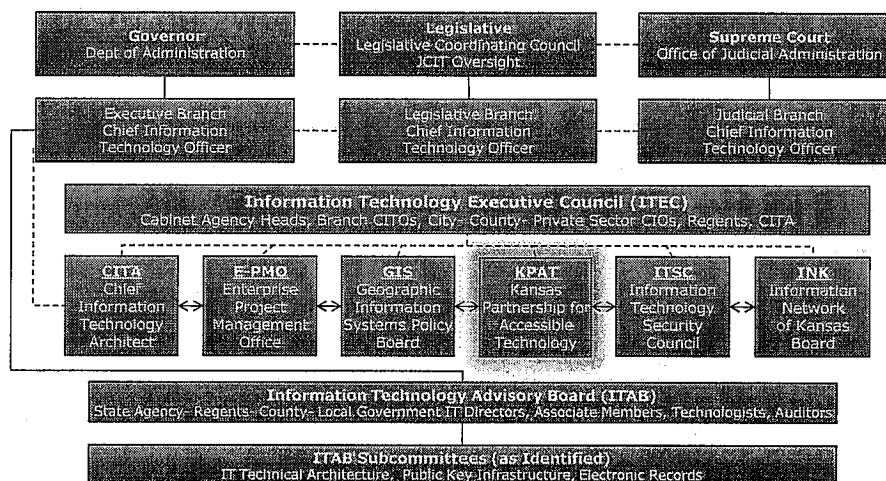
## Kansas Partnership for Accessible Technology

- 24 members – Executive Order allows up to 30
- Meets quarterly
- Initially chaired by DISC Director of Enterprise Technology Initiatives; Vice-chair is Executive Director of the Kansas Commission on Disability Concerns
- After first year, chair/vice-chair elected by membership
- Staffed by Director of Web/IT Accessibility, Cole Robison, housed in DISC
- Website located at <http://da.ks.gov/kpat/>

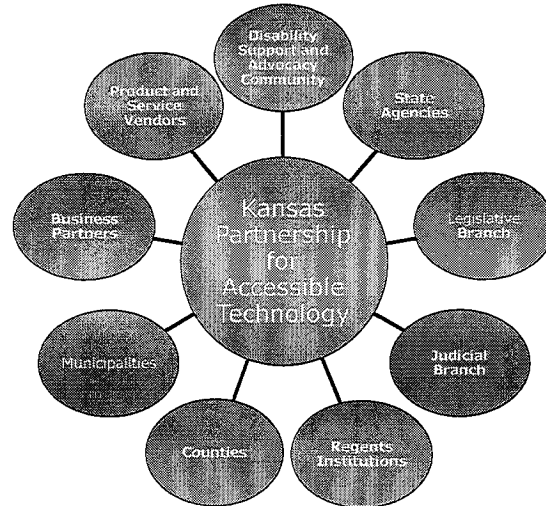
## Kansas Partnership for Accessible Technology – Current Membership

Three CITO's, CITA	Director of Purchases
State Archivist	SRS, KHPA, Aging
State GIS Coordinator	Dept. of Education
Regents IT Council	Ks. Assoc of Counties
INK Executive Director	League of Municipalities
State ADA Coordinator	DISC
School for the Blind	KDEM
School for the Deaf	Telecom Access Program
KanEd	IT Accessibility Director
Ks. Commission on Disability Concerns	

## IT Governance Model



## Relationship to Stakeholder Communities



## Kansas Partnership for Accessible Technology - Initiatives

- ✓ ITEC Policy 1210 Update
- ✓ Kansas State Technical Architecture Update
- Agency support (*ongoing*)
- Outreach (*ongoing*)
- Procurement Standards (*under development*)
- Website Accessibility Assessment (*planning*)
- IT Project planning and approval process
- Training

## Emerging Accessibility Issues

Technology lifecycle means accessibility issues and implementation are always evolving.

### Examples:

- Online audio/video
- Online conferencing
- Web 2.0 (Rich Internet Applications)
- Unified Communications

## Contacts

### Cole Robison

Director of Statewide Web/IT Accessibility  
Division of Information Systems and Communications  
(785) 291-3016  
cole.robison@da.ks.gov

### Duncan Friend

Chair, Kansas Partnership for Accessible Technology  
Division of Information Systems and Communications  
(785) 296-8137  
duncan.friend@da.ks.gov

### Martha Gabehart

Vice Chair, Kansas Partnership for Accessible Technology  
Executive Director, Kansas Commission on Disability Concerns  
(785) 296-1722  
mgabehart@kcdcinfo.com



Mark Parkinson, Governor  
Thomas E. Wright, Chairman  
Michael C. Moffet, Commissioner  
Joseph F. Harkins, Commissioner

**Presentation to Joint Committee on Information Technology**

**Susan Duffy, Executive Director  
Tom Ryan, Information Technology Director**

**September 24, 2009**

**KCC Project 2010 Business Process Innovation and Improvement**

**Background**

The Kansas Corporation Commission met with the JCIT in August 2008 and presented a plan to automate interactions with regulated entities and internal business processes. The committee expressed support for our efforts and the CITO approved the high-level project plan in early September 2008. We are here today to provide the committee an update on the KCC Business Process Innovation and Improvement (BPI<sup>2</sup>) project.

**Vendor Selection**

Under the sponsorship of the Commissioners, the BPI<sup>2</sup> Steering Committee created a twenty member evaluation team representing the divisions most impacted. The Request for Proposal, published in December 2008, identified four areas the KCC wanted to automate:

- eFiling
- Document Management
- Case Management
- Work Flow

Eight vendors submitted responses with cost proposals ranging from \$900,000 to \$1,800,000. The evaluation team selected three vendors for an On-Site Demonstration. Two vendors were then selected for the Negotiations phase and both vendors submitted comparable Best and Final Offers (BAFO). The KCC's Steering Committee selected ACO Information Services of Mobile, Alabama as our partner for business process automation. ACO is focused on automating state regulatory agency processes and has built an excellent reputation in this area and has implemented utility commission systems in Alaska, South Carolina, Louisiana, Alabama, Mississippi and Puerto Rico. ACO's final bid totaled \$550,000 for software and implementation support services.

The KCC acknowledges the invaluable assistance provided by the Division of Purchases and the Enterprise Project Management Office throughout the vendor selection process, in particular Bob Sachs, Carey Brown and Mary Grace.

*Attachment 10*

## **Project Management**

The KCC has taken two steps to ensure the project's success. First, the KCC created a project analyst position from an existing vacancy and hired Dan Consolver, an experienced IT manager, who will focus on supporting BPI<sup>2</sup> over the next 15 months.

Second, the KCC engaged Mitch Ummel and Ken Orr to provide Independent Verification and Validation services throughout the implementation phase. Ken and Mitch have worked with several Kansas state agencies, most recently with the Kansas Department of Corrections, and are highly regarded for their knowledge in process analysis and IV&V. As a result of their work during the project's planning phase, they hold the confidence of the KCC's Steering Committee and will provide continuity throughout implementation.

## **Project Implementation**

Following CITO approval of the Detailed Project Plan for Phase I, the KCC held a project implementation Kick-Off meeting on August 11, 2009 for the Topeka staff. A video recording was made for the benefit of staff in KCC offices throughout the state. Chairman Wright introduced ACO Information Services, identified the BPI<sup>2</sup> project as a high priority for the coming year and reinforced his vision of using technology to work smarter.

BPI<sup>2</sup> will be implemented in a series of seven iterations. The iterations are designed to ensure a smooth transition to the new system with minimal disruption to ongoing agency activity. To date Iteration 1 is complete and Iteration 2 is ongoing with scheduled completion by mid-October. After Iteration 2 the KCC will seek CITO approval of the Detailed Project Plan for Phase II. During project roll-out the KCC will involve internal departments and external utilities as appropriate. The testing and roll-out plans will minimize the KCC's exposure to risk by incrementally transitioning processes to the new system.

## **Project Goals**

In August 2008 the KCC identified these project goals:

- Replace legacy technical architecture
- Establish technologies consistent with proven web based computing standards
- Reshape the corporate culture
- Put information at users fingertips
- Install technology to ensure continuous process improvement and innovation over the next three to ten years
- Capture KCC institutional knowledge with automated business rules
- Create a trucking portal to integrate state and federal agency information

A rare window of opportunity exists. By year-end 2010 the Commission will take advantage of this opportunity to implement an infrastructure that will fundamentally change the way we do business, elevate service levels and add the KCC to the list of technically efficient state entities in Kansas.

### **Iteration Plan and Key Deliverables**

**Iteration 1 - Create Detailed Project Plan, Formalize Project Environment, and Hold Kickoff Meeting.**  
Develop a detailed Project Plan for Iteration 2 and a high-level plan for remaining Iterations. This element is complete when CITO approves the project plan and grants approval to proceed. Configure the STAR development environment. Hold the KCC 2010 BPI<sup>2</sup> Kickoff meeting at the KCC and familiarize KCC staff with the overall implementation plan.

#### **Iteration 2 - Requirements Discovery, Elaboration and Gap Analysis**

Complete the configuration survey, gap analysis and base system analysis. Identify functional scope including data mapping, e-filing and system interfaces. Perform solution and support technology training and mentoring for end users and technical staff.

#### **Iteration 3 - Business Process Analysis and Base System Configuration**

Configure and test STAR's base system. Initiate system customization development based on KCC priorities. Develop and test data mapping and migration scripts. Perform initial interface analysis and design. Perform solution and support technologies training and mentoring for end users and technical staff.

#### **Iteration 4 – Docket Management System Deployed**

Build, configure and certify the KCC production environment. Implement STAR on KCC hardware in a quasi-production mode to facilitate testing. Migrate test data from the existing production (legacy) environment. Interface with the existing file-based document management repository with read-only access. Develop and test data mapping and migration scripts. Perform solution and support technology training and mentoring for end users and technical staff.

#### **Iteration 5 – Production Roll-out of Docket Management, eFiling and Web Portal**

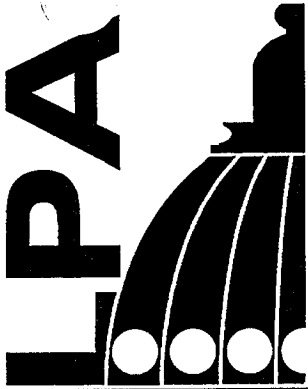
Complete development and testing for docket management, eFiling and public web portal. Perform data migration and cut-over to production. Freeze current production (legacy) environment and modify to allow read-only access. Go-live on new docket management, eFiling and web portal. Develop and test data mapping and migration scripts. Perform solution and support technology training and mentoring for end users and technical staff.

#### **Iteration 6 – Transportation, Fiscal, Assessments and Interfaces**

Complete development and testing for Transportation, Fiscal and other interfaces as agreed in Iteration 1 and subsequently. Implement quarterly assessment management process. Perform remaining system customizations according to KCC's priorities. Develop and test data mapping and migration scripts. Migrate data and cut-over to production all remaining legacy functions as identified in the project plan. Perform final training and mentoring for end users and technical staff.

#### **Iteration 7 – Post Implementation Acceptance**

Stabilize the production environment and resolve all outstanding high and medium priority issues. Perform final system acceptance. Release retainage amount for payment to ACO following three months of zero reports of high or medium priority issues. Complete all CITO close-out activities.



# Legislative Post Audit Compliance & Control Audit Report Highlights

Highlights

## State Agency Information Systems: Reviewing Selected Security Controls in State Agencies

### Report Highlights

July 2009 • 09CC03

#### Audit Concern

The Legislative Post Audit Committee has directed us to conduct ongoing information systems security audits as an adjunct to our compliance and control audits.

#### Other Relevant Facts & Findings

- The agencies reviewed in this report were the Judicial Branch, the Department of Transportation, the Kansas Public Employees Retirement System, the Board of Nursing, and the State Treasurer's Office.
- Good password controls include policies, training, server settings, and periodic password testing.
- Manufacturers develop software patches to address vulnerabilities as they are discovered.
- Only 6 of 133 servers (5%) and 4 of 161 workstations (2%) were significantly behind on operating system patches (e.g., Windows or Linux).
- 30 of 133 servers (23%) were significantly behind on application patches (e.g., Microsoft Office, Adobe Reader).

Estimated Cost Savings as a  
Result of This Audit:  
NONE

**AUDIT QUESTION:** How Well Do Selected State Agencies Control Network Passwords and Keep Operating Systems Up-To-Date?

#### AUDIT ANSWER and KEY FINDINGS:

- Each of the five agencies we reviewed could do a better job of controlling passwords:
  - three agencies had weak password policies
  - two agencies had weak password settings.
  - we were able to crack 23% to 58% of the agencies' passwords, primarily because many users create passwords that meet the network's requirements for strong passwords, but still are relatively easy to crack
- In general, the agencies did a good job of installing security patches on server and workstation operating systems (such as Microsoft Windows), but didn't do as good a job of installing patches on applications (such as Adobe Reader and Java).

#### We Recommended

- The agencies should address the problems we found with their password policies and settings, provide periodic password training to staff, and periodically test passwords.
- The agencies should install the missing security patches and arrange for periodic vulnerability scans of their networks.
- The State's Enterprise Security Office should educate all State agencies about the importance of vulnerability scanning.
- The Legislature should consider requiring all agencies get periodic vulnerability scans from the Enterprise Security Office.

**Agency Response:** The agencies generally concurred with the report's findings, conclusions, and recommendations, and all report already having started addressing the recommendations.

Attachment 11  
JIT 9-24-09



**DO YOU HAVE AN IDEA FOR  
IMPROVED GOVERNMENT EFFICIENCY OR COST SAVINGS?**

If you have an idea to share with us, send it to [ideas@lpa.ks.gov](mailto:ideas@lpa.ks.gov), or write to us at the address shown. We will pass along the best ones to the Legislative Post Audit Committee.

**LEGISLATIVE DIVISION OF  
POST AUDIT**

800 SW Jackson  
Suite 1200  
Topeka, Kansas 66612-2212  
Telephone (785) 296-3792  
FAX (785) 296-4482  
E-mail: [LPA@lpa.ks.gov](mailto:LPA@lpa.ks.gov)  
Website:  
<http://kslegislature.org/postaudit>

Barbara J. Hinton,  
Legislative Post Auditor

For more information about this  
audit report, please contact

**ALLAN FOSTER**  
(785) 296-3792  
[Allan.Foster@lpa.ks.gov](mailto:Allan.Foster@lpa.ks.gov)



LEGISLATURE OF KANSAS

**LEGISLATIVE DIVISION OF POST AUDIT**



800 SOUTHWEST JACKSON STREET, SUITE 1200  
TOPEKA, KANSAS 66612-2212  
TELEPHONE (785) 296-3792  
FAX (785) 296-4482  
E-MAIL: lpa@lpa.state.ks.us

June 25, 2009

To: Members, Legislative Post Audit Committee

Representative Virgil Peck Jr., Chair	Senator Terry Bruce, Vice-Chair
Representative Tom Burroughs	Senator Anthony Hensley
Representative John Grange	Senator Derek Schmidt
Representative Peggy Mast	Senator Chris Steineger
Representative Tom Sawyer	Senator Dwayne Umbarger

This report contains the findings, conclusions, and recommendations from our completed performance audit, *State Agency Information Systems: Reviewing Selected Security Controls in State Agencies*.

The report includes several recommendations for the Judicial Branch, the Department of Transportation, the Kansas Public Employees Retirement System, the Board of Nursing, the State Treasurer's Office, the State's Enterprise Security Office, and the Joint Committee on Information Technology. We would be happy to discuss these recommendations or any other items in the report with any legislative committees, individual legislators, or other State officials.

Barbara J. Hinton  
Legislative Post Auditor

# READER'S GUIDE

<b><i>The Big Picture</i></b>		<b><i>The Details</i></b>	
<b>Executive Summary</b>	Provides an overview of the questions we asked and the answers we found	<b>"At-a-Glance Box"</b>	Used to describe key aspects of the audited agency; generally appears in the first few pages of the main report
<b>Conclusions and Recommendations</b>	Located at the end of the report sections, and referenced in the Executive Summary	<b>Side Headings</b>	Point out key issues and findings
<b>Agency Response</b>	Included as the last Appendix in the report	<b>Charts, Tables, and Graphs</b>	Visually help tell the story of what we found
<b>List of Figures</b>	Lists all figures used in the report and their location (as shown at the end of the Executive Summary)	<b>Narrative Text Boxes</b>	Highlight interesting information or provide detailed examples

This audit was conducted by Allan Foster. Scott Frank was the audit manager. If you need any additional information about the audit's findings, please contact Allan Foster at the Division's offices.

Legislative Division of Post Audit  
 800 SW Jackson Street, Suite 1200  
 Topeka, Kansas 66612

(785) 296-3792  
 E-mail: [LPA@lpa.ks.gov](mailto:LPA@lpa.ks.gov)  
 Web: [www.kslegislature.org/postaudit](http://www.kslegislature.org/postaudit)

## Table of Contents

<b>How well do selected State agencies control network passwords and keep operating systems up-to-date?</b>	
<i>Each of the Five Agencies We Reviewed Could Do a Better Job of Controlling Passwords</i> .....	page 3
<i>The Agencies Did a Good Job of Patching Operating Systems, But Not as Good a Job of Patching Applications on Servers and Workstations.</i> .....	page 8
<b>Conclusion.</b> .....	page 11
<b>Recommendations for Executive Action</b> .....	page 12
<b>Recommendations for Legislative Action</b> .....	page 12

## List of Figures

<b>Figure 1-1: Comparing Agency Password Controls to Best Practice</b> .....	page 6-7
<b>Figure 1-2: Summary of the Operating System and Application Vulnerabilities Found on Servers and Workstations</b> .....	page 9

## List of Appendices

<b>Appendix A: Scope Statement</b> .....	page 13
<b>Appendix B: Agency Response</b> .....	page 15

# **State Agency Information Systems: Reviewing Selected Security Controls in State Agencies**

---

Each year State agencies become more dependent on their computer systems and on the data those systems contain to make decisions and fulfill their missions. More and more, computing is moving out of the data center and into the hands of staff who use the data to make decisions. Computers and computer networks also are being used to communicate with the public, provide services, and conduct business.

While these are positive developments that can result in increased efficiency, effectiveness, and better service, there are also significant risks associated with advances in technology that agencies should address and manage. At present there is little oversight of agencies' computer operations to monitor whether these risks are being adequately managed. This information system audit looks at two particularly important areas of IT security across a broad selection of State agencies, and answers the following question:

## **How well do selected State agencies control network passwords and keep operating systems up-to-date?**

To answer the question we chose to review five State agencies of various sizes for this audit: the Judicial Branch, the Department of Transportation, the Kansas Public Employees Retirement System, the Board of Nursing, and the State Treasurer's Office. At each agency, we reviewed password policies and server settings, obtained the agency's encrypted password file and attempted to crack its employees' passwords, and conducted a vulnerability assessment. The Enterprise Security Office—part of the Division of Information Systems and Communications within the Department of Administration—did the vulnerability scans for us and assisted us with interpreting the results.

A copy of the scope statement for this audit approved by the Legislative Post Audit Committee is included in *Appendix A*.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## How Well Do Selected State Agencies Control Network Passwords and Keep Operating Systems Up-To-Date?

### *Answer in Brief:*

*Each of the five agencies we reviewed could do a better job of controlling passwords. Three of the five agencies had weak password policies. Although most of the agencies had good password settings on their servers, we still were able to crack a significant percentage of the agencies' passwords—primarily because many users create passwords that meet the network's requirements for strong passwords, but still are relatively easy to crack. In general, the agencies did a good job of installing security patches on server and workstation operating systems (such as Microsoft Windows), but didn't do as good a job of installing patches on applications (such as Adobe Reader and Java). These and other findings are discussed in more detail in the sections that follow.*

### *Each of the Five Agencies We Reviewed Could Do a Better Job of Controlling Passwords*

Using passwords to control access to networks and computers is inherently risky, because it's become relatively easy to crack passwords. Despite the risk, passwords remain the most common form of security because they are far less expensive to use than more secure alternatives, such as tokens and thumbprint identification.

Because passwords are risky, it's extremely important that all aspects of an agency's system for controlling passwords are sound. To help ensure that users create strong passwords, agencies need the following:

- **Strong password policies**—Policies document important agency password requirements and help ensure consistency by making these requirements clear to everybody who needs to know them.
- **Strong password controls**—These are the agency's procedures that actually put the policies into practice. The following are the most important elements of a good system of password controls:
  - *Training* to help ensure that users understand the agency's policies and know how to make strong passwords.
  - *Server settings* that help ensure that users' passwords comply with the agency's policies. For example, if an agency's policies require users to create passwords that are at least eight characters long, the server should be set to reject passwords that are shorter than eight characters.
  - *Periodic testing* of the passwords to identify weak passwords, and areas where users need more training. This can be done with any number of inexpensive password cracking software packages that are available on line.

In this audit, we evaluated the password controls for five State entities:

- Board of Nursing
- Department of Transportation
- Kansas Public Employees Retirement System (KPERs)
- Office of Judicial Administration
- State Treasurer's Office

In order to evaluate the password controls for each agency, we compared the agency's password policies and the password settings that control access to its networks against best practices. We also had each agency provide us a copy of its master password file and attempted to crack the passwords using free software. This was strictly a test of strength of the agencies' passwords, and not an assessment of whether we could get through their firewalls and other layers of security to access their networks.

Our results are summarized in *Figure 1-1* on pages 6 and 7. The shaded cells in the figure indicate areas where the agencies' policies or control settings didn't meet best practices. Because of the highly confidential nature of these findings, we haven't identified the entities by name.

As the figure shows:

- **Three of the five agencies we reviewed had weak password policies.** Only two agencies had adopted strong password policies. One agency had almost no password policies but has since adopted strong policies and instituted the stronger requirements for their staff. Although the other two agencies had more complete policies, those policies were deficient in many areas such as requiring too few characters for passwords and not having policies to prevent people from reusing passwords.
- **Two of the agencies had weakly configured password settings on the servers that control access to their networks.** These are the settings that help ensure that the user's passwords comply with the agency's policies. While the agencies did better in this area, there were still some significant problems:
  - *One agency had very few control settings. For that agency, the risk was extremely high, because it allowed very short (five character) passwords and didn't require users to ever change them. These settings would allow a user to create incredibly weak passwords like "12345" or "password" and use those passwords forever.*
  - *Three agencies used a weak method of encryption for storing users' passwords, making them much easier to crack. Encryption methods systematically scramble passwords so they can't be easily read. There is an older encryption format that isn't as strong, and agencies generally should avoid storing passwords in this format unless they use very old systems that can't handle the newer format. Because none of the three agencies were using old systems, there was no reason to store passwords this way.*
  - *Three agencies required fewer than eight characters for passwords. Until recently either seven or eight characters was considered acceptable. However, many sources, including us, no longer consider seven characters sufficient.*

- **We cracked a significant number of passwords at each of the four agencies we were able to test, despite the fact that they had decent passwords.** There were two major reasons we were so successful:

- *Many of the users had "good" but not "great" passwords. Three of the four agencies we tested required complex passwords—passwords that include three of the four possible character types (uppercase, lowercase, numbers, and special characters). However, even complex passwords can be fairly easy to crack, depending on where the user places the numbers or special characters in their passwords. The overwhelming majority of the passwords we cracked met the complexity requirements, but they were constructed in a way that made them easy to crack. For example, a password such as "Password1" contains three of the four possible character types and contains 9 characters, yet is easy to crack. The accompanying profile box provides more information on how to create strong passwords.*
- *Three agencies used older, weak encryption. As described above, networks store users' passwords in one of two types of encrypted formats, and the weaker one allows passwords to be cracked more easily.*

### Passwords That Seem Complex May Be Easy To Crack

One of the important best practices for passwords is to require complex passwords. Complex passwords include a combination of three of the four types of characters on the keyboard—uppercase letters, lowercase letters, numbers, and special characters. The reason such passwords are considered complex is that it takes a long time to try every combination of characters—even for password cracking software. However, that statement assumes that passwords are random.

Unfortunately, people generally don't create random passwords. Studies have shown that when people use uppercase letters in passwords, they tend to use them at the start of the password. When people use numbers or special characters, they tend to use them at the end of the password. People also tend to use only those special characters that are on the top row of the keyboard. When you take those patterns into account, you eliminate a lot of possibilities.

People who develop password cracking software take advantage of these studies. Most software uses dictionary words or combinations of lower case letters for the base of a password, and then randomly substitutes other types of characters at the beginning and end of the password. This method only cracks those passwords that follow the patterns described above, but it may only take one password to break into a system.

Here are a few typical examples of passwords that meet the complexity requirements (each incorporates three of the four types of characters), but are pretty easy to crack (in our case, within five minutes) because of where the numbers and special characters have been placed:

- Computer1
- Mortimer11
- William#1
- Easter12
- steelers#1
- Abcdefg1

There are many strategies for creating passwords that are very strong and easy to remember, but one of the easiest is just to take a dictionary word and mix in some numbers and special characters. From the examples above, if we took "William#1" and made a couple easy changes it could be "wiL#1iam." It's basically the same password, but the character types are in different places. This password would be extremely difficult to crack.



**Figure 1-1  
Comparing Agency Password Controls to Best Practice**

PASSWORD POLICY AND CONTROL AREAS	Agency									
	1		2		3		4		5	
	Policy	Settings	Policy	Settings	Policy	Settings	Policy	Settings	Policy	Settings
<b>PASSWORD CHARACTERISTICS</b>										
Passwords should be at least 8 characters long.	6	5	7	7	8	8	7	7	7	8
Passwords should include at least 3 of 4 types of characters (uppercase, lowercase, numbers, special characters).	3 of 4	Disabled	2 of 4	Enabled	3 of 4	Enabled	3 of 4	Enabled	Enabled	No Setting (a)
<b>CHANGING PASSWORDS</b>										
Users should have to change passwords every 30-90 days.	No Policy	No Setting	30 days	35 days	60 days	56 days	30 days	42 days	60 days	No Setting (a)
Users should have to keep a new password for at least 1-2 days before they can change it.	(b)	No Setting	(b)	1 day	(b)	3 days	(b)	1 day	(b)	No Setting (a)
Users shouldn't be allowed to reuse a password for at least 1 year.	No Policy	No Setting	60 days	420 days	120 days	336 days	No Policy	1,008 days	365 days	No Setting (a)
<b>ACCOUNT LOCKOUT</b>										
Users' accounts should be locked out after 3-10 invalid attempts to log in.	No Policy	5 attempts	3 attempts	3 attempts	3 attempts	3 attempts	No Policy	5 attempts	3 attempts	(c)
Accounts should be locked out for 15-30 minutes.	No Policy	30 minutes	No Policy	5 minutes	Until Admin Unlocks	Until Admin Unlocks	No Policy	30 minutes	No Policy	(c)
The account lockout counter shouldn't reset for at least 15-30 minutes.	(b)	10 minutes	(b)	5 minutes	(b)	30 minutes	(b)	30 minutes	(b)	(c)

11-11

PASSWORD STORAGE											
Agency should not store passwords with weak encryption.	(b)	Weak	(b)	Strong	(b)	Weak	(b)	Strong	(b)	Weak	
OVERALL ASSESSMENT OF POLICIES AND SETTINGS											
Policies	Very Weak		Weak		Strong		Incomplete		Strong		
Settings	Very Weak		Fairly Strong		Fairly Strong		Strong		Weak		
PASSWORD CRACKING RESULTS											
Percent of passwords cracked within <u>5 minutes</u>	Not tested (d)		3%		35%		30%		39%		
Percent of passwords cracked within <u>24 hours</u>			23%		43%		45%		58%		
Issues with passwords	Not tested (d)										
<i>Weak Encryption</i>					X				X		
<i>Some Passwords Weak</i>			X (e)						X (f)		
<i>Good But Not Great Passwords</i>			X		X		X		X		
<i>Group Passwords</i>							X				
<p>Gray shading indicates areas that don't meet best practices.</p> <p>(a) This agency has its IT administrator assign all passwords, and employees aren't allowed to change them. The agency hasn't ever changed its passwords.</p> <p>(b) Policies don't typically address these areas.</p> <p>(c) The agency doesn't use account lockout, but has another control that accomplishes the same purpose.</p> <p>(d) We weren't able to extract this agency's password file, and therefore couldn't test the strength of the passwords. However, because of the agency's very weak password controls, agency officials agreed that the passwords also were likely to be very weak.</p> <p>(e) Some passwords were created before the agency adopted its current policies and were set to not expire. These passwords tended to be very short and weak.</p> <p>(f) Many of the passwords assigned by the administrator were well-constructed, but some only included two types of characters and thus were weak.</p> <p>Source: LPA analysis of agency policies, server settings, and password crack results.</p>											

One agency's experience illustrates the importance of using strong password encryption and training on how to create strong passwords. After we cracked 43% of the agency's passwords on our first test, officials corrected the problems with how passwords were encrypted and trained their staff on password best practices. They asked us to repeat our test to see if their efforts paid off. In the second test, we were able to crack only 4% of their passwords.

---

***The Agencies Did a Good Job of Patching Operating Systems, But Not as Good a Job of Patching Applications On Servers and Workstations***

The second major piece of this audit was to evaluate how well each of the agencies keeps its software up-to-date. Over time, vulnerabilities in computer software are discovered that could allow someone to break into or otherwise harm an agency's network. Software manufacturers are constantly developing fixes, or "patches," for the vulnerabilities as they are discovered. It's up to each agency's information technology staff to install the patches in order to keep their systems up-to-date.

Given the number of different types of software installed on modern networks, keeping up with patching can be a very difficult and time-consuming job. The most effective method of checking for missing patches is to periodically scan the network with vulnerability scanning software.

To determine whether the agencies did a good job of patching their software, we worked with staff from the State's Enterprise Security Office to conduct vulnerability scans of the agencies' servers and workstations. We looked for three types of things at each agency:

- patches missing from operating systems (e.g., Microsoft Windows or Linux)
- patches missing from applications (e.g., Microsoft Office, Adobe Reader)
- miscellaneous vulnerabilities not related to patches

All of the scans were done with the full knowledge and cooperation of the agencies. The vulnerability scans produce volumes of information about potential vulnerabilities—some of which are considered severe, but many of which are fairly minor. We provided the detailed results to each agency, but limited our analyses to only the most severe vulnerabilities.

**The agencies have done a good job of keeping the operating systems on their servers and workstations up-to-date.** The results of our vulnerability scan for operating systems are summarized in the top section of *Figure 1-2*. As was the case with passwords, these results are highly confidential, so we haven't matched the agency names with the results. Also, the agency letters used in this section don't correspond with the agency numbers in the password section.

11-13

**Figure 1-2**  
**Summary of the Operating System and Application Vulnerabilities**  
**Found on Servers and Workstations**

	AGENCY (a)										Total	
	A		B		C		D		E			
<b>OPERATING SYSTEMS</b>												
<b>Servers</b>												
# scanned	34	100%	41	100%	10	100%	10	100%	38	100%	133	100%
# missing <u>at least one</u> operating system patch	6	18%	3	7%	1	10%	5	50%	2	5%	17	13%
# missing <u>3 or more</u> operating system patches	3	9%	0	0%	1	10%	1	10%	1	3%	6	5%
<b>Workstations</b>												
# scanned	18	100%	12	100%	23	100%	55	100%	53	100%	161	100%
# missing <u>at least one</u> operating system patch	1	6%	1	8%	1	4%	14	25%	3	6%	20	12%
# missing <u>3 or more</u> operating system patches	0	0%	0	0%	1	4%	2	4%	1	2%	4	2%
<b>APPLICATIONS</b>												
<b>Servers</b>												
# scanned	34	100%	41	100%	10	100%	10	100%	38	100%	133	100%
# missing <u>at least one</u> application patch	16	47%	21	51%	3	30%	3	30%	6	16%	49	37%
# missing <u>3 or more</u> application patches	6	18%	18	44%	1	10%	2	20%	3	8%	30	23%
<b>Workstations</b>												
---not quantified---												

(a) The agency letters in this figure don't correspond with the agency numbers in **Figure 1-1** to help ensure that specific agencies can't be identified.

Source: LPA analysis of vulnerability scan results.

- **Only six of 133 servers (5%) were significantly behind (missing three or more) on operating system patches.** We did identify one server that was missing more than 100 patches. This turned out to be a test server that the agency wasn't actively using, and it took the server out of service after the scan.
- **Only four of 161 workstations (2%) were significantly behind on operating system patches.**

In addition to the servers noted in the figure, several agencies had unpatched servers that we didn't include in our analysis. In most cases, these servers had old, but critical applications that will fail if new operating system patches are installed. This can happen with poorly written software, or old software that's no longer supported and updated by the vendor. Another agency was having a new system developed and the vendor couldn't patch a couple of servers until the project was finished. Because these agencies presented sound business cases for continuing to operate these servers without patches, we didn't include them in the analysis that's presented in *Figure 1-2*.

**The agencies haven't done as good a job of patching the applications on servers and workstations.** The results of our vulnerability scan for application patches are summarized in bottom section of *Figure 1-2*. As the figure shows, the percent of servers missing three or more application patches ranged from 8% to 44%. By comparison, the range for operating system patches was much lower (0% to 10%).

Here's some more information about the missing application patches:

- **Each agency had at least one server with multiple Java vulnerabilities.** Java was by far the most common application vulnerability on servers. Java is a flexible programming language that is widely used in all kinds of software applications, especially in web applications. Java vulnerabilities can enable an attacker to launch malicious code on a server to take it over. In some cases agencies were running applications that required older versions of Java. While the agencies may not be able to upgrade to the newest version, they can still download patches for the older versions they use.
- **Two agencies had antivirus software that was significantly out-of-date on at least one server.** This is a very dangerous situation because new viruses are released every day. Servers should always have up-to-date antivirus software.
- **Some of the vulnerabilities could be avoided by removing unnecessary applications from servers.** According to best practices, an agency should only install applications on servers that need to be there. In general, there's no need to have common desktop software such as Microsoft Office, Adobe Reader, or Windows Media Player on a server, yet we found vulnerabilities associated with each of these. (The exception to best practice would be if these types of software are needed to help run other applications that really do need to be on a server.) Limiting the number of applications installed on a server reduces the chances for vulnerabilities.

11-14

In addition to the servers, there also were numerous unpatched applications on the workstations we scanned. However, because of the volume of results (there generally are more applications on workstations than servers, and we scanned three times as many workstations) we didn't attempt to quantify the number of missing application patches.

**One agency had workstations exposed to the Internet.** During the scans we also observed a few workstations in Agency D whose locations were visible from the Internet—one of which had a number of operating system vulnerabilities. (Best practice is for all agency workstations to be visible only inside the agency network and not be exposed directly to the Internet.) Agency officials told us those workstations weren't housed in their main offices and that they were in the process of changing their addresses so they would no longer be visible outside the agency's network.

***Conclusion:***

While security policies and network controls are important aspects of an agency's security management, not all security can be built in up front. The findings of this audit emphasize how important it is for agencies to continue to monitor the security of their networks on an on-going basis. The number of passwords we were able to "crack" using free and widely available password-cracking software—even in the agencies that had adopted good policies and strong server settings—shows that agencies still need to check periodically to make sure their staff have created strong passwords. The number of missing patches we identified on servers and workstations—especially the application patches—illustrates how important it is for agencies to scan their networks periodically to identify the patches they've missed.

Passwords can be tested using inexpensive software and the results of those tests are easy to interpret—either the passwords could be cracked quickly or they couldn't. On the other hand, the software used to scan networks can be very expensive, and interpreting the results can be very difficult. In order to ensure that all agencies are able to have their networks scanned periodically, while also keeping the cost manageable, it might make sense for the State to have a central agency responsible for periodically scanning all networks on behalf of the agencies.

**Recommendations for Executive Action:**

1. To help ensure that users within the agencies we audited create strong passwords, those agencies should do the following:
  - a. Adopt new policies or amend existing policies to address each of the policy weaknesses identified in *Figure 1-1* on page 6 and 7.
  - b. Change their server configurations to address each of the control setting issues identified in *Figure 1-1*.
  - c. Provide periodic training to staff on how to create strong passwords.
  - d. Periodically test the strength of their users' passwords with password cracking software.
2. To help ensure that the agencies we audited have up-to-date networks, those agencies should do the following:
  - a. Install the missing patches to address the "severe" vulnerabilities identified through our vulnerability scans.
  - b. Arrange to have their networks periodically scanned for vulnerabilities, either in-house, through the State's Enterprise Security Office (within the Division of Information System and Communications), or by an outside vendor.
  - c. In addition, Agency D should follow through with its plan to obtain new addresses for the workstations we identified that were exposed to the Internet.
3. To help ensure that all agencies periodically scan for vulnerabilities on their servers and workstations, the State's Enterprise Security Office should communicate to all State agencies the importance of vulnerability scanning.

**Recommendations for Legislative Action:**

1. To ensure that all agency networks are scanned for vulnerabilities on a regular basis, and that it is done in the most cost-effective manner, the Joint Committee on Information Technology should introduce legislation that would require all State agencies to have a periodic vulnerability scan conducted by the Enterprise Security Office.

## APPENDIX A

### Scope Statement

This appendix contains the scope statement for this audit of selected information technology security controls. This audit was conducted as part of the ongoing information system security audit work authorized by the Legislative Post Audit Committee.



## SCOPE STATEMENT

### **State Agency Information Systems: Reviewing Selected Security Controls in State Agencies**

Each year State agencies become more dependent on their computer systems and on the data those systems contain to make decisions and fulfill their missions. More and more, computing is moving out of the data center and into the hands of staff who use the data to make decisions. Computers and computer networks also are being used to communicate with the public, provide services, and conduct business. While these are positive developments that can result in increased efficiency and effectiveness and better service, there also are significant risks associated with advances in technology that agencies should be address and manage. At present there is little oversight of agencies' computer operations to monitor whether these risks are being adequately managed.

To help address these risks, the Legislative Post Audit Committee approved information system audits to be done as an adjunct to the Division's compliance and control audits. This information system audit looks at three particularly important areas of IT security across a broad selection of State agencies:

- 1. How well do select State agencies control network passwords and keep operating systems up-to-date?** For a sample of agencies, we would test the strength of the agencies' passwords with password-cracking software, and would use vulnerability scanning software to check a sample of the agencies' networks for missing security patches and other known vulnerabilities. For any agencies where we find problems, we would conduct in-depth interviews and review policies and procedures as necessary to determine the causes.

**Estimated time to complete: 7-9 weeks.**

## APPENDIX B

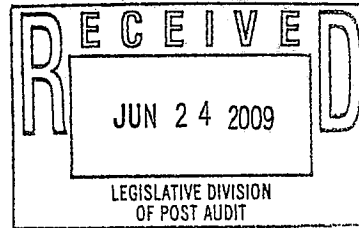
### Agency Responses

On June 17 we provided copies of the draft audit report to the Judicial Branch, the Department of Transportation, the Kansas Public Employees Retirement System, the Board of Nursing, the State Treasurer's Office, and the Division of Information Systems and Communication (DISC). Because the responses from the audited agencies contained confidential information, we have summarized them below. DISC didn't have anything confidential to respond to, so we've included its entire response.

The agencies generally concurred with the report's findings, conclusions, and recommendations, and all report already having started addressing the recommendations. One agency indicated it can't comply with one of our recommendations until after it does a major upgrade to its network operating system, but is committed to doing so. Another agency pointed out that the password tests and network scans we conducted bypassed its normal security measures.

June 23, 2009

Barbara Hinton, LPA  
800 Southwest Jackson Street, Suite 1200  
Topeka, KS 66612-2212



Dear Ms. Hinton,

I am delighted to respond to the recent audit findings (09CC03) of July 2009 performed by your office on 5 state entities over the past several weeks. As you are aware, the Enterprise Security Office assisted in one aspect of this inspection and consequently, some of the findings contained in the report come as no surprise.

The first area of consideration in this audit concerns how well selected state agencies control network passwords. The Kansas IT Security Council was responsible for recommending policy concerning this issue resulting in ITEC policy 7230, General Information Technology Enterprise Security Policy and its adjunct 7230A, the Security Requirements document. The latter is explicit in its treatment of passwords.

*Passwords must be:*

- Individually owned
- kept confidential and not shared with other users
- changed whenever disclosure has occurred or may have occurred, and
- changed at least every 60 days
- changed significantly (i.e., not a minor variation of the current password)
- a minimum of seven characters and contain alphanumeric characters and
- where allowed include special characters

*Passwords must not be:*

- repeated for at least six cycles of change or a year
- repeating sequences of letters or numbers (e.g. rrr, 123123)
- names of persons, places, or things that can be closely identified with the user (i.e., spouse, children or pet names)
- the same as the user id
- words that can be found in a dictionary
- displayed during the entry process
- written down and displayed in an obvious place
- the same for all systems the user accesses
- stored in any file program, command list, procedure, macro or script where
- It is susceptible to disclosure or use by anyone other than its owner.

June 23, 2009

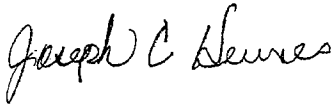
Page 2

Notwithstanding this policy, it is at once disappointing and understandable that some agencies are not in compliance, as an enforcement mechanism does not exist under the current governance structure. ITEC 7230/7230A was constructed with the understanding that if agencies had no organic security policy, that the ITEC policy documents would be the minimum defaults standard. It appears that some agencies in the audit failed to either have their own standard or to follow ITEC 7230A. What this highlights is the need for more periodic audits of this nature with the findings ultimately made public giving transparency to the policy and compliance process.

Regarding the Operating Systems and Applications Vulnerabilities' findings, it should be encouraging that awareness of operating systems vulnerabilities and the need for patching was found to be very good. Efforts to add additional applications patching (e.g., Adobe, Java and Microsoft Office) would appear to be in order. Over time, the later has not received as much publicity and effort and this should be addressed in an enterprise wide notification program.

Regarding the Recommendations for Executive Action, we concur with all of the suggestions. The Enterprise Security Office currently has capabilities to perform scans on a limited basis. To engage in an expanded, legislated, enterprise wide scanning program will require additional resources given the current and envisioned work load of the office. The current software package used for scanning has some inherent limitations with respect to false positive generation and reporting. As such, to follow the proposed recommendations, the need for one additional full time employee and software enhancements should be considered.

Sincerely,



Joe Hennes  
DISC Director

cc: Larry Kettlewell



9401 E K Drive  
Wichita, Kansas 67207-1804  
Tel: (316) 682-4537  
Fax: (316) 682-1201  
Web: www.ksturnpike.com

MARY E. TURKINGTON  
Chairman – Topeka

MICHAEL L. JOHNSTON  
President / CEO – Wichita

September 24, 2009

**Subject:** Response to JCIT questions posed to Kansas Turnpike Authority on September 22, 2009

**To the members of the Joint Committee on Information Technology**

The following is a written statement to the Joint Committee on Information Technology concerning questions posed by Aaron Klaassen with the Legislative Research Department on behalf of the Committee.

**Common computer projects between Kansas Department of Transportation and the Kansas Turnpike Authority**

**Q:** Are there any computer projects that KDOT and KTA are working together on? If so, what are they?

**A:** While both agencies are transportation related the business goals and operational needs of the two organizations are quite different and therefore the computer systems we use to support them are by necessity also quite different. The Authority's computer projects are designed specifically to support our toll business and the customers of the state's only toll road. All our business software is developed and maintained with in-house staff. We utilize only one IT consultant who works almost exclusively on toll system development and maintenance. While the two agencies certainly share many customers, the system sharing is limited primarily to the 800 Mhz radio system, the KANROAD/511 system and data sharing from their respective SCAN weather systems.

**Q:** Are there possibilities where KTA and KDOT could work together? In the future?

**A:** The Secretary of Transportation sits on the KTA board, and the Authority and KDOT have for more than 50 years maintained a mutual level of respect and cooperation. We are currently working on a cooperative effort with the KDOT ITS (Intelligent Transportation Systems) group to provide fiber along I-70 between Topeka and Kansas City and on I-35 South of Wichita for cameras and variable message boards which are part of Secretary Miller's ITS program. The Authority has developed some expertise with fiber optics. Several years ago we under took an effort to install 70 miles of fiber optic cable through some of the toughest terrain in Kansas, the scenic Flint Hills. In this endeavor we trained and developed a team of in-house staff in the procedures involved in installing, splicing and utilizing this fiber. This experience provided us the expertise to offer our assistance.

**Rep. Gary K. Hayzlett**  
Vice-Chairman  
Lakin

**Paul V. Dugan, Sr.**  
Secretary-Treasurer  
Wichita

**Sen. Dwayne Umbarger**  
Member  
Thayer

**Deb Miller**  
KDOT - Secretary of  
Transportation  
Member  
Topeka

*Attachment 12  
JCIT 9-24-09*

Response to JCIT questions posed to Kansas Turnpike Authority on September 22, 2009  
Page 2

If you would like any additional clarification or information concerning these or other questions please do not hesitate to contact me.

Respectfully yours,



Marty R. Wiltse  
Chief Information Officer  
Kansas Turnpike Authority



## State Broadband Project Overview

Joint Committee on Information  
Technology

Sept. 24, 2009

### Presentation Overview

#### Project Background

- American Recovery and Reinvestment Act (ARRA)  
Overview
- State Efforts to-date
- Initial Mapping Agreement

#### Project Overview

- Vendor Designation
- Grant Proposal
  - Planning
  - Mapping
  - Relationship to other efforts

1  
Attachment 13  
JCIT 9-24-09

## American Recovery and Reinvestment Act (ARRA)

Broadband Programs are administered by two federal agencies, in coordination w/FCC

- U.S. Department of Commerce National Telecommunications and Information Administration (NTIA)
- USDA Rural Utilities Service (RUS)

## U.S. DOC National Telecommunications and Information Administration (NTIA)

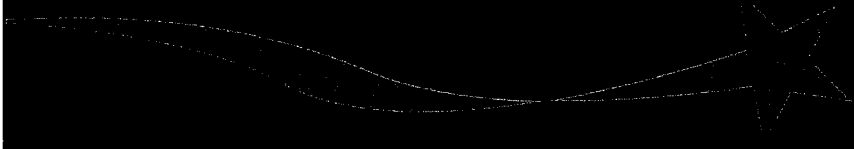
### **Broadband Technology Opportunities Program (BTOP)**

- \$4.7 billion in competitive grants nationwide
- Requires 20% non-federal match, but can be waived
- Applicants may be governments, educational institutions, non-profits, vendor community, others – if project deemed to be “in the public interest”
- First wave includes \$240 million: up to \$3.8M for data/mapping, up to \$500,000 for planning to states, one time only
- Up to \$150 million for sustainable adoption
- Up to \$50 million for public computer centers
- Up to \$1.2 billion for last/middle mile build-out funding.




## United States Department of Agriculture Rural Utilities Service (RUS)

### Broadband Initiatives Program (BIP)

- \$2.5 billion overall loans and grants
  - 75% of areas served by projects must be “rural” without sufficient access to high-speed broadband
  - Infrastructure that does not qualify for BTOP
  - Different criteria; more focused on infrastructure build-out
- 

### Round One of BTOP/BIP

- The current round closed 8/14/09
  - Requests for \$28 billion worth of projects; only \$4 billion available
  - Between 30-40 applications from Kansas entities requesting at least \$216 million in grants and \$152 million in loans, plus another 30-40 nationwide or regional requests affecting Kansas.
  - Federal rules still changing.
- 

## State of Kansas Efforts

- Kansas Department of Commerce designated lead coordinating agency by Governor
- Planning group formed this spring, working to identify stakeholders and approach
- Group includes representation from Commerce, DISC, KCC, State Library, Kan-Ed, Kansas Hospital Association, Agriculture, Aging, Health and Environment, and others

## State of Kansas Efforts (continued)

- Responded to joint Request for Comment on broadband program/needs by NTIA/RUS
- Toured state, holding seven regional focus groups to gain input from health community, county and local government, economic development and anchor institutions—talking non-infrastructure projects
- Convened industry representatives twice to-date – plans to continue their involvement, dialogue
- Created scoring matrix to use in evaluating proposals for state endorsement, vetted w/industry and stakeholder group.

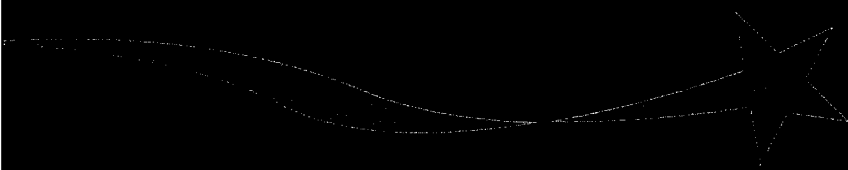
## Infrastructure Scoring Model

- Unserved Target Population - % of Total Project
- Rural Target Population
- Broadband Speed
- Process and Implementation
- Shovel Ready
- Local Providers - Application from provider currently operating in or serving Kansas vs. application from provider not currently in Kansas
- Permanent Job Creation
- Scalability


## Public Interest Projects Scoring Model

- Projects that meet the needs of the state for Telemedicine, Distance Learning, Economic Development, E-Government
- Projects that leverage partnerships and/or programs of existing anchor institutions, including schools, libraries, medical facilities and public safety organizations
- Projects with an emphasis on the needs of unserved Kansans
- Projects that place an emphasis on the needs of rural Kansans
- Projects that utilize local providers/partners for project development

## The State's Role with Applications

- The state will be asked to “green light” applications that meet the state’s priorities.
  - Scoring and final decisions come from the federal government.
  - We will review applications under BTOP or a combination of BIP/BTOP. BIP-only applications will not be reviewed by the state.
- 

## Mapping and Planning

- States are eligible for \$1.9 to \$3.8 million for mapping, plus \$500,000 for planning.
  - Through our designee, Connected Nation, we submitted an application for mapping and planning dollars in the Aug. 14 round.
  - Our mapping effort is already underway (prior to state grant awards).
- 

## Initial Mapping Contract

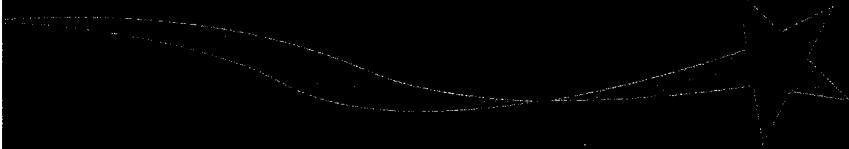
- Prior to the Mapping/Planning Notice of Funding Availability (NOFA), Kansas was working on mapping with the non-profit Connected Nation
- This effort was funded through a grant from the Information Network of Kansas (\$185,000) with assistance from Kansas Farm Bureau (\$15,000). Total cost around \$200,000.
- NOFA expanded data collection requirements beyond existing agreement and included requirement for five years of maintenance

## Kansas Mapping and Planning Grant Request

- For mapping, \$3.6 million federal plus \$903,415 match to total \$4.5 million.
- For planning, \$500,000 federal plus \$125,736 match to total \$625,736.
- Striving to maximize the in-kind portion of the match and seek grants for the cash portion.
- NTIA begins awards starting September 14, 2009 (haven't heard yet)


## State Mapping Project Overview

Data Collection/Mapping consists of:

- Gathering NTIA-defined data from ~100 Kansas providers, as well as “anchor institutions” (hospitals, libraries, etc.)
  - Preliminary set of data due Nov. 1, 2009
  - Substantially complete set of data due Feb. 1, 2010
  - Final set of data to be provided Mar. 1, 2010
  - Map updated semiannually for five years
- 

## State Planning Project Overview

Planning proposal consists of:

- Development and staffing of a broadband task force with focus on regional collaboration and planning
  - Coordination with Kansas colleges and universities on surveys (barriers, demand, etc.)
  - Some cost modeling for unserved areas
  - State Broadband summit
  - Intent to establish ongoing function
- 

## What we are doing now

- Continuing outreach (communicating w/industry, state working group, other parties)
- Continuing planning in support of grant proposal (communication, kickoff, etc.)
- Revising agreement with Connected Nation
- Connected Nation is continuing to collect data prospectively (incorporating NOFA requirements) as well as beginning preparation for map



**KANSAS**  
DEPARTMENT OF COMMERCE

(785) 296-3481

[www.kansascommerce.com](http://www.kansascommerce.com)



**KANSAS FARM BUREAU**  
**The Voice of Agriculture**

2627 KFB Plaza, Manhattan, Kansas 66503-8508 • 785-587-6000 • Fax 785-587-6914 • www.kfb.org  
800 SW Jackson St., Suite 1300, Topeka, Kansas 66612-1219 • 785-234-4535 • Fax 785-234-0278

*PUBLIC POLICY STATEMENT*

**JOINT COMMITTEE ON INFORMATION TECHNOLOGY**

**RE: Rural Broadband Access**

**September 24, 2009**  
**Topeka, Kansas**

**Testimony provided by:**  
**Brad Harrelson**  
**State Policy Director**  
**KFB Governmental Relations**

---

Mr. Chairman and members of the Committee, I am Brad Harrelson, State Policy Director—Governmental Relations for Kansas Farm Bureau. KFB is the state's largest general farm organization representing more than 40,000 farm and ranch families through our 105 county Farm Bureau Associations.

KFB appreciates this opportunity to comment on broadband access. Kansas Farm Bureau has taken an aggressive leadership role in spearheading an initiative to promote universal access to broadband internet service in Kansas.

Broadband access is essential to the success of rural Kansas and Kansas Farm Bureau members. It gives farmers, ranchers, Main Street entrepreneurs and the entire community access to global markets, an increased customer base, expanded educational and employment opportunities and a connection to the outside world that those who have broadband take for granted.

KFB member generated policy supports increased broadband access. It is a major policy issue for our organization.

*Attachment 14*  
*JCIT 9-24-09*



KFB has also reached out to non-agriculture entities to create statewide partnerships to pursue this policy priority. KFB has fostered an environment in which broadband is now recognized statewide as the essential element for our rural revitalization efforts.

In fact, KFB received a letter from all six members of our Kansas Congressional Delegation supporting two Broadband Stimulus applications.

We expect the full implementation of our broadband initiative to serve as a national example for rural states that are seeking to address the problems of demographic shifts and economic recession.

Our effort to achieve universal broadband access will unfold accordingly:

The entity Connect Kansas will work with all broadband providers in Kansas to create detailed maps of broadband coverage. Connect Kansas will use a nationally-recognized model for spurring broadband development and increasing broadband adoption. KFB was heavily involved in facilitating contact between the state and the organization Connected Nation to establish the mapping agreement.

In addition to supporting the state broadband map, KFB has applied for two federal broadband stimulus grants. The first seeks more than \$7 million to develop sustainable broadband access across the state by:

- Conducting comprehensive research on broadband use and barriers to adoption;
- Launching a statewide grassroots technology planning and awareness campaign in each of Kansas' 105 counties;
- Facilitating a partnership between the state and broadband providers, including estimating the true cost of extending service to underserved and unserved areas; and
- Increasing the use and ownership of computers and related devices that incite demand for broadband.

Our second application seeks \$2.6 million to develop a Broadband Communications Center (BCC) in Sedan, Kansas. Sedan, an economically depressed community of 1,300, has already mobilized significant, enthusiastic community support for the BCC.

The BCC will encompass all aspects of rural life, from education to health care to economic development. It will mobilize a community focused on technology, not size or location.

The establishment of the BCC represents a unique partnership of education, healthcare, community and business stakeholders with the common mission of revitalizing their community.

Aggressive program goals targeting bioscience education, workforce development and healthcare will create the foundation needed to create jobs in a community that has been weakened by demographic shifts, economic recession, floods and absence of a technology infrastructure. The Center will have a telemedicine room, distance learning classrooms, a computer lab, and video-conferencing rooms.

If Kansas is to achieve its full potential in the 21<sup>st</sup> century, all citizens must have access to broadband internet service. A detailed, accurate map of broadband service gaps; a sustainability plan; and a community project that will serve as a national model will surely advance the goal of universal access. Kansas Farm Bureau stands ready to assist you as you consider this important issue.

Congress of the United States  
Washington, DC 20515

August 31, 2009

The Honorable Lawrence Strickling  
Assistant Secretary  
National Telecommunications and Information Administration  
United States Department of Commerce  
1401 Constitution Avenue, NW  
Washington, DC 20230

RE: Kansas Farm Bureau Foundation Grant Application  
Public Computer Centers and Sustainable Broadband Adoption  
Easy Grants ID Nos. 799 & 196

Dear Mr. Assistant Secretary:

We write to offer our strong support for funding of the Kansas Farm Bureau Foundation Public Computer Center and Sustainable Broadband Adoption proposals submitted under the Broadband Technology Opportunities Program.


For ninety years, the Kansas Farm Bureau has assisted rural communities with sustainable development. Today, it is working with multiple public and private partners to bring new opportunities for families and businesses across the state, with a particular focus on education, health care, and entrepreneurship. Continued success in these efforts depends on extending broadband connectivity to unserved areas for schools, hospitals and rural health care facilities, homes and businesses, and on farms and ranches.


The Kansas Farm Bureau has developed two holistic approaches to address a lack of broadband service. First, the proposals would create grassroots demand for infrastructure deployment, promoting computer ownership and technological literacy. Secondly, the proposals seek funding for a unique Broadband Communications Center to be developed in the economically distressed community of Sedan, Kansas. This component will meet current and future needs of all sectors of the community.

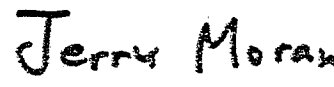
Kansas recognizes the strategic importance of broadband infrastructure. The applications before you compliment efforts already underway in the state to map broadband availability. Together, these efforts offer a comprehensive and long-term approach that will lead to better education, health care, and entrepreneurial opportunities in rural areas, as well as ensuring that farmers and ranchers can succeed in a highly competitive and changing agriculture industry.

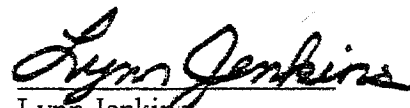
The Kansas Farm Bureau's proposals exemplify national goals of broadband deployment, job retention and creation, and more stable rural economies. We are confident that these proposals will perpetuate broadband availability state-wide and will affirmatively impact communities and families in our state. Thank you for your favorable consideration of these applications and please keep us informed of their progress.

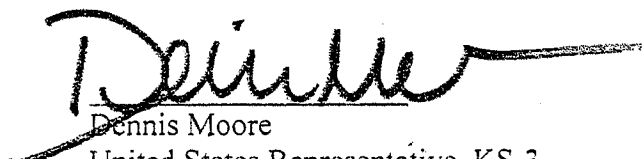
Sincerely,

  
Pat Roberts  
United States Senator

  
Sam Brownback  
United States Senator

  
Jerry Moran  
United States Representative, KS-1

  
Lynn Jenkins  
United States Representative, KS-2

  
Dennis Moore  
United States Representative, KS-3

  
Todd Tiahrt  
United States Representative, KS-4

September 24, 2009

Subject: Response to JCIT Questions Posed to the Kansas Department of Transportation on  
April 29<sup>th</sup>, 2009

To the members of the Joint Committee on Information Technology:

During the April 29, 2009 Joint Committee on Information Technology (JCIT), some questions were posed to myself and the Kansas Department of Transportation (KDOT) for which we did not have immediate answers and to which we responded that we would find the answers and reply in writing. This letter is in response to those questions and we have separated our responses by the information technology project we were reporting on when the questions were asked.

**Comprehensive Program Management System (CPMS) Replacement, Subproject IV**

Q: Does the Department of Transportation participate in KanView?

A: *Yes, KDOT fully participates in KanView and our annual revenue and expenditure data from FY2006, FY2007, FY2008 and FY2009 can currently be found in KanView.*

Q: Does the Kansas Turnpike Authority (KTA) utilize or have plans to utilize CPMS?

A: *The operational needs of our two organizations are quite different. Much of the functionality of CPMS and our replacement system WinCPMS was developed to support project and fund management for an integrated, multimodal transportation system across the State. Since the core business of the KTA is to maintain and operate the state's only toll road with no federal funding streams, CPMS is not an application that will be of much value to KTA and there are no plans for them to utilize WinCPMS in the future. If the need ever did arise where KTA needed access to any of KDOT's systems, we would gladly work with them to accommodate their request.*

*Attachment 15  
JCIT 9-24-09*

Q: How much interaction is there between the IT staff of KDOT and KTA?

A: *We do share a number of systems. The statewide 800 MHz radio system maintained by KDOT is shared with the KTA and we interface occasionally when issues arise with that system. 511/KANROAD road condition information is entered by the KTA into KDOT systems for integrated, statewide road conditions on 511. We also cooperate on fiber optic projects including Intelligent Transportation System projects.*

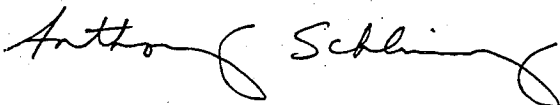
### **Financial Management System Integration (SMART) Project**

Q: Why is KDOT not planning on utilizing the inventory features of SMART at the SMART go-live timeframe of July 2010?

A: *The consumable inventory module was included in the FMS acquisition at the request of KDOT as a future implementation item. It was not intended to be part of the initial implementation and would be included in a future phase. The timeframe for this migration has not yet been determined. The capital inventory module is included in the FMS (SMART) initial implementation however KDOT did not include this module functionality as part of its system decommissioning effort. The integration of a new capital inventory system with our equipment management system will be a major system implementation project (for managing our heavy equipment/shop management etc.). With the additional efforts that were ongoing at the time (Crew Card, WinCPMS and SMART) and the information provided about the inventory module, the Agency did not believe that it would have been prudent to pursue at this time.*

If you would like any additional clarification or information on these projects or others, please do not hesitate to contact me.

Respectfully yours,



Anthony T. Schlinsog  
Chief Information Officer  
Kansas Department of Transportation

BUREAU OF COMPUTER SERVICES

Anthony Schlinsog, Chief

Dwight D. Eisenhower State Office Building

700 S.W. Harrison Street; Topeka, KS 66603-3745 • (785) 296-3727 • Fax: (785) 296-6222

Hearing Impaired - 711 • e-mail: [publicinfo@ksdot.org](mailto:publicinfo@ksdot.org) • Public Access at North Entrance of Building

15-2