

MINUTES OF THE SENATE WAYS AND MEANS COMMITTEE

The meeting was called to order by Chairman Jay Emler at 10:30 a.m. on March 3, 2010, in Room 548-S of the Capitol.

All members were present.

Committee staff present:

J. G. Scott, Kansas Legislative Research Department
Michael Steiner, Kansas Legislative Research Department
Dylan Dear, Kansas Legislative Research Department
Amy Deckard, Kansas Legislative Research Department
Aaron Klaassen, Kansas Legislative Research Department
Leah Robinson, Kansas Legislative Research Department
Jonathan Tang, Kansas Legislative Research Department
Jill Wolters, Office of the Revisor of Statutes
Daniel Yoza, Office of the Revisor of Statutes
Melinda Gaul, Chief of Staff
Shirley Jepson, Committee Assistant
James Fisher, Intern

Conferees appearing before the Committee:

Allan Foster, Principal Information Technology Auditor, Legislative Division of Post Audit

Others attending:

See attached list.

Introduction of proposed legislation

Senator Vratil moved to introduce a concurrent resolution requesting the Kansas supreme court to survey and study the Kansas court system (9rs1943). The motion was seconded by Senator Umbarger. Motion carried on a voice vote.

Action on Subcommittee report on Attorney General

Senator Taddiken moved to reopen the Subcommittee report on the Governor's budget recommendation the Attorney General for FY 2011. The motion was seconded by Senator Teichman. Motion carried on a voice vote.

Senator Taddiken moved to amend the Subcommittee report on the Governor's budget recommendation on the Attorney General for FY 2011 by inserting language pertaining to replacing \$17 million to the Interstate Water Litigation Fund (Attachment 1). The motion was seconded by Senator Lee. Motion carried on a roll call vote of 10-2 with 1 pass vote.

The Committee discussed whether it was appropriate to add the language to a budget bill or whether it should be addressed in separate legislation.

Senator Emler moved to adopt the Subcommittee report on the Governor's budget recommendation on the Attorney General for FY 2011 as amended. The motion was seconded by Senator Masterson. Motion carried on a voice vote.

Subcommittee report on Department of Revenue

Senator Schodorf presented the Subcommittee report on the Governor's budget recommendation for the Department of Revenue for FY 2011 and moved for the adoption of the Subcommittee report on the Department of Revenue for FY 2011 (Attachment 2). The motion was seconded by Senator Teichman. Motion carried on a voice vote.

Subcommittee report on Court of Tax Appeals

CONTINUATION SHEET

Minutes of the Senate Ways and Means Committee at 10:30 a.m. on March 3, 2010, in Room 548-S of the Capitol.

Senator Schmidt presented the Subcommittee report on the Governor's budget recommendation for the Court of Tax Appeals for FY 2011 and moved for the adoption of the Subcommittee report on the Court of Tax Appeals for FY 2011 (Attachment 3). The motion was seconded by Senator Lee. Motion carried on a voice vote.

Hearing on HB 2408 - State agencies periodic reviews of network security.

Daniel Yoza, Office of the Revisor of Statutes, provided an explanation of **HB 2408** (Attachment 4). Mr. Yoza stated that **HB 2408** would require the chief information technology officer (CITO) of each branch of government to develop a schedule to conduct vulnerability scans of their computer networks and carry out scans periodically. Responding to a question from the Committee, Mr. Yoza indicated that the legislation was brought forth by the Joint Committee on Information Technology (JCIT).

Allan Foster, Legislative Division of Post Audit (LPA), provided background information on **HB 2408** (Attachment 5). Mr. Foster stated that the bill would implement recommendations made in a July 2009 information technology security audit and addressed by JCIT. Mr. Foster stated that they found vulnerability in a number of computer applications on agency servers. LPA recommended that JCIT consider legislation requiring vulnerability scans on a periodical basis.

The Committee expressed concern that there is currently a policy in place which directs agencies to perform vulnerability scans. With no sanctions addressed in the legislation, the Committee questioned whether agencies would perform the scans and if they did not, there would be no penalty. The Committee also questioned who would pay for the scans.

The Committee felt the issue is important and the vulnerability of the state agencies' computer systems is a liability to the state if scans are not conducted on a routine basis.

The hearing on HB 2408 was closed.

Senator Kelly moved to not report **HB 2408** out favorably. The motion was seconded by Senator Kultala.

Senator McGinn made a substitute motion to extract language currently in the legislation and replace with language to dissolve the Joint Committee on Information Technology. The motion was withdrawn.

The original motion passed on a voice vote.

- ◆ The Committee requested a report on JCIT - how many times they meet each year, who receives the JCIT annual report and details of how the committee was put in place.

Senator Vratil moved to request that the Committee chairman write a letter to the chief information technology officer (CITO) of each branch of the government requesting information on how the recommendations of the LPA audit are being addressed and what steps are being taken to insure vulnerability scans are being performed in a timely manner. The motion was seconded by Senator Schmidt. Motion carried on a voice vote.

Briefing on Enhanced Medicaid Match

Amy Deckard, Legislative Research Department, provided a briefing on the Enhanced Medicaid Match. Ms. Deckard stated that the Centers for Medicare and Medicaid Services (CMS) recently announced it had reconsidered its previous determination that the "Clawback" payments were not eligible for the enhanced federal match authorized by the 2008 American Recovery and Reinvestment Act (ARRA). The application of the enhanced federal contribution rate will decrease the amount the state owes the federal government by \$24.7 million over two years.

The Clawback refers to monthly payments made by states to the federal government for individuals whose prescription services were previously made by the states but are now made by the federal government under

CONTINUATION SHEET

Minutes of the Senate Ways and Means Committee at 10:30 a.m. on March 3, 2010, in Room 548-S of the Capitol.

Part D of the 2003 Medicare Modernization Act.

The enhanced match will be retroactive back to the beginning of the ARRA benefit period, October 2008. Current estimates from the Kansas Health Policy Authority (KHPA) indicate reduced State General Fund (SGF) payments in FY 2010 of \$16.4 million and \$8.3 million in FY 2011.

Adjournment

The next meeting is scheduled for March 4, 2010.

The meeting was adjourned at 11:50 a. m.

SENATE WAYS AND MEANS COMMITTEE

GUEST LIST

DATE: March 3, 2010

NAME	REPRESENTING
Maibow Jacobson	DDA
ALLAN Foster	LPA
Jim Conant	KDOR
Emely Mettsen-Schellus	Ks Health Institute
Kathie Woods	
Janae Jones	Virtual Health Group
KOB MEALY	KEMMEY & Assoc.
Cassie Sparks	Intern - Sen. Browner
Sara Haworth	Intern - Sen. Vicki Schmidt
Suzanne Wickle	KS Action for Children
Brad Williams	Board of Regents
Hannah Sanders	KHDA
Sheela D. Duro	Bumart
Joy Schwartz	Pratt Leadership
Brenda Dancy	Pratt Leadership
Billie Thompson	Pratt Leadership class
Ted Whitson	Pratt Leadership class
Laurie Kovach	Pratt Leadership
Lude Egging	Pratt Leadership
Matt Casey	GIA
Mike Deacon	James Bladen
Jackson Lindsay	Hein Law
Dan Gibb	KSAG

SENATE WAYS AND MEANS COMMITTEE

GUEST LIST

DATE: March 3, 2010

NAME	REPRESENTING
Tom BEALL	KSAO
Jana El-Koubyssi	KSAO
Dustin Meyer	KHPA
Scott Brunner	KHPA
Mike Huttless	HGR
Bruce Witt	Via Christ, Health
Dean Tollefson	himself
Denny Specklein	Kansas State Fair
Amy Craig	Kansas State Fair
Sarah Blasi	Pratt Leadership
Chris Hill	Pratt Leadership
Elizabeth Bell	Pratt Leadership

Proposed amendment
Senator Taddiken
February 25, 2010

Sec. 39. ATTORNEY GENERAL [insert new subsection as follows]

(i) (1) On July 1, 2011, or as soon thereafter as moneys are available, the director of accounts and reports shall transfer \$2,000,000 from the state water plan fund to the interstate water litigation fund of the attorney general.

(2) On July 1, 2012, or as soon thereafter as moneys are available, the director of accounts and reports shall transfer \$3,000,000 from the state water plan fund to the interstate water litigation fund of the attorney general.

(3) On July 1, 2013, or as soon thereafter as moneys are available, the director of accounts and reports shall transfer \$3,000,000 from the state water plan fund to the interstate water litigation fund of the attorney general.

(4) On July 1, 2014, or as soon thereafter as moneys are available, the director of accounts and reports shall transfer \$3,000,000 from the state water plan fund to the interstate water litigation fund of the attorney general.

(5) On July 1, 2015, or as soon thereafter as moneys are available, the director of accounts and reports shall transfer \$3,000,000 from the state water plan fund to the interstate water litigation fund of the attorney general.

(6) On July 1, 2016, or as soon thereafter as moneys are available, the director of accounts and reports shall transfer \$3,000,000 from the state water plan fund to the interstate water litigation fund of the attorney general.

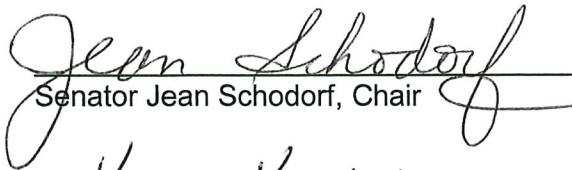
Also amend the title and section 1 to include fiscal years 2016 and 2017.

Senate Ways & Means Cmte
Date 3-03-2010
Attachment 1

FY 2011

SENATE WAYS AND MEANS SUBCOMMITTEE

Kansas Department of Revenue



Senator Jean Schodorf, Chair



Senator Kelly Kultala



Senator Vicki Schmidt



Senator Ruth Teichman

Senate Ways & Means Cmte
Date 3-03-2010
Attachment 2

House Budget Committee Report

Agency: Kansas Department of Revenue

Bill No. HB 2706

Bill Sec. 54

Analyst: Steiner

Analysis Pg. No. --

Budget Page No. 78

Expenditure Summary	Agency Request FY 2011	Governor Recommendation FY 2011	House Budget Committee Adjustments
Operating Expenditures:			
State General Fund	\$ 17,214,120	\$ 16,353,414	\$ 0
Other Funds	93,493,861	93,343,001	0
Subtotal	<u>\$ 110,707,981</u>	<u>\$ 109,696,415</u>	<u>\$ 0</u>
Capital Improvements			
State General Fund	\$ 0	\$ 0	\$ 0
Other Funds	0	0	0
Subtotal	<u>\$ 0</u>	<u>\$ 0</u>	<u>\$ 0</u>
TOTAL	<u><u>\$ 110,707,981</u></u>	<u><u>\$ 109,696,415</u></u>	<u><u>\$ 0</u></u>
FTE positions	1096.0	1096.0	0.0
Non FTE Uncl. Perm. Pos.	20.0	20.0	0.0
TOTAL	<u><u>1,116.0</u></u>	<u><u>1,116.0</u></u>	<u><u>0.0</u></u>

Agency Request

The **agency** requests FY 2011 operating expenditures of \$110,707,981, including \$17,214,120 from the State General Fund. The request is an all funds increase of \$3,993,331, or 3.7 percent, and a State General Fund increase of \$331,330, or 2.0 percent, above the FY 2010 estimate. The request includes one enhancement to replace 12 agency vehicles. The enhancement totals \$160,860 and is funded entirely through the Division of Vehicles Operating Fund. Without the enhancement, the request would be an all funds increase of \$3,832,471, or 3.6 percent above the FY 2010 estimate. The overall increase is partially attributable to an increase in costs associated with fringe benefits and an increase in the Division of Vehicles Modernization Fund. The increase was offset by modest declines in several special revenue funds including the VIPS/CAMA Technology Hardware Fund, the Vehicles Dealers and Manufacturers Fee Fund and the Special County Mineral Production Fund.

Governor's Recommendation

The **Governor** recommends FY 2011 operating expenditures of \$109,696,415 including \$16,353,414 from the State General Fund. The recommendation is an all funds increase of \$3.5 million, or 3.3 percent, and a State General Fund decrease of \$22,892, or 0.1 percent, from the Governor's FY 2010 recommendation. The increase is mostly attributable to the continuation of the Division of Vehicles Modernization Project.

The recommendation is an all funds decrease of \$1,011,566, or 0.9 percent, and a State General Fund decrease of \$860,706, or 5.0 percent, below the agency's FY 2011 request. The decrease is due to the Governor recommending the agency's reduced resources package of \$860,706. Included in the Governor's FY 2011 recommendation is a transfer of \$1.0 million from the Southeast KS Business Recovery State Emergency Fund (Southeast Kansas Business Restoration Assistance Program) to the State General Fund for FY 2011. The transfer amount represents an unused portion of funding set aside for business recovery efforts in southeast Kansas as a result of flooding.

House Budget Committee Recommendation

The **Budget Committee** concurs with the Governor's recommendation.

House Committee Recommendation

The **House Committee** concurs with the House Budget Committee's recommendation with the following recommendation:

1. Consider at Omnibus the possibility of stopping or slowing all of the Department of Revenue's technology upgrades in order to achieve savings. Included in the upgrades would be the Division of Vehicles Modernization Program and the VIPS/CAMA Program. Also included would be an overview of all of the Department of Revenue's fees and how those funds are allocated within the Department.
-

Senate Budget Committee Report

Agency: Kansas Department of Revenue

Bill No. 556

Bill Sec. 54

Analyst: Steiner

Analysis Pg. No. --

Budget Page No. 78

Expenditure Summary	Agency Request FY 2011	Governor Recommendation FY 2011	Senate Budget Committee Adjustments
Operating Expenditures:			
State General Fund	\$ 17,214,120	\$ 16,353,414	\$ (401,897)
Other Funds	93,493,861	93,343,001	0
Subtotal	<u>\$ 110,707,981</u>	<u>\$ 109,696,415</u>	<u>\$ (401,897)</u>
Capital Improvements			
State General Fund	\$ 0	\$ 0	\$ 0
Other Funds	0	0	0
Subtotal	<u>\$ 0</u>	<u>\$ 0</u>	<u>\$ 0</u>
 TOTAL	 <u><u>\$ 110,707,981</u></u>	 <u><u>\$ 109,696,415</u></u>	 <u><u>\$ (401,897)</u></u>
 FTE positions	 1096.0	 1096.0	 0.0
Non FTE Uncl. Perm. Pos.	20.0	20.0	0.0
TOTAL	<u><u>1,116.0</u></u>	<u><u>1,116.0</u></u>	<u><u>0.0</u></u>

Agency Request

The **agency** requests FY 2011 operating expenditures of \$110,707,981, including \$17,214,120 from the State General Fund. The request is an all funds increase of \$3,993,331, or 3.7 percent, and a State General Fund increase of \$331,330, or 2.0 percent, above the FY 2010 estimate. The request includes one enhancement to replace 12 agency vehicles. The enhancement totals \$160,860 and is funded entirely through the Division of Vehicles Operating Fund. Without the enhancement, the request would be an all funds increase of \$3,832,471, or 3.6 percent above the FY 2010 estimate. The overall increase is partially attributable to an increase in costs associated with fringe benefits and an increase in the Division of Vehicles Modernization Fund. The increase was offset by modest declines in several special revenue funds including the VIPS/CAMA Technology Hardware Fund, the Vehicles Dealers and Manufacturers Fee Fund and the Special County Mineral Production Fund.

Governor's Recommendation

The **Governor** recommends FY 2011 operating expenditures of \$109,696,415 including \$16,353,414 from the State General Fund. The recommendation is an all funds increase of \$3.5 million, or 3.3 percent, and a State General Fund decrease of \$22,892, or 0.1 percent, from the Governor's FY 2010 recommendation. The increase is mostly attributable to the continuation of the Division of Vehicles Modernization Project.

2-4

The recommendation is an all funds decrease of \$1,011,566, or 0.9 percent, and a State General Fund decrease of \$860,706, or 5.0 percent, below the agency's FY 2011 request. The decrease is due to the Governor recommending the agency's reduced resources package of \$860,706. Included in the Governor's FY 2011 recommendation is a transfer of \$1.0 million from the Southeast KS Business Recovery State Emergency Fund (Southeast Kansas Business Restoration Assistance Program) to the State General Fund for FY 2011. The transfer amount represents an unused portion of funding set aside for business recovery efforts in southeast Kansas as a result of flooding.

Senate Subcommittee Recommendation

The **Senate Subcommittee** concurs with the Governor's recommendation with the following adjustments:

1. Delete \$401,897, all from the State General Fund, for FY 2011 as part of the agency's 2.5 percent reduction.
2. Review at Omnibus the 9.0 vacant FTE positions in the Tax Operations Division. The agency is currently holding open 9.0 FTE positions due to reductions in the division's State General Fund appropriation. The agency has estimated that each vacant position has the potential to collect approximately \$1.3 million in tax revenue. Additionally, the agency has indicated that the average salary for the vacant 9.0 FTE positions is approximately \$50,000. The Subcommittee would like to note that funding some of the positions within the Division could yield a significant return on investment.
3. The Subcommittee would like to note SB 406 which would impose a \$10 fee for any delinquent taxpayer who enters into an installment plan in excess of ninety days from the date of the payment plan agreement. The supplemental note on SB 406 indicated that the number of people entering into payments plans has increased from 15,223 in 2007 to 33,090 in 2009. The fiscal note indicated the fee would generate approximately \$340,000 in revenue for FY 2011. Finally, the Subcommittee notes the revenues generated from the \$10 fee could be used to fill some of the vacant 9.0 FTE positions in the Tax Operations Division which could result in increased tax revenue collection. SB 406 has been passed by the Senate and is currently in the House Committee on Taxation.
4. The Subcommittee encourages passage of HB 2521 which would require the electronic filing of sales and withholding tax when the combination of both exceed \$45,000. All fees for paper filing in the original bill have been removed. The bill is required in order for the agency to implement its reduced resource package which totaled \$862,984, all from the State General Fund. If the necessary legislation does not pass then the Subcommittee recommends the Ways and Means Committee review at Omnibus. The bill is currently on General Orders in the House.
5. The Subcommittee expressed concern regarding the sweep of the Special County Mineral Production Tax Fund in FY 2009. The 2009 Legislature transferred \$1.5 million from the Special County Mineral Product Tax Fund to the State General Fund in 2009. The Special County Mineral Production Tax Fund is funded through an excise tax upon the severance and production of coal, oil, or natural gas and 7.0 percent of the collected tax is transferred to counties for reimbursement of the extraction of coal, oil, and natural gas. The Governor did

not recommend any further transfers from the Special County Mineral Production Tax Fund in FY 2010 or FY 2011.

6. The Subcommittee would like to commend the Department of Revenue for the accelerated collection of \$30.0 million.
7. The Subcommittee notes the Department of Revenue has simplified the electronic filing process which has resulted in significant costs savings. Included in the costs savings is a decrease in the number of paper forms. The Subcommittee would like the agency to simplify and improve the process for requesting paper forms.

FY 2011

SENATE WAYS AND MEANS SUBCOMMITTEE

Court of Tax Appeals



Senator Vicki Schmidt, Chair



Senator Janis Lee



Senator Mark Taddiken

Senate Ways & Means Cmte
Date 3-03-2010
Attachment 3

House Budget Committee Report

Agency: Court of Tax Appeals

Bill No. --

Bill Sec. --

Analyst: Steiner

Analysis Pg. No. --

Budget Page No. Vol. I, 78

Expenditure Summary	Agency Request FY 2011	Governor Recommendation FY 2011	House Budget Committee Adjustments
Operating Expenditures:			
State General Fund	\$ 1,455,698	\$ 1,382,913	\$ 0
Other Funds	580,992	653,777	0
Subtotal	<u>\$ 2,036,690</u>	<u>\$ 2,036,690</u>	<u>\$ 0</u>
Capital Improvements			
State General Fund	\$ 0	\$ 0	\$ 0
Other Funds	0	0	0
Subtotal	<u>\$ 0</u>	<u>\$ 0</u>	<u>\$ 0</u>
TOTAL	<u><u>\$ 2,036,690</u></u>	<u><u>\$ 2,036,690</u></u>	<u><u>\$ 0</u></u>
FTE positions			
FTE positions	26.0	26.0	0.0
Non FTE Uncl. Perm. Pos.	0.0	0.0	0.0
TOTAL	<u><u>26.0</u></u>	<u><u>26.0</u></u>	<u><u>0.0</u></u>

Agency Estimate/Request

The **agency's** request for FY 2011 operating expenditures is \$2,036,690, including \$1,455,698 from the State General Fund. Included in the agency's estimate is \$5,000 in the Duplicating Fees Fund and \$575,992 in the Filing Fee Fund. The request is an all funds increase of \$58,307, or 5.3 percent, and a State General Fund increase of \$28,807, or 2.0 percent, above the FY 2010 revised estimate. The increase is largely attributable to increased costs associated with fringe benefits such as higher insurance premiums and KPERS employer contributions.

Governor's Recommendation

The **Governor** recommends FY 2011 operating expenditures of \$2,036,690, including \$1,382,913 from the State General Fund, which is the same as the agency's FY 2010 estimate.

House Budget Committee Recommendations

The **Budget Committee** concurs with the Governor's recommendation.

House Committee Recommendation

The **Committee** concurs with the Budget Committee recommendation.

Senate Budget Committee Report

Agency: Court of Tax Appeals

Bill No. 556

Bill Sec. 53

Analyst: Steiner

Analysis Pg. No. --

Budget Page No. 78

Expenditure Summary	Agency Request FY 2011	Governor Recommendation FY 2011	Senate Subcommittee Adjustments
Operating Expenditures:			
State General Fund	\$ 1,455,698	\$ 1,382,913	\$ (33,986)
Other Funds	580,992	653,777	33,000
Subtotal	<u>\$ 2,036,690</u>	<u>\$ 2,036,690</u>	<u>\$ (986)</u>
Capital Improvements			
State General Fund	\$ 0	\$ 0	\$ 0
Other Funds	0	0	0
Subtotal	<u>\$ 0</u>	<u>\$ 0</u>	<u>\$ 0</u>
TOTAL	<u><u>\$ 2,036,690</u></u>	<u><u>\$ 2,036,690</u></u>	<u><u>\$ (986)</u></u>
FTE positions	26.0	26.0	0.0
Non FTE Uncl. Perm. Pos.	0.0	0.0	0.0
TOTAL	<u><u>26.0</u></u>	<u><u>26.0</u></u>	<u><u>0.0</u></u>

Agency Request

The **agency's** request for FY 2011 operating expenditures is \$2,036,690, including \$1,455,698 from the State General Fund. Included in the agency's estimate is \$5,000 in the Duplicating Fees Fund and \$575,992 in the Filing Fee Fund. The request is an all funds increase of \$58,307, or 5.3 percent, and a State General Fund increase of \$28,807, or 2.0 percent, above the FY 2010 revised estimate. The increase is largely attributable to increased costs associated with fringe benefits such as higher insurance premiums and KPERS employer contributions.

Governor's Recommendation

The **Governor** recommends FY 2011 operating expenditures of \$2,036,690, including \$1,382,913 from the State General Fund, which is the same as the agency's FY 2010 estimate.

Senate Subcommittee Recommendations

The **Senate Subcommittee** concurs with the Governor's recommendation with the following recommendations:

1. Delete \$33,986, all from the State General Fund, for FY 2011 to reduce the agency's budget by 2.5 percent.
2. Add \$33,000, all from the Court of Tax Appeals Filing Fee Fund in FY 2011, to offset the agency's State General Fund reduction. The agency has indicated that filing fees will be increased in FY 2011 to offset decreases in the agency's State General Fund appropriation. The addition of \$33,000 will increase the expenditure limitation on the agency's Filing Fee Fund by \$33,000 from \$648,777 to \$681,777.
3. The Subcommittee would like to note that as the agency's State General Fund appropriation has been reduced, the agency has had to rely on fees to fund agency operations. The Subcommittee expresses concern that any further budget cuts to the agency could prevent individuals from accessing the Court of Tax Appeals.
4. The Subcommittee would like to bring to the attention of the Committee the cost saving measure the agency has adopt as a result of continuing budget reductions. The current chief hearing officer is also serving as the agency's executive director. Furthermore, the Subcommittee would like to note that in light of the agency's budget reductions the backlog of current cases has been eliminated despite the increase in filings. In 2009 the agency had 7,422 filings and in FY 2011 the agency is expecting to have 11,494 filings.
5. The Subcommittee would also like to note that the agency may be forced to eliminate travel to attend hearings throughout the State if further reductions are made to the agency's budget. Substantive legislation may be required if the agency is forced to suspend travel.

Office of Revisor of Statutes
300 S.W. 10th Avenue
Suite 24-E, Statehouse
Topeka, Kansas 66612-1592
Telephone (785) 296-2416 FAX (785) 296-6668

MEMORANDUM

To: Senate Ways and Means
From: Daniel Yoza, Assistant Revisor
Date: March 1, 2010
Subject: HB 2408

House Bill 2408 requires the chief information technology officer (CITO) of each branch of government to develop a schedule to conduct vulnerability scans of each state agency's computer networks and to require each state agency to carry such scans out according to the schedule.

The scans shall be conducted in accordance with policies of each branch of government's CITO.

This bill requires each state agency to do a vulnerability scan at least once per year.
This bill, if passed, would take effect on July 1, 2010.



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
www.kslegislature.org/postaudit

Testimony for the Senate Ways and Means Committee on HB 2408

Allan Foster, Principal IT Auditor

March 3, 2010

Mr. Chairman and members of the Committee, thank you for allowing me to appear before you on behalf of the Legislative Post Audit Committee to provide neutral testimony on HB 2408.

As you may know, this bill would implement recommendations made in our July 2009 IT security audit, *State Agency Information Systems: Reviewing Selected Security Controls in State Agencies*. Based on our recommendation, the JCIT Committee introduced this bill. The Post Audit Committee also considered introducing it but decided to defer to JCIT.

Our audit focused on several things, one of which was how agencies were managing the vulnerabilities in their servers and workstations. "Vulnerabilities" are flaws in the computer code that make up an operating system or an application on the computer. There are millions of lines of code in any one computer. These flaws are what allow viruses to infect a computer or allow a criminal to take over your computer and steal your identity. One of the things we did to evaluate agencies' vulnerabilities was to work with the staff of the Enterprise Security Office of DISC to actually scan their servers and a sample of workstations with software designed to identify such vulnerabilities. That software is a very effective and efficient way to identify a very broad range of vulnerabilities. You just attach to the agency's network and start it running. It runs for a couple of hours then provides a very comprehensive list of vulnerabilities ranked by importance, and how to fix them.

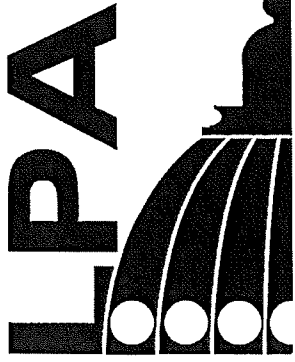
The table on page 9 of the report shows a summary of the results of our scans of the five agencies. Overall, we found that agencies did a pretty good job of controlling the vulnerabilities in their operating systems, with only 5% of servers and 2% of workstations having three or more un-patched vulnerabilities. This was not totally unexpected because Microsoft makes it fairly easy to keep operating systems patched.

However, the results were far worse when we looked at vulnerabilities in applications on servers, such as Adobe Reader and Windows Office. Nearly one quarter of the servers were susceptible to three or more vulnerabilities. It used to be that hackers focused almost totally on operating system vulnerabilities, but in the last couple years that focus has shifted to application vulnerabilities, so failing to patch software like Adobe can be a very dangerous thing.

Senate Ways & Means Cmte
Date 3-03-2010
Attachment 5

Since there are so many different types of applications that can be on servers it's almost impossible to know when you have vulnerabilities that need to be patched unless you periodically run vulnerability scanning software. Thus our recommendation that JCIT consider legislation requiring vulnerability scans. Also, because this software isn't free, and takes some skill to use well, it would be most efficient if some central office such as the Enterprise Security Office purchase the software and do the scans for agencies.

I'd be happy to answer any questions you may have.



COMPUTER SECURITY AUDIT REPORT

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

**A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
July 2009**

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 I-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.

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

	AGENCY (a)										Total	
	A	B	C	D	E							
OPERATING SYSTEMS												
Servers												
# 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%
Workstations												
# 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%
APPLICATIONS												
Servers												
# 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%
Workstations												
---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.

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.