



COMPUTER SECURITY AUDIT REPORT

**State Agency Information Systems: Reviewing the
Kansas Health Policy Authority's Management of
Those Systems**

Executive Summary ***with Conclusions and Recommendations***

**A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
August 2008**

Legislative Post Audit Committee

Legislative Division of Post Audit

THE LEGISLATIVE POST Audit Committee and its audit agency, the Legislative Division of Post Audit, are the audit arm of Kansas government. The programs and activities of State government now cost about \$10 billion a year. As legislators and administrators try increasingly to allocate tax dollars effectively and make government work more efficiently, they need information to evaluate the work of governmental agencies. The audit work performed by Legislative Post Audit helps provide that information.

We conduct our audit work in accordance with applicable government auditing standards set forth by the U.S. Government Accountability Office. These standards pertain to the auditor's professional qualifications, the quality of the audit work, and the characteristics of professional and meaningful reports. The standards also have been endorsed by the American Institute of Certified Public Accountants and adopted by the Legislative Post Audit Committee.

The Legislative Post Audit Committee is a bipartisan committee comprising five senators and five representatives. Of the Senate members, three are appointed by the President of the Senate and two are appointed by the Senate Minority Leader. Of the Representatives, three are appointed by the Speaker of the House and two are appointed by the Minority Leader.

Audits are performed at the direction of the Legislative Post Audit Committee. Legislators

or committees should make their requests for performance audits through the Chairman or any other member of the Committee. Copies of all completed performance audits are available from the Division's office.

LEGISLATIVE POST AUDIT COMMITTEE

Representative Peggy Mast, Chair
Representative Tom Burroughs
Representative John Grange
Representative Virgil Peck Jr.
Representative Tom Sawyer

Senator Nick Jordan, Vice Chair
Senator Les Donovan
Senator Anthony Hensley
Senator Derek Schmidt
Senator Chris Steineger

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.state.ks.us
Website:
<http://kslegislature.org/postaudit>

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

The Legislative Post Audit Committee and the Legislative Division of Post Audit have launched an initiative to identify ways to help make State government more efficient. If you have an idea to share with us, send it to ideas@lpa.state.ks.us, or write to us at the address above.

You won't receive an individual response, but all ideas will be reviewed, and Legislative Post Audit will pass along the best ones to the Legislative Post Audit Committee.

The Legislative Division of Post Audit supports full access to the services of State government for all citizens. Upon request, Legislative Post Audit can provide its audit reports in large print, audio, or other appropriate alternative format to accommodate persons with visual impairments. Persons with hearing or speech disabilities may reach us through the Kansas Relay Center at 1-800-766-3777. Our office hours are 8:00 a.m. to 5:00 p.m., Monday through Friday.



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

August 20, 2008

To: Members of the Kansas Legislature

This executive summary contains the findings, conclusions, and recommendations from our completed performance audit, *State Agency Information Systems: Reviewing the Kansas Health Policy Authority's Management of Those Systems*.

The report includes several recommendations for the Kansas Health Policy Authority. 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.

If you would like a copy of the full audit report, please call our office and we will send you one right away

A handwritten signature in black ink that reads "Barbara J. Hinton". The signature is fluid and cursive, with the first letters of each name being capitalized and prominent.

Barbara J. Hinton
Legislative Post Auditor

EXECUTIVE SUMMARY

LEGISLATIVE DIVISION OF POST AUDIT

Overview of the Kansas Health Policy Authority

The Health Policy Authority was created in 2005 to better coordinate health care programs. *In creating the Authority, the Legislature consolidated State-funded health insurance programs such as Medicaid, the State Employees Health Plan, the State Self Insurance Fund, Medikan, and the State Children's Health Insurance Program (HealthWave) by moving them to the Authority. The Authority contracts with two consulting firms, EDS and MAXIMUS, to process Medicaid claims and to manage the eligibility process.*

The Authority contracts with DISC to handle the technical aspects of its information technology network. *The Authority has a small information technology staff to manage technology issues such as security, but they aren't technical staff and aren't involved in the day-to-day aspects of network operations. DISC provides the Authority four dedicated support staff who are responsible for maintaining the Authority's network and servers, monitoring the performance of the systems, and providing network security and customer support.*

Question 1: How Well Does the Authority Manage the Security of Its Information Systems?

Although there are many good aspects to the Authority's security-management system, it lacks important safeguards in each of the major parts of that system. *To effectively manage computer security, agencies need a dynamic security-management process that includes risk assessment, policy development, policy dissemination, and monitoring. Each of these activities should flow into the next in a cycle of activity that helps the agency ensure that policies remain current and that important risks are addressed. To assess how well the Authority manages security, we compared its system to the best practices described above. As the figure on the next page shows, we found that the Authority performs many good security activities covering each of the major categories of security-management. However, the Authority's system is missing several important activities in each category, limiting the effectiveness of its security-management program.*

The Authority doesn't consider risks that are specific to the agency as part of its risk-assessment process. *Risk assessment is a process that allows officials to identify the security risks the agency faces, and to focus the agency's limited resources more effectively. A good*

Comparing the Authority's Security Management System To Best Practices

Positive Aspects of the Authority's System	Problem Areas We Found
<u>RISK ASSESSMENT</u>	
The information technology manager uses the ITEC security self-assessment to identify areas where policies are needed.	- The Authority hasn't taken steps needed to assess the agency's unique risks. - The information technology manager doesn't involve anyone else in the risk-assessment process.
<u>POLICY DEVELOPMENT</u>	
- The Authority's policy development group has been very active, developing and recommending new policies in a number of areas. - The information technology manager appears to understand the need for good security policies. - The Authority appears to work well with DISC support staff in resolving the policy problems they identify.	- The Authority had too many policies in draft form that have been awaiting approval for months. Policies aren't put into place until they're approved. - The Authority relies heavily on the ITEC default policies but hasn't done enough to make staff aware of them - Three of the Authority's policies were inadequate, and it had no policy in another area
<u>POLICY DISSEMINATION/PROMOTING SECURITY AWARENESS</u>	
- The Authority provides good security awareness training to new employees - The Authority publishes its policies on its intranet site	- The Authority doesn't provide ongoing security awareness training, and does a poor job of disseminating information about its security policies. - Employees who came to the Authority from SRS weren't required to take the security awareness training. As a result there are a large number of employees who haven't had training since 2005. - DISC support staff didn't always know when the Authority approved new policies. As a result, we identified two network settings relating to passwords that weren't set properly because the staff weren't aware of the policies. - The Authority's staff showed a lack of security awareness and understanding of the agency's security policies in answering our security awareness survey. - The lack of security awareness among the staff allowed our consultant to access confidential documents and to get some employee passwords.
<u>MONITORING AND EVALUATION</u>	
DISC support staff have developed a good process for monitoring the network. As a result, <u>technical</u> issues are well-monitored.	- The Authority management doesn't monitor: ➤ <i>work done by support staff</i> ➤ <i>compliance with policies</i> ➤ <i>effectiveness of policies</i>
<u>FLOW BETWEEN AREAS</u>	
	- The Authority's security policies don't flow from a complete risk assessment - The Authority generally doesn't use content from its policies in training - Management doesn't use the results of the technical monitoring or managerial monitoring in assessing risks
Source: LPA review of the Authority's security management system	

process helps identify the agency's critical assets, its unique security risks, and strategies or methods to help mitigate the risks. To be most effective, it should be a joint effort between an agency's business officials and security officials. In reviewing the Authority's risk assessment process, we identified two significant problems. First, the Authority hasn't taken steps needed to assess the agency's unique risks. The risk assessment process was limited to completing a security self assessment covering generic security policies. That isn't sufficient to identify risks unique to the Authority. Second, the Information Systems Manager doesn't involve anyone else in the process. Involving the DISC support staff and business staff would add important knowledge and expertise currently missing from the assessment process.

The Authority's process for developing policies could be improved by approving policies more quickly. The Authority generally has a good process for developing new information technology policies. Two groups are involved in developing policies. Policies are developed and recommended by a technical group consisting of information technology staff and a variety of Authority business officials. Draft policies are reviewed and approved by an executive group consisting of upper-level Authority directors and managers. The technical group has been very active in recommending security policies. We discovered, however, that there was a significant backlog of security policies waiting to be approved. As of August 2008, several policies covering important security areas such as responding to security incidents and protecting confidential information outside the office had been in draft form for over a year. Approval is important because the Authority doesn't begin using a policy until it's been approved.

The Authority relies too heavily on default policies without adequately making staff aware of them, and too many of its own policies are in draft form. To determine whether the Authority had developed sound policies to address important security issues, we identified 76 policy areas, and compared the Authority's policies in each area against best practices. The Authority had policies to address all but one of the areas we looked for. However, we identified several problems. First, the Authority relies on Information Technology Executive Council (ITEC) default policies for 23 of the 76 security areas, but hasn't formally adopted them or done enough to make staff aware of them. (The default security requirements are a compilation of minimum security requirements ITEC adopted for agencies to use when they don't have their own policies.) Second, the Authority has developed its own draft versions of 21 policies, but hasn't yet implemented them. Finally, three of the policies related to computer disposal, reviewing users' access to sensitive files, and password requirements, were inadequate in some respect, and the Authority had no policy requiring annual Health Insurance Portability and Accountability Act (HIPAA) training.

The Authority hasn't done an adequate job of promoting security awareness and disseminating policies to its staff. *Because many security risks hinge on users' behaviors, it's important for an agency to train its staff on security awareness and policies, and to periodically refresh that training. We found several problems in this area. While the Authority does train new staff, it doesn't provide systematic ongoing security awareness training, and it does a poor job of disseminating information about its security policies. Our security awareness survey showed that the Authority's staff had a lack of general security awareness and understanding of the agency's security policies. In addition, a consultant we hired was able to enter the Authority's offices, access confidential documents, and persuade some staff to divulge their passwords, all of which further illustrate the lack of security awareness among staff.*

Management doesn't monitor the implementation and effectiveness of the Authority's security system. *The Authority should conduct two types of security monitoring—technical monitoring to ensure the network remains protected, and managerial monitoring to ensure security policies and procedures are followed and are effective. DISC support staff have developed a very good set of procedures for technical monitoring of the network, including doing vulnerability scans, reviewing firewall and intrusion detection system logs, and reviewing user accounts. However, in terms of managerial monitoring the Authority's management appears to do very little to monitor security. They don't monitor the work done by the DISC support staff, and haven't yet done anything to see if Authority staff are complying with the Authority's policies, or to evaluate the effectiveness of those policies.*

The Authority's security-management activities don't feed into each other, creating a static system. *In a dynamic security-management system, the results of the activities feed into one another, making the system self correcting. We found there wasn't an adequate flow of information between any of the Authority's security activities. Policies don't flow from risk assessment, the Authority has done a poor job of disseminating the policies it has adopted, and management hasn't monitored whether policies are being followed or if they are effective.*

Question 1 Conclusion. *Although there are many good aspects to the Authority's security-management system, overall the system is disjointed and incomplete. The problem doesn't appear to be a lack of commitment to security on the part of Authority officials. Instead, officials don't appear to have sufficient knowledge of security and security management. Creating the Information Systems and Project Management Office and the information systems manager position was an important step in improving security, but unless the Authority is able to develop more expertise in security-management, it will be difficult to develop the kind of dynamic security-management system that's needed in today's rapidly changing environment.*

Question 1 Recommendations. *We recommended the Authority do the following:*

- *develop expertise in security-management best practices*
- *conduct an annual risk assessment involving Authority officials and DISC support staff that focuses on its unique risks, and use the results to help determine if new policies are needed*
- *improve the timeliness of the executive policy group's policy approval process*
- *formally adopt the ITEC Default Security Requirements for all security areas in which it hasn't developed its own policies, and make employees aware of those policies*
- *require employees to receive annual training on HIPAA, and improve the three policies we found deficient*
- *improve security awareness training for new employees and require annual follow-up training for all employees*
- *implement recommendations made by the consultant we hired in its report on social engineering*
- *monitor the effectiveness of the security policies and procedures and DISC support staffs' activities, and regularly consult with DISC support staff about the results of their monitoring activities*

Question 2: How Well Does the Authority Secure Its Information Technology Resources?

The Authority does a good job of securing its information technology resources, but some things should be improved. *We hired Fishnet Security, a well-known security consulting firm, to conduct extensive testing of the security of the Authority's network. Both the Authority's internal network and the data connection with its primary vendor, EDS, are very well secured. Fishnet was unable to hack into any of the Authority's servers or workstations, and we couldn't crack any passwords. We did identify one medium-risk issue having to do with the Authority's e-mail encryption system, and several low-risk issues. The Authority has resolved all these issues.*

We also looked to see if Authority staff had more access to the Medicaid Management Information System (MMIS) than they needed to do their jobs, but found few instances of excessive rights. However, the system that officials use to manage users' access rights to the System doesn't provide the kind of reports necessary for them to properly monitor those rights in the future.

Finally, the Authority didn't follow a systematic process in responding to the three security incidents it has had since its inception (some hard drives were stolen from storage, a CD containing confidential information was lost, and an e-mail was sent out with a Social Security number in it). We found that the Authority didn't follow a systematic process in responding to the incidents. As a result, management did a poor job of documenting the actions it took in response to the incidents, and didn't critically evaluate its responses to the incidents to determine if they were adequate or needed to change.

Question 2 Conclusion. *In general, the issues we found in this question had little to do with the current security of the Authority's information technology resources. Its network was secure, its employees' access rights generally seemed appropriate, and its response to security incidents, while incomplete, still addressed the most important issues—what caused the incidents and how can they be prevented in the future. However, as we've discussed throughout parts of this report, security can't remain static; it has to respond to a changing environment.*

The issues we found in this question had more to do with the lack of a systematic approach. For example, while employees' access rights seemed appropriate now, there's no system to ensure that they don't accumulate unnecessary access rights in the future. While the Authority's responses to security incidents weren't bad, the ad hoc nature of those responses caused them to be incomplete, and the lack of systematic procedures increases the risk that an incident may be mishandled in the future. Of the areas we looked at, only the technical security of the network appears to be supported by a systematic process. DISC support staff have developed a good set of regularly scheduled monitoring tasks that are spelled out in their procedure manual. As the network changes, their monitoring activities help them identify new vulnerabilities that need to be addressed. That systematic approach is one of the main reasons Fishnet was unable to penetrate the Authority's network. It's important that the Authority develops more systematic approaches to the other security issues in the future.

Question 2 Recommendations. *We recommended the Authority do the following:*

- *work with SRS to develop management reports that would allow supervisors to efficiently review their employees' access to the Medicaid Medical Information System on a periodic basis*
- *expedite the approval and implementation of its existing draft incident response policy*
- *take care to follow all elements of best practice in responding to future security incidents, including logging all actions its staff take in response to the incident, and conducting a follow-up evaluation of the effectiveness of its response*

These appendices can be found in the full report:

APPENDIX A: *Scope Statement*

APPENDIX B: *Agency Responses*

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. Our address is: Legislative Division of Post Audit, 800 SW Jackson Street, Suite 1200, Topeka, Kansas 66612. You also may call us at (785) 296-3792, or contact us via the Internet at LPA@lpa.state.ks.us.