# COMPUTER SECURITY AUDIT REPORT

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

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

08CC01

# *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**

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

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

**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
Barbara J. Hinton, Legislative Post Auditor

## 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 26, 2008

To: Members, Legislative Post Audit Committee

| | |
|---|---|
| Senator Derek Schmidt, Chair | Representative Virgil Peck Jr., Vice-Chair |
| Senator Les Donovan | Representative Tom Burroughs |
| Senator Anthony Hensley | Representative John Grange |
| Senator Nick Jordan | Representative Peggy Mast |
| Senator Chris Steineger | Representative Tom Sawyer |

This report 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.

Barbara J. Hinton
Legislative Post Auditor

# EXECUTIVE SUMMARY

LEGISLATIVE DIVISION OF POST AUDIT

## Overview of the Kansas Health Policy Authority



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

*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.*

..... page 8

**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.*

..... page 9

**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*

..... page 10

*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.*

..... page 14

**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 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*

..... page 18

*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.*



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.

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

This is part of a series of specialized compliance and control audits designed to focus on an important area of agency operations that generally hasn't been reviewed: the technical aspects of operating information systems. This audit focused on the management of information security at the Kansas Health Policy Authority.

The Kansas Health Policy Authority became a State agency on July 1, 2005. Its purpose was to develop and maintain a coordinated health policy agenda that combined effective purchasing and administration with health-promotion-oriented public health strategies. The legislation moved major health programs into the Authority such as Medicaid, the State Employees Health Plan, Medikan, and the State Children's Health Insurance Program (HealthWave). The Authority's fiscal year 2008 budget is $1.4 billion, with 235 full-time equivalent positions.

Over the last few years, concerns have been expressed about the lack of monitoring of State computer systems. 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.

These are positive developments that can result in increased efficiency and effectiveness and better service. However, significant risks are associated with these advances in technology that agencies should be addressing and managing. For example, in managing the State's major health insurance programs, the Kansas Health Policy Authority must handle and maintain confidential and highly sensitive information on thousands of Kansans.

This audit answers the following questions:

1. **How well does the Authority manage the security of its information systems?**

2. **How well does the Authority secure its information technology resources?**

To answer these questions, we reviewed information system standards and best practices, interviewed Authority officials, reviewed and

evaluated Authority policies, reviewed and tested various controls used by the Authority to secure its systems, and had in-depth technical assessments done of its network security. The more specialized technical assessments were done by Fishnet Security, an information technology security consulting firm.

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. Our findings begin on page 5, following a brief overview.

***The Health Policy Authority Was Created In 2005 to Better Coordinate Health Care Programs***

The Kansas Health Policy Authority was created by the 2005 Legislature and became a State agency on July 1, 2005. The enabling legislation shifted 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) into one agency—the Authority. The Authority's mission is to develop and maintain a coordinated health policy that combines effective purchasing and administration with health-promotion-oriented public health strategies.

As the State Medicaid agency, the Authority oversees two major contractors that process Medicaid data—MAXIMUS and EDS. MAXIMUS manages the eligibility process, while EDS processes all Medicaid claims through the Medicaid Management Information System (MMIS). In fulfilling their duties, both MAXIMUS and EDS handle a large amount of confidential client information, including all eligibility requests and Medicaid claims transactions.

## The Kansas Health Policy Authority
### AT A GLANCE

**Authority:** Created by K.S.A. 75-7401.

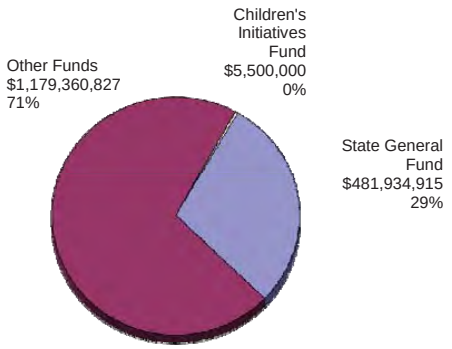
**Staffing:** In fiscal year 2007, the Authority had 215 full-time-equivalent positions.

**Budget:** The Authority receives only about 30% of its funding from the State General Fund. It gets most of its funding from "Other Funds," which is primarily federal Medicaid funds, federal State Children's Health Insurance Program funds, Hospital Provider Assessment funds, drug rebates, and funds recovered from estates. For fiscal year 2007, the Authority took in and spent nearly $1.7 billion. The majority of these expenditures are in the "Other Assistance" category which covers paying for health services for clients in programs such as Medicaid and HealthWave. The category of "Non-Expense Items" accounts for expenditures that would be duplicated in other agencies' budgets. The largest Authority non-expense items are transfers of Medicaid funds from the Authority to SRS, KDHE, Department on Aging, and the Juvenile Justice Authority.

**FY 2007 Expenditures**

| Type | Amount | % of Total |
|---|---|---|
| Other Assistance | $1,242,637,291 | 75% |
| Non-expense Items | $345,450,971 | 21% |
| Contractual Services | $67,206,254 | 4% |
| Salaries & Wages | $10,689,502 | 1% |
| Capital Outlay & Improvements | $248,139 | 0% |
| Commodities | $563,585 | 0% |
| **Total Expenses:** | **$1,666,795,742** | **100%** |

**Sources for Funding Those Expenditures**




**Total Funding:** **$1,666,795,742**

Source: *The Governor's Budget Report*, Vol. 2, FY 2009.

***The Authority Contracts With DISC To Handle The Technical Aspects Of Its Information Technology Network***

The Authority has a small information technology staff consisting of an information systems manager and four other staff who manage its telecommunications infrastructure, information security, and technology projects. They aren't technical staff, nor are they involved in the day-to-day aspects of running the Authority's network.

For technical support, the Authority contracts with the Department of Administration's Division of Information Systems and Communication (DISC). Under this contract, 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?

| | |
|---|---|
| ***ANSWER IN BRIEF:*** | *Although there are many good aspects to the Health Policy Authority's security-management system, some important aspects are missing from each of the major parts of the system. The Authority doesn't consider risks that are specific to the agency as part of its risk assessment. While the Authoritys generally has a good process for developing policies, the process could be improved by approving policies more quickly. In addition, the Authority relies too heavily on default policies without adequately making staff aware of them, and has too many draft policies awaiting approval. The Authority also hasn't done an adequate job of promoting security awareness and disseminating its policies, and management doesn't monitor the implementation and effectiveness of the security system. Finally, the Authority's security activities don't feed into each another, creating a static system. These and other findings are discussed in the sections that follow.* |

### *The Authority Lacks Important Pieces In Each of the Major Parts of Its Security-Management System*

In today's rapidly changing environment, effective computer security involves more than purchasing software and hardware and adopting some security policies. Rather, effective computer security comes from an on-going and dynamic security-management process that includes the following activities:

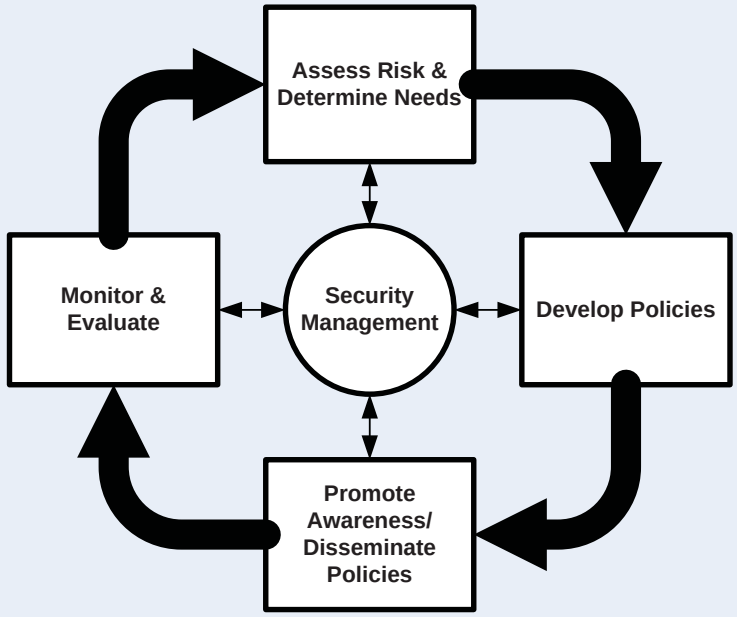
- risk assessment
- policy development
- policy dissemination
- monitoring and evaluation

Each security-management activity should feed into the next activity, creating a cycle of activities that helps ensure that security policies remain current, and that important risks are addressed. ***Figure 1-1*** on page 6 illustrates how the different activities should fit together. As staff go through the cycle, they receive feedback on how well the risks have been mitigated, and whether there are additional risks that should be addressed. Weaknesses in the system show up quickly.

To assess how well the Authority manages security, we compared its system to the model described above. Our findings are summarized in ***Figure 1-2*** on page 7.

As the figure shows, the Authority performs many good security activities covering each of the major categories of security management. These include developing security policies, completing a self-assessment of its security policies, and providing security-awareness training to newly hired employees. In addition, in 2007 the Authority created the Information Systems and Project Management

**Figure 1-1**
**Security-Management System**




Source: *Information Security Management: Learning from Leading Organizations,* GAO/AIMD-98-68, General Accounting Office, May 1998.

office with an information systems manager and four other positions to coordinate information technology issues within the agency—a much-needed step. One of the manager's responsibilities is to coordinate with the DISC support staff who handle the technical aspects of network security. DISC staff reported that since it appointed a contact person who's knowledgeable about information technology and security, the Authority has been much more open to their suggestions about security matters.

The figure also shows, however, that the Authority's system is missing several important security activities in each category, limiting the effectiveness of its security-management program. These issues are discussed in the following sections.

### *The Authority Doesn't Consider Risks That Are Specific to the Agency As Part of Its* ***Risk Assessment***

The purpose of a security-management system is to mitigate risks. For example, agencies install antivirus software and train staff to be careful with e-mail because there's a risk employees will open e-mail attachments that spread viruses. Unless officials understand the specific risks their agency faces, however, they have no way of knowing if the policies they've adopted actually will mitigate their most important risks, or if their agency remains vulnerable.

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. An effective risk assessment process should be a joint

**Figure 1-2**
**Comparing the Authority's Security-Management System To Best Practices**

| Positive Aspects of the Authority's System | Problem Areas We Found |
|---|---|
| ***RISK ASSESSMENT*** | |
| • 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.<br>• The information technology manager doesn't involve anyone else in the risk-assessment process. |
| ***POLICY DEVELOPMENT*** | |
| • The Authority's policy development group has been very active, developing and recommending new policies in a number of areas.<br>• The information technology manager appears to understand the need for good security policies.<br>• 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.<br>• The Authority relies heavily on the ITEC default policies but hasn't done enough to make staff aware of them<br>• Three of the Authority's policies were inadequate, and it had no policy in another area |
| ***POLICY DISSEMINATION/PROMOTING SECURITY AWARENESS*** | |
| • The Authority provides good security-awareness training to new employees<br>• 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.<br>• 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.<br>• 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.<br>• The Authority's staff showed a lack of security awareness and understanding of the agency's security policies in answering our security-awareness survey.<br>• The lack of security awareness among the staff allowed our consultant to access confidential documents and to get some employee passwords. |
| ***MONITORING AND EVALUATION*** | |
| • DISC support staff have developed a good process for monitoring the network. As a result, technical issues are well-monitored. | • The Authority management doesn't monitor:<br>➢ *work done by support staff*<br>➢ *compliance with policies*<br>➢ *effectiveness of policies* |
| ***FLOW BETWEEN AREAS*** | |
| | • The Authority's security policies don't flow from a complete risk assessment<br>• The Authority generally doesn't use content from its policies in training<br>• 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

effort between an agency's business officials and security officials to identify the following:

- the agency's critical information technology assets, such as critical databases, servers, and personnel.
- the agency's unique security risks, and the impact those security risks might have on specific business operations.
- the strategies or methods that can help mitigate specific business risks (these will be translated into policies in the policy development phase of the process)

This year, the Authority's Information Systems Manager began using a security self-assessment developed by the State's Information Technology Executive Council (ITEC) as the Authority's risk assessment. This security self-assessment is a checklist of security policies agencies complete annually to determine how well they have addressed basic areas of information technology security. It's a good tool for identifying an agency's generic security policy needs.

In reviewing the Authority's risk assessment process, we identified two significant problems:

- **The Authority hasn't taken steps needed to assess the agency's unique risks.** The security self-assessment is a useful part of a risk assessment. However, by relying on the security self-assessment alone the Authority hasn't identified the risks that are unique to the agency, or those that are the most important. For an agency like the Authority, these risks might include things like someone intercepting communications between the Authority and its Medicaid information vendor, or not being able to get the type of management information it needs to monitor employees' access to critical data. In addition, the Authority hasn't yet inventoried its critical information technology assets, including the hardware, applications, and data it uses to conduct its business.
- **The Information Systems Manager doesn't involve anyone else in the risk assessment process**. As a result, he isn't able to take advantage of the knowledge and expertise of either the DISC support staff who maintain the Authority's network, or any of the Authority's other business staff, who use the network.

### *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 them:

- **A technical group that drafts and recommends new policies.** The technical group includes a mix of Authority and DISC information technology staff, some officials from business units, the Authority's privacy officer, and a representative from the legal department.

- **An executive group that reviews and approves the policies.** The executive group includes the upper-level Authority directors and managers, such as the Executive Director and the Chief Finance Officer.

The technical group drafts policies and recommends them to the executive group. The group, chaired by the Information Systems Manager, has been very active, developing a number of policies that address important security areas. Essentially all the Authority's security policies have been developed since the Information Systems Manager started in early 2007.

While the Authority's system to develop policies conforms to best practice in many respects, we did find that there's a significant backlog of policies to be approved by the executive group. In conducting our review of the policy development process, we identified seven draft policies addressing many important security issues, such as policies on responding to security incidents and protecting confidential information outside the office. By August 2008, the executive group had approved two of these. However, three of the remaining four draft policies have been awaiting approval for more than a year. Approval is important, because the Authority doesn't begin using a policy until it's been approved by the executive group.

---

***The Authority Relies Too Heavily on Default Policies Without Adequately Making Staff Aware of Them, and Too Many Policies Are in Draft Form***

To determine whether the Authority had developed sound policies to address important security issues, we identified 76 areas covering such things as physical security, password controls, and data security, then 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, but we noted the following problems:

- **The Authority relies on ITEC default policies for 23 of the 76 security areas, but hasn't formally adopted them or made staff aware of them**. The Information Systems Manager told us the Authority relies on the policies in the ITEC default security requirements document for areas where it hasn't developed its own policies. (The default security requirements are a compilation of minimum security requirements developed by ITEC for agencies to use when they don't have their own policies.) The Authority relied on the default policies to some extent for important security areas, including risk assessment, contractor security, passwords, and firewall policies. While there's nothing wrong with using the default policies in key areas, the Authority has never formally adopted any of the default policies. More importantly, it hasn't done enough to inform its staff about them. If they don't know about the policies, they can't implement them.

- **The Authority has developed its own draft versions of 21 policies, but hasn't yet implemented them.** As discussed earlier, the Authority doesn't begin using its policies until they've been approved by its executive group.

- **Three of the policies are inadequate, and the Authority has no policy in another area.**

- The policy on computer disposal doesn't specify how many passes to securely eliminate Authority data from a hard drive
- The policy on reviewing users' access to sensitive files fails to require that it be done annually
- The password policies don't require passwords to be as strong as we think they should be given the amount of sensitive information handled by Authority users
- The Authority doesn't have a policy requiring annual training on the federal Health Insurance Portability and Accountability Act (HIPAA)

***The Authority Hasn't Done an Adequate Job Of Promoting Security Awareness and Disseminating Policies***

In today's security environment, everyone has an important role in security—many risks can't be mitigated with software or computer settings and instead hinge on users' behaviors. The strongest system of network security easily can be bypassed by a "helpful" employee who shares his or her password, or by inattentive employees who open e-mail attachments they shouldn't. Unfortunately, hackers have become very adept at manipulating users' behaviors. Because security isn't most users' main responsibility, and because following policies can be inconvenient and often goes against people's natural behaviors, it's important for an agency to train its staff on security awareness and policies, and to periodically refresh that training.

**The Authority doesn't provide systematic ongoing security-awareness training, and does a poor job of disseminating information about its security policies.** Although the Authority provides good security-awareness training to new employees, it doesn't conduct the systematic ongoing training called for in its policies. As a result, most employees are trained on security awareness only once. Many employees transferred in from the Department of Social and Rehabilitation Services (SRS) when the Authority was created in 2005. Because these employees had been trained at SRS, they were grandfathered in and weren't required to redo the training. As a result, many employees haven't been formally trained on security awareness since 2005.

The Authority also does an inadequate job of making sure its staff are aware of and understand its security policies. Although the Authority publishes all its security policies on its intranet site and has discussed policies at a staff meeting, as noted earlier, its staff missed a large number of questions about those policies on our survey. That's because publishing the policies without taking additional steps to make people aware of them isn't sufficient.

For example, the DISC support staff who administer the Authority's network told us they usually don't know when new policies are approved. As a result, we identified two network settings relating to

passwords that weren't set properly because the DISC staff weren't aware of the policies.

**The Authority's staff showed a lack of general security awareness and understanding of the agency's security policies.** To measure employees' security awareness and knowledge of policies, we developed a security-awareness survey and sent it to Authority staff. Of the 298 staff we sent the survey to, 166 (56%) replied. Here are the results:

- **Staff correctly answered 83% of the questions on general security awareness**. These questions covered such things as e-mail attachments, spyware, and physical security.
- **Staff correctly answered 71% of the questions on the Authority's specific security policies.** These questions covered such things as identifying and storing confidential data, backing up data on their computers, and sharing passwords.

Because this is the first time we've administered such a survey, we don't have any other results to use as a comparison. However, given the large amount of confidential medical data the Authority handles, we expected better results. The especially large number of incorrect responses (29%) on the policy questions illustrates the Authority's weakness in making people aware of its policies.

**The lack of security awareness among the Authority's staff allowed a consultant we hired to access confidential documents and to get some staff to divulge their passwords.**
We contracted with Fishnet Security, an information systems security consulting firm, to conduct some very technical security tests of the Authority's network, which are discussed in more detail in Question 2. In addition, we had Fishnet assess the level of security awareness among the Authority's staff by attempting to gain access to the agency's offices, and by trying to get staff to divulge their passwords over the phone or by e-mail.

Among other things, the Fishnet consultant was able to:

- enter KHPA's locked offices in the Landon State Office Building and roam around the offices unchallenged
- remove confidential documents from file cabinets and bookcases and take them to a conference room to photograph
- convince some of the Authority's staff to give him their passwords over the phone

The consultant concluded that the Authority's "friendly employee culture," lack of security awareness among staff, and lack of physical access controls were what allowed him such widespread access. His findings are described in more detail in the profile on the next page.

**KHPA Staff's Lack of Security Awareness Allowed a Consultant To Access Confidential Documents and Trick Users Into Divulging Their Passwords**

In an attempt to get a more realistic measure of the level of Authority staff security awareness, we hired Fishnet to attempt to "social engineer" KHPA staff. Social engineering is a term for attempting to fool someone into doing something they shouldn't. Hackers frequently use these techniques to talk someone into allowing them into a locked office, or into giving them passwords or other information they can use to break into a network.

With the Authority management's knowledge, we asked a consultant to try to gain access to Authority offices in the Mills Building and the Landon Office Building, and to use e-mail and phone calls to try to get users' passwords. At various times the Fishnet consultant impersonated an auditor from Post Audit (using a very realistic forged business card), the Authority's Information Systems Manager, and a DISC support staff person. The following are the results of his efforts:

**E-mail/Phone Tests**
Fishnet set up a free e-mail account with an address similar to the Information Systems Manager's name and mailed e-mail to 30 staff members whose addresses he obtained from the agency web site and Department of Administration communication directory. His claim was that he was working for DISC and needed their passwords to install security software on their computers. In all, 14 employees failed to notice that the e-mail wasn't an agency e-mail and answered the e-mail. He followed up the e-mails with a phone call to the same employees. One provided a password over the phone. Two others weren't willing to give their passwords over the phone, but agreed to write them down and leave it under their keyboard for him.

He didn't reach all the staff on the first day, so he called the rest a few days later. By that time the employees had heard that someone was trying to get passwords, and most refused to provide any information to him. Even so, one employee was willing to give him some of his other identifying information, but not his password.

**Surveillance**
The consultant was able to take advantage of publicly accessible areas within and around the Authority facilities to determine useful information, such as how employee identification badges were designed, how access systems worked, the habits of service vendors, and cleaning crew hours of operation. He used the Internet to gather further information, such as agency phone numbers, lines of business, and personnel information. At Kinko's he created a forged LPA business card, and decided to try to use his Fishnet identification badge instead of forging an Authority one even though they didn't look much alike.

**Physical Access**
The consultant entered the Authority offices in the Landon Building through a door that was propped open and freely roamed the offices. He was able to plug his computer into a network jack in an empty cubicle. He also located an unsecured wireless access point, connected wirelessly, and sent e-mail to us. (We later tracked down the wireless access point in another agency's offices in the Landon Building, and had them turn it off.) Using an Authority conference room as a staging area, he pulled files from various file cabinets and bookshelves and took them to the conference room to review. (He provided photographs of various documents such as those shown on the following page.) He also roamed the offices checking to see if he could access Authority computers. All were either powered off or locked. No one questioned his identity.

## *Management Doesn't Monitor the Implementation and Effectiveness of the Authority's Security System*

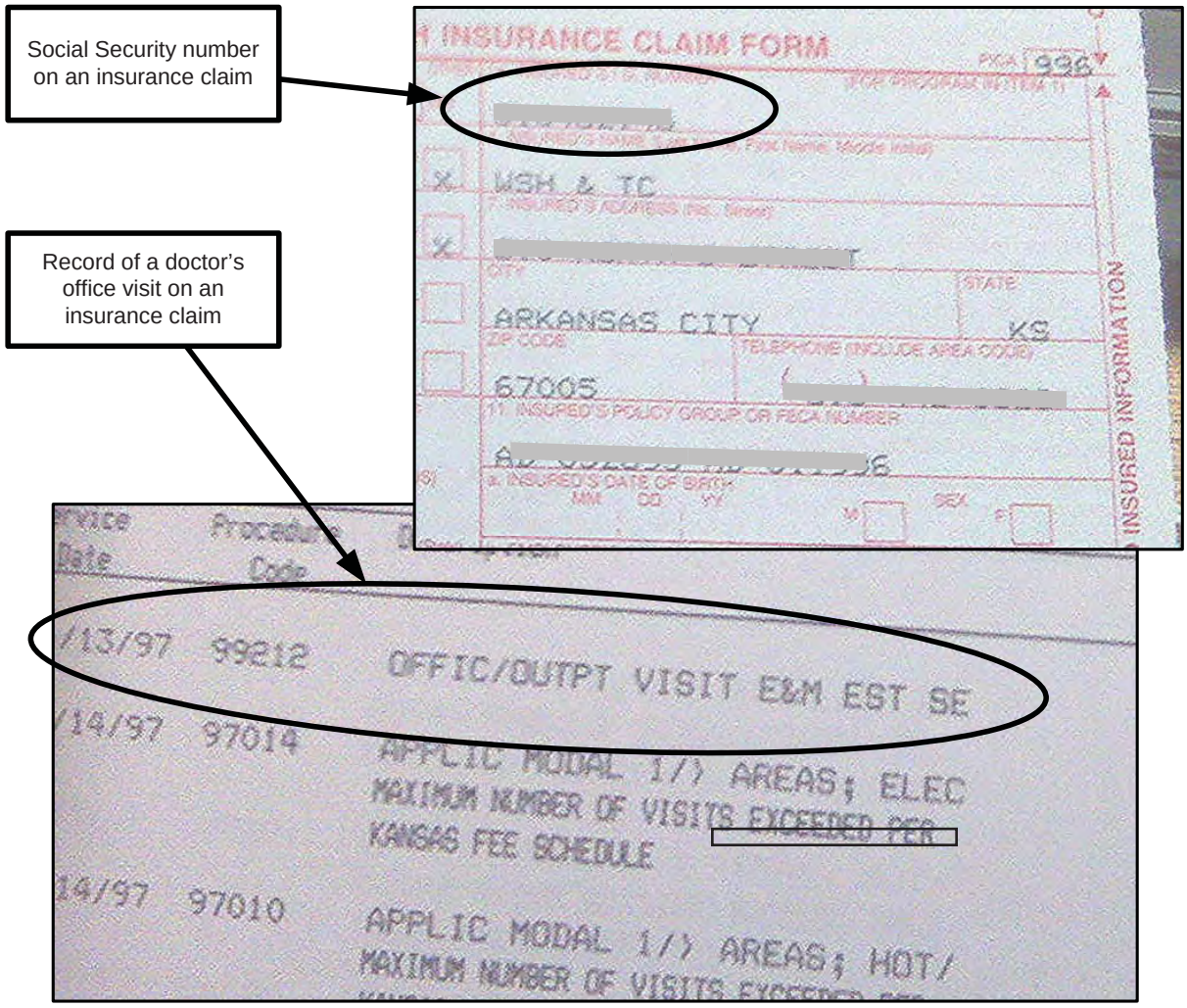
Monitoring is an important aspect of security management, and should occur at two levels:

- **technical monitoring**—ensuring that the network remains protected and identifying attempts to attack it
- **managerial monitoring**—ensuring that policies and procedures are being followed and that they are effective

As described in the Overview, the Authority contracts with DISC to handle all the technical aspects of its network. DISC support

The consultant wasn't able to gain access to the offices in the Mills Building, but described a method he could have used to access the offices after hours. He was able to steal some of the Authority's trash from the elevator while the cleaning crew was working. He then found an office under construction on another floor, and used it to go through the trash bags looking for sensitive information.

**Dumpster Diving** (finding information in the trash)
He was able to go through Authority trash bags looking for sensitive documents. He didn't find any sensitive information, but told us he did find contact information that could have been useful in further attacks.




staff have developed a very good set of policies and procedures for monitoring the network. Their procedures specify a number of monitoring activities that are to be carried out daily, weekly, and monthly. They include such activities as vulnerability scans of the network, reviewing firewall and intrusion detection system logs, and reviewing user accounts. In Question 2 we looked at the overall security of the network and found the DISC staff had done a very good job of keeping it secured.

In terms of managerial monitoring, however, we found that the Authority's management appeared to do very little to monitor security. Management doesn't monitor the work done by the DISC support staff, and hasn'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 Information Systems Manager told us he'd like to do more to monitor DISC's work, but he didn't think his staff had the expertise to do so.

---

***The Authority's Security-Management Activities Don't Feed Into Each Other, Creating a Static System***

As discussed earlier, a security-management system should be a dynamic process with the results of one activity flowing into the next. That flow is what makes the model self-correcting—the results of one activity feed into another. For example, if security officials conducted periodic monitoring of policy compliance and discovered that a significant number of employees were sharing their passwords with other employees in violation of policy, it would indicate that a policy wasn't working as intended. In response, officials could modify the policy to make it stronger, and conduct additional training to make sure people understood the risks of continuing to share passwords. With a static system, however, it might be a long time before anyone noticed the problem.

We looked at the Authority's security-management system to determine the extent to which activities flowed into each other. We found that there wasn't an adequate flow of information between any of the Authorities security activities. As described earlier, the largest problems were:

- The Authority's security policies don't flow from a complete risk assessment.
- The Authority has done a poor job of disseminating the policies it has adopted, and generally doesn't use content from policies in training.
- Management hasn't monitored whether policies are being followed or if they are effective, and doesn't use the results of the monitoring DISC does in assessing risks.

***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.

***Recommendations For Executive Action:***

1. To help develop a more dynamic security-management program, the Authority should develop expertise in security management best practices within its information technology staff. The possible options for developing that expertise include:

   a. hiring a security expert from outside the Authority.

   b. obtaining outside training for a member of the current information technology staff.

   c. consulting with DISC officials who are knowledgeable about security management.

2. To help ensure it's able to identify and address its most significant security risks, the Authority should conduct an annual risk assessment that:

   a. involves a range of information technology and business officials, the Authority's privacy officer, and DISC support staff.

   b. focuses on the agency's unique security risks.

   c. includes an inventory of the Authority's critical information technology assets.

   d. incorporates the results of security monitoring conducted by Authority officials and DISC support staff.

3. To help ensure the policy development process results in effective information security policies that are developed and approved in a timely manner:

   a. the technical policy group should use the results of the annual risk assessment to develop new policies or adjust existing policies to mitigate the agency's most significant security risks.

   b. the executive policy group should move quickly to review and approve all the remaining draft information security policies currently awaiting approval. The executive group also should examine ways to improve the timeliness of its policy approval process.

4. To address the issues we identified with its current security policies, the Authority should:

    a. formally adopt the ITEC Default Security Requirements for all security areas in which it hasn't developed its own policies, and ensure the appropriate employees are aware of the default policies.

    b. develop a policy requiring employees receive annual training on the federal Health Insurance Portability and Accountability Act (HIPAA).

    c. Make the following modifications to its current policies:

        i. add a requirement to its policy on disposing computers for three overwrite passes to securely remove data from the hard drives.

        ii. add a requirement to its policy on managing users' access to sensitive files that the required review of access rights be conducted annually.

        iii. strengthen its password policies by requiring more complex passwords.

5. To help ensure its employees have a sufficient understanding of general security issues as well as the specific security policies that apply to them, the Authority should:

    a. Develop a systematic, multi-layered approach to security awareness and policy training that:

        i. expands the current training for new employees including topics that address the Authority's security policies.

        ii. requires annual follow-up training on security awareness and policies.

        iii. includes ad-hoc training as needed to address other security issues that arise.

    b. Implement the following recommendations made by Fishnet in its report on social engineering. Those recommendations broadly cover the following areas:

        i. improving the general security awareness of Authority staff.

        ii. enhancing the physical controls at the Authority's offices.

        iii. removing information that could assist a hacker from the Authority's website.

6. To better monitor the effectiveness of its security policies and procedures, the Authority should:

   a. periodically evaluate staff's compliance with security policies and the effectiveness of those policies.

   b. conduct regular monitoring of DISC support staffs' activities.

   c. regularly consult with DISC support staff to learn the results of their monitoring activities, and to get their feedback on the effectiveness of the Authority's policies and procedures.

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

| | |
|---|---|
| ***ANSWER IN BRIEF:*** | *Overall, the Authority does a good job of securing its IT resources, but we found some things that should be improved. Based on our reviews and on more technical work done by a consultant, we found that both the internal network and the data connection to the Authority's primary vendor are very well secured. We found very few vulnerabilities with the network, and all but one have been fixed. On the other hand, the system the Authority uses to manage employee access to Medicaid data doesn't provide the kind of reports necessary to properly monitor that access. Finally, the Authority didn't use a systematic process in responding to its security incidents, primarily because it lacked a formal incident response policy or procedure. These and other findings are discussed in the sections that follow.* |

### *The Authority Does a Good Job of Securing Its Information Technology Resources, But Some Things Should Be Improved*

To answer this question, we chose to focus on three critical areas:

- the security of the Authority's network
- how well the Authority manages its employees' access to Medicaid Medical Information System (MMIS) data
- management's responses to security incidents

**Both the Authority's internal network and the data connection with its primary vendor are very well secured.** Along with looking at the security of the network itself, we also were concerned about the level of protection of the data that come in and out of the Authority's network. In examining the network, we looked at five high-risk areas:

- the firewalls that protect the Authority's network from outside attack
- the data connection between the Authority and EDS, the contractor that handles Medicaid claims
- outgoing e-mail that could contain confidential medical information
- user passwords that control access to the network
- the Authority's internal network, including servers, workstations, and printers

Some of the work we wanted to do was highly technical and required specialized skills that we lacked. We hired Fishnet Security, a well-known security consulting firm, to do extensive testing of the security of the network. Fishnet reviewed the settings for the firewalls and the data connection between the Authority and EDS. It also conducted a vulnerability assessment of the Authority's network, and attempted to use the information from the assessment to penetrate the network. Fishnet was allowed to exploit any vulnerability it found in order to hack into a server or a workstation, but was prohibited

from attempting any denial-of-service attacks (these tests use a flood of data to shut down a service, server, or network, and can cause as much harm as an actual attack by a hacker). All testing was done with the knowledge and cooperation of the Authority's management.

The major findings of the tests are summarized in ***Figure 2-1*** on page 20. As the figure shows, the review and testing of the Authority's network revealed very few issues, and all but one of the problems we found were very minor and all have since been fixed.

The one medium-level risk we identified involved the "lexicon" feature of the Authority's e-mail encryption system. The lexicon feature checks outbound e-mail for medical terms in order to prevent confidential patient data from leaving the agency. Because some officials had innocuous e-mails such as press releases blocked by the lexicon feature, the Authority turned off the feature for everybody. Because the lexicon offers valuable protections, it would have been much more prudent for the Authority to selectively disable the feature only for employees who don't deal with confidential information, rather than turning it off for everybody.

In addition to the problem with the lexicon feature of the Authority's e-mail system, there were a handful of other minor issues with the Authority's network:

- Some of the routers that are part of the Authority's data connection with EDS were set to be visible outside the network. Although the routers were password protected, being visible removed a layer of security and could have made them easier to hack.
- There were issues with a couple of password settings:
  - *The minimum password age was set at zero days (best practice is one day). Zero days allows users to repeatedly change their passwords until the system allows them to go back to their original password, circumventing a different control that limits users' ability to reuse a particular password.*
  - *The system was set to lock a user out after 10 failed login attempts (best practice is three attempts). The lower the setting, the more difficult it is for a hacker to guess a user's password. In addition, the lock-out time was set differently than the policy called for.*
- There were some very minor issues with the internal network configuration. There was a weak level of encryption enabled on some servers. One workstation had insecure software installed and some printers had insecure services enabled—all of which could make these resources vulnerable to a denial-of-service attack.

Overall, the network was very well secured. Fishnet was unable to hack into any of the Authority's servers or workstations, and we couldn't crack any passwords (after letting the software run for six days, we quit trying). In comparison, in our 2003 audit of the Kansas

**Figure 2-1**
**Summarizing the Results of the Network Security Reviews**

| | Area of the Authority's Network That Was Evaluated | | | | |
|---|---|---|---|---|---|
| | *External Firewalls* | *Data Connection With EDS* | *E-mail Encryption System* | *Network Passwords* | *Internal Network Configuration* |
| What was done to evaluate this part of the network? | • Fishnet reviewed firewall settings<br>• Fishnet attempted to penetrate the network from outside | • Fishnet reviewed the connection settings<br>• *No direct testing was done* | • LPA reviewed which features were enabled and how the system was configured<br>• *No direct testing was done of the encryption system* | • LPA reviewed the password settings<br>• LPA attempted to crack staff's passwords | • Fishnet used security software scan the network for vulnerabilities<br>• Fishnet attempted to hack into several servers and workstations |
| What vulnerabilities were found? | *none* | • Some routers were visible to computers outside the Authority's network. | • A feature that protects confidential patient data by checking all outgoing e-mail for medical terms was disabled. | • There were issues with three password settings:<br>➢ *minimum password age was too low*<br>➢ *number of failed log-in attempts before a lock out was too high*<br>➢ *lock-out time differed from Authority policy* | • There were three minor vulnerabilities:<br>➢ *insecure software on one computer*<br>➢ *weak level of encryption enabled on some servers*<br>➢ *an insecure service, was enabled on some printers* |
| What's the risk level for these problems? | n/a | Low | **Medium** | Low | Low |
| Has the vulnerability been addressed? | n/a | Yes | Yes | Yes | Yes |
| What's the current level of security for this part of the network? | High | High | High | High | High |

Source: Fishnet Security reports, 5/9/08 and 6/17/08; and LPA review of e-mail encryption system and network password controls

Department of Health and Environment, we were able to crack 60% of the Department's passwords within three minutes, and 90% within 11 hours.

Fishnet gave the Authority good reviews for its network security, saying that its firewall was "a good example of a secure and functional firewall solution," and rating the Authority's security profile as "above average" compared to similar organizations.

**The system the Authority uses to manage access rights to the Medicaid Management Information System (MMIS) doesn't provide the kind of reports needed to properly monitor those rights.** An important security principal is to give employees the least amount of access to sensitive data that they need in order to do their jobs. A common problem organizations experience is that employees tend to "accumulate" access to more and more systems over time as their responsibilities change within the organization. Therefore, it's important for security managers to have supervisors review their employees' access rights at least annually to make sure they're still needed.

We observed that while the system the Authority uses is good for managing access rights one employee at a time, it can't generate a summary report that shows all the employees (and their access rights) who work for a particular supervisor. Without such a report, it would be very difficult for a supervisor to do an annual review. When we checked to see whether Authority employees had indeed collected excessive access to MMIS data, we found relatively few problems. This is likely because the Authority is a new agency, and employees haven't had a lot of time to accumulate access rights.

In addition to reviewing employees' access rights, we checked to make sure the Authority was properly disabling or eliminating the network accounts for former employees. We reviewed the accounts for all employees who'd left the Authority in the last year, and found that all were properly disabled.

**The Authority didn't follow a systematic process in responding to its three security incidents.** In general, "security incidents" happen any time sensitive data are lost or disclosed, an unauthorized person gains access to the network or facilities, legitimate access to systems is lost, or an employee unacceptably uses the Authority's computers. The Authority has had three security incidents since its inception:

- the hard drives and memory were stolen from a number of old computers in a storage room in the basement of the Landon State Office building
- a CD with Medicaid information was delivered to the Authority's main office, but was lost before it reached the analyst it was intended for

- an e-mail containing a nurse's Social Security number was sent to a vendor

We compared how the Authority responded to each these incidents to best practices in these areas. For incidents such as these, we would have expected management to do the following:

- conduct a thorough investigation to determine the nature, cause, and impact of the incident
- keep a good record of all actions its staff takes
- analyze the effectiveness of its response to the incident
- change policies and procedures to prevent similar incidents or to improve its response

The Authority appeared to have conducted thorough investigations of all three incidents, and we thought they did a good job of developing policies to prevent similar incidents in the future. However, we did find two problems with the Authority's response to each incident:

- **Management did a poor job of documenting the actions it took in response to any of the three incidents.** Documenting the actions taken in response to an incident is important for several reasons:
  - *to avoid people working at cross purposes during the incident response*
  - *to aid in a forensics investigation if such an investigation becomes necessary*
  - *to assist in evaluating management's response to the incident*
- **Management didn't critically evaluate its responses to the incidents to determine if they were adequate or needed to change.** Because security incidents don't occur very often in a well-protected system, and because a quick and effective response is essential to protecting an agency's data, it is very important that management evaluate the agency's response to each incident to see if the procedures need to be improved.

The main reason for the problems we found was the absence of an incident response policy or procedure to follow. As a result, the Authority responded to each incident in a very ad-hoc manner. The Authority has since developed a draft incident response policy, but that policy hasn't been approved by management. As noted in Question 1, draft policies don't go into effect until after they are approved. It's also important to note that two of the three incidents occurred before the current Information Systems Manager position was created, so there was no one with the responsibility to coordinate and manage the agency's response to those incidents.

| | |
|---|---|
| ***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.<br><br>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. |

| | |
|---|---|
| ***Recommendations For Executive Action:*** | 1. To help ensure that employees' access to the Medicaid Medical Information System is limited to what they need to perform their job duties, the Authority should work with the Department of Social and Rehabilitation Services to develop management reports that would allow supervisors to efficiently review their employees' access rights on a periodic basis.<br><br>2. To help ensure that it responds effectively to security incidents, the Authority should expedite the approval and implementation of its existing draft incident response policy. In responding to future incidents, the Authority should take care to follow all elements of best practice, including logging all actions its staff take in response to the incident, and conducting a follow-up evaluation of the effectiveness of its response. |

## APPENDIX A

### Scope Statement

This appendix contains the scope statement for this audit of the Kansas Health Policy Authority. 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 the Kansas Health Policy Authority's Management of Those Systems

The Kansas Health Policy Authority was created by the 2005 Legislature, and became a State agency on July 1, 2005. Its purpose was to develop and maintain a coordinated health policy agenda that combined effective purchasing and administration with health-promotion-oriented public health strategies. The legislation moved major health programs into the Authority such as Medicaid, the State Employees Health Plan, Medikan, and the State Children's Health Insurance Program (HealthWave). The Authority's fiscal year 2008 budget is $1.4 billion, with 235 full-time equivalent positions.

During the last few years, concerns have been expressed about the lack of monitoring of State computer systems. 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.

These are positive developments that can result in increased efficiency and effectiveness and better service. However, significant risks are associated with these advances in technology that agencies should be addressing and managing. For example, in managing the State's major health insurance programs, the Authority must handle and maintain confidential and highly sensitive information on thousands of Kansans. 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 audit looks at the Authority and will address the following questions:

1. **How well does the Authority manage the security of its information systems?** To answer this question, we will review the Authority's system of managing its information system security, with an emphasis on how the security function is structured and managed, and on security policies and procedures.

2. **How well does the Authority secure its information technology resources?** We will work in conjunction with Fishnet Security in answering this question. (Fishnet is a Kansas City, Missouri based corporation specializing in information technology security.) Fishnet will conduct a detailed security vulnerability assessment of the Authority's systems. If Fishnet identifies significant vulnerabilities, we will attempt to determine what security management weaknesses allowed those vulnerabilities to exist.

**Estimated time to Complete: 20-24 weeks.**

## APPENDIX B

### Agency Responses

On August 11, 2008, we provided copies of the draft audit report to the Kansas Health Policy Authority, and to the Division of Information Systems and Communication (DISC). The Authority's response is included as this Appendix. Because there were no recommendations for DISC, it chose not to submit a response. The Authority generally concurred with the report's findings, conclusions, and recommendations.

*Coordinating health & health care for a thriving Kansas*

KHPA™

KANSAS HEALTH POLICY AUTHORITY


August 18, 2008

Ms. Barbara J. Hinton
Legislative Post Auditor
800 SW Jackson Street, Suite 1200
Topeka, KS 66612-2212

Dear Ms. Hinton:

Thank you for the opportunity to respond to the audit *State Agency Information Systems: Reviewing the Kansas Health Policy Authority's Management of Those Systems*. My staff have reviewed the recommendations included in the audit and will begin implementing those directly under our control.

As the report notes, the Kansas Health Policy Authority (KHPA) created its own network environment in December 2007. At our inception as an agency, KHPA staff used computer networks managed by the Department of Administration and the Department of Social and Rehabilitation Services. Rather than continue to rely on other agencies for the customer support, network configuration, and security protocols, we decided to build our own network architecture to unify the operational elements that make up KHPA: the Medicaid and State Children's Health Insurance Programs and the State Employees Health Benefits Plan.

KHPA identified an information technology manager and other information security staff to oversee the KHPA network infrastructure. We also negotiated an agreement with the Division of Information Systems and Communications (DISC) to provide network, server, desktop computer, and customer service support to KHPA. This structure has allowed KHPA to grow rapidly, adding server capacity and computers for new positions, while maintaining connectivity to critical existing systems like the Worker's Compensation document management and payment systems, the Medicaid Management Information System, and the State Employee's Health Plan eligibility system.

Building our own network required KHPA to create policies and procedures to protect the information we store and work with on a daily basis. The audit describes our policy development process and improvements that could be made in the timeliness of approving policies, explicit adoption of default policies from the Information Technology Executive Council (ITEC), and staff training. We have begun to implement these recommendations as part of an expanded new employee orientation and required training program for all staff. KHPA is very aware of the sensitive information we have and use to purchase health care for 360,000 Kansans. The survey responses described in the

Rm. 900-N, Landon Building, 900 SW Jackson Street, Topeka, KS 66612-1220
www.khpa.ks.gov

Medicaid and HealthWave:
Phone: 785-296-3981
Fax: 785-296-4813

State Employee Health Benefits and Plan Purchasing:
Phone: 785-368-6361
Fax: 785-368-7180

State Self Insurance Fund:
Phone: 785-296-2364
Fax: 785-296-6995

audit demonstrates the success of our initial efforts at training new employees and maintaining consistency among the existing staff.

Finally, I would like to recognize the work of our DISC support team. Through our service level agreement, DISC manages our network environment, handles customer support, hardware and software set up, and many other vital elements of our computing infrastructure. They have been involved in our policy development process and have identified vulnerabilities that prevented issues that would have crippled our ability to serve our customers. The glowing report from the Fishnet vulnerability assessment on our network security, including firewalls, data connections, and network configurations, is due to the knowledge and expertise our DISC partners bring to our information technology platform. DISC staff and management have been a tremendous support to KHPA and we appreciate their diligence.

As for the specific recommendations in the audit, KHPA will implement all six of the recommendations in question 1 of the audit report. Within current resources, KHPA will identify additional training for KHPA information technology staff on security management and work to incorporate an annual risk assessment in the state's mandated 3 year information technology planning process. The suggested policy changes and training in recommendations 4 and 5 are being developed now. There also are planned audits of staff compliance with security policies and oversight of DISC activities. The recommendations in question 2 also will be addressed through additional reports on MMIS access and implementation of the incident response policy developed by KHPA.

We appreciate the effort of Allan Foster and the Fishnet Security in conducting the audit. They offered good suggestions and were a pleasure to work with. Thank you for the opportunity to respond to the draft audit report.

Sincerely,

Dr. Marcia Nielsen
Executive Director