PERFORMANCE AUDIT REPORT

State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2012)

A Report to the Legislative Post Audit Committee
By the Legislative Division of Post Audit
State of Kansas
December 2012

R-12-012

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 $14 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 ten members, the two majority caucuses each have three members, while the two minority caucuses each have two members.

Audits are performed at the direction of the Legislative Post Audit Committee. Legislators or committees should make their requests for performance audits through the chair 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 Mary Pilcher-Cook, Chair
Senator Terry Bruce
Senator Anthony Hensley
Senator Laura Kelly
Senator Dwayne Umbarger

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

LEGISLATIVE DIVISION OF POST AUDIT

800 SW Jackson
Suite 1200
Topeka, Kansas 66612-2212
Telephone (785) 296-3792
FAX (785) 296-4482
Website: **http://www.kslpa.org**
Scott Frank, Legislative Post Auditor

HOW DO I GET AN AUDIT APPROVED?

By law, individual legislators, legislative committees, or the Governor may request an audit, but any audit work conducted by the division must be directed by the Legislative Post Audit Committee, the 10-member joint committee that oversees the Division's work. Any legislator who would like to request an audit should contact the division directly at (785) 296-3792.

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
WWW.KSLPA.ORG

December 6, 2012

To: Members, Legislative Post Audit Committee

Senator Mary Pilcher-Cook, Chair
Senator Terry Bruce
Senator Anthony Hensley
Senator Laura Kelly
Senator Dwayne Umbarger

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

This report contains the findings, conclusions, and recommendations from our completed performance audit, *State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY2012)*. We would be happy to discuss the findings, recommendations, or any other items presented in this report with any legislative committees, individual legislators, or other State officials.

Sincerely,

Scott Frank
Legislative Post Auditor

This audit was conducted by Dan Bryan, Nathan Ensz, and Stan Wiechert. Justin Stowe was the audit manager. If you need any additional information about the audit's findings, please contact Dan Bryan at the Division's offices.

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

(785) 296-3792
Website: www.kslpa.org

Table of Contents

Do Selected State Agencies Have Adequate IT Security Controls to Help Ensure that Confidential Information is Protected?

List of Figures

List of Appendices

State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2012)

Each year, state agencies collect and process sensitive and confidential data in their computer systems including citizen Social Security numbers, medical information, and income data. Some agencies are responsible for protecting millions of confidential records, which makes them a potentially enticing target for hackers.

Currently, there is limited oversight of agencies' security controls to ensure that agencies are adequately protecting confidential data. The Kansas Information Technology Executive Council (ITEC) has developed guidance to assist state agencies in developing adequate security controls, but ITEC does not monitor or audit how well those controls are implemented. Consequently, agencies have a significant amount of autonomy in how they develop, apply, and monitor security controls.

The Legislative Post Audit Committee approved information system audits as an adjunct to the division's compliance and control audits. This information system audit looks at seven important information technology (IT) security areas across a broad selection of state agencies.

This information security audit answers the following question:

Do selected state agencies have adequate IT security controls to help ensure that confidential information is protected?

A copy of the scope statement for this audit approved by the Legislative Post Audit Committee is included in ***Appendix A.*** For reporting purpose, we've collapsed the seven questions listed in the scope statement into one.

To answer this question, we evaluated the IT security management process and several security controls used by nine state agencies to protect confidential information. For each security control, we reviewed agencies' policies and procedures and compared them to state IT requirements and best practices. We also performed several technical tests of agency controls including vulnerability scans and attempts to crack staff passwords. Finally, we interviewed agency officials and staff to determine how well policies and procedures were being followed in practice, and surveyed agency staff to determine their knowledge of IT policies and procedures. The Enterprise Security Office within the Department of Administration assisted us with some of our technical work.

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 the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This audit report provides a summary of our findings across all nine agencies, but does not describe the security findings for individual agencies. Because those specific findings contain information that would jeopardize the agencies' security, we are keeping those findings confidential under K.S.A. 45-221(12). We provided each agency with a separate, confidential report to address any agency specific problems we identified through our work.

Our findings begin on page 7, following a brief overview.

State Agencies' Confidential Information Could Be Breached from Outside or Within an Agency

State agencies collect and maintain increasingly large volumes of information related to a variety of services and programs. Much of that information is sensitive or confidential, and to protect it, safeguards must be put in place to prevent unauthorized access from both outside or within the agency.

Hackers attempt to gain unauthorized access to confidential data from outside an agency in two ways. Both methods represent a potential threat to the security of confidential information, as described below.

- **In some cases, hackers may target a specific agency because of the confidential information it maintains.** Some state agencies make enticing targets because hackers know that those agencies maintain large amounts of confidential information such as credit card information, social security numbers, and tax data. The street value of this information varies widely, but can be lucrative. For example, identifying information such as an individual's name and social security number can be worth up to $25 per record.
- **More frequently, hackers use broad attacks against numerous networks and sort out the information they are able to collect afterwards.** Instead of targeting a specific agency, a hacker could look for vulnerabilities across a wide range of computer systems that could easily be exploited to gain access For example, a hacker might use automated software to find an active server and then try hacking into the server using default user names or common passwords. Once access is gained, the hacker typically collects all possible information and reviews it retroactively to determine if it has any value.

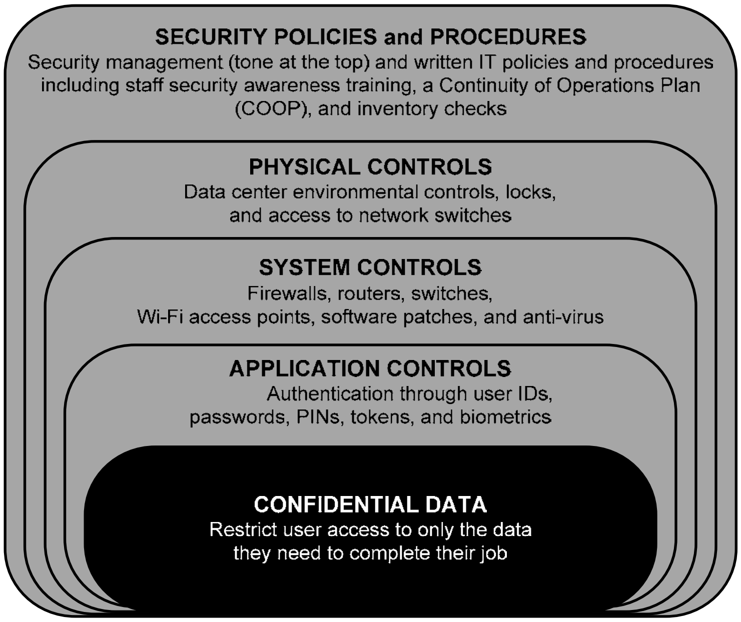
Confidential data could also be intentionally or inadvertently breached from within an agency. Although many IT security controls are intended to prevent network access from outside an agency, some are also designed to help limit employees' unauthorized access to confidential information. Specifically, they help protect confidential data from theft and help ensure that only authorized staff can view it. For example, settings that automatically lock idle computers can help prevent other users from using that computer to access restricted information.

Agencies Must Protect Confidential Information Through Multiple Layers of IT Security

A primary purpose of IT security controls is to help ensure that confidential and personal information is not stolen or lost. To accomplish this, agencies should use multiple layers of security.

Each layer of security is an additional barrier that helps protect against data loss or theft. ***Figure OV-1*** on the next page shows the security layers that agencies often rely on to help secure confidential information. As the figure shows, security layers are comprised of many different security controls including IT policies or software applications. Using multiple layers of security requires hackers or unauthorized individuals to overcome numerous barriers to reach sensitive or confidential data.

Figure OV-1
Security Layers Used to Protect Confidential Data


SECURITY POLICIES and PROCEDURES
Security management (tone at the top) and written IT policies and procedures including staff security awareness training, a Continuity of Operations Plan (COOP), and inventory checks
PHYSICAL CONTROLS
Data center environmental controls, locks, and access to network switches
SYSTEM CONTROLS
Firewalls, routers, switches, Wi-Fi access points, software patches, and anti-virus
APPLICATION CONTROLS
Authentication through user IDs, passwords, PINs, tokens, and biometrics
CONFIDENTIAL DATA
Restrict user access to only the data they need to complete their job

Agencies rely on a wide range of IT security controls to help protect confidential data. Those controls exist in multiple layers to help provide numerous barriers to unauthorized access from both outside of and within an agency.

Source: LPA summary of common network security layers adapted from Cisco.

Agency officials make choices regarding how secure to make each layer given their business needs and resources. Agency officials must manage their operations within finite resources, and adding additional security controls often requires additional staff time and money. Consequently, agency officials must balance how much risk they are willing to assume against their business needs and resources. Based on that assessment, they select which security controls and layers are necessary.

Ideally, each security layer should be independently secure to minimize the risk that confidential information is compromised. A weakness in only one or two security layers can make it much easier for someone to gain access to confidential information. For example, in March 2011, hackers gained access to the network of RSA, an internet security firm, by sending infected email attachments that exploited an unpatched vulnerability in Adobe Flash. The breach, which was caused by failures of the system layer (software patches) and policy layer (security awareness training), resulted in a loss of proprietary data that cost the firm $66 million to remediate.

ITEC has created security standards for many security layers to help agencies protect confidential data. The Legislature statutorily created the Information Technology Executive Council (ITEC) in 1998. ITEC comprises 17 members from all three branches of state government, as well as local governments and private businesses. To help protect confidential data, ITEC has developed state security standards that represent the minimum security requirements almost all state agencies must comply with. In this audit, we have frequently used the ITEC requirements as the benchmark for good security practices.

Do Selected State Agencies Have Adequate IT Security Controls to Help Ensure that Confidential Information is Protected?

Answer in Brief:

Most agencies' IT security controls we reviewed were not strong enough to help ensure that confidential information was adequately protected. Most agencies had weak controls to help ensure strong and secure staff passwords (p.8), and almost all agencies did a poor job of patching software vulnerabilities for both workstations and servers (p.11). Most agencies did not adequately train staff on IT security issues (p.13), and none of the agencies had fully developed and tested a continuity of operations plan (p.15). While most agencies adequately controlled their IT inventory, four agencies were missing or had lost track of computers (p.15). On the other hand, we found only a few problems with network access points, which were largely controlled by the Office of Information Technology Services (p.17).

In addition to addressing specific security issues, agencies should also have a comprehensive security management process to develop and enforce strong IT security controls (p.18). None of the agencies had a fully developed security management process, but all nine had at least some process components (p.19). Finally, security controls were far stronger at agencies where management made IT security a priority (p.21)

These and other findings are discussed in the sections that follow.

We Evaluated Various Aspects of IT Security at Nine State Agencies

We selected nine agencies largely based on the amount of confidential information they maintain. That information could include social security numbers, tax return information, or other personally identifiable information. The nine agencies we evaluated were:

- Department of Commerce
- Department of Corrections
- Department of Education
- Department of Labor
- Department of Revenue
- Department of Wildlife, Parks, and Tourism
- Juvenile Justice Authority
- State Board of Indigents' Defense Services
- State Treasurer's Office

We evaluated six important IT security controls in each of our nine selected agencies. We selected those controls because we thought they were important to IT security, and because they fell within several different security layers. The security layers are discussed in more detail in ***Figure OV-1*** on page 4.
In order of the severity of problems we found, those six controls were:

- Passwords (*application layer*) – controls access to an agency's network and confidential data.

- Software patches (*system layer*) – fixes known vulnerabilities in agency software that could be exploited by hackers.

- Security awareness training (*policy layer*) – informs staff about IT security risks and what actions they can take to better secure confidential data.

- Continuity of operations plan (*policy layer*) – provides a roadmap for an agency to reestablish operations after an emergency such as a tornado or large-scale hardware failure.

- IT hardware inventory (*policy layer*) – helps ensure that all computers and hardware that can access and store confidential information are accounted for.

- Network switches and Wi-Fi (physical and *system layer*) – controls both wired and wireless access to an agency's network.

In this audit, we evaluated each control independently. This allowed us to evaluate the strength of the individual controls, but does not necessarily allow us to conclude whether a hacker would be able to exploit any weaknesses. For example, to test the strength of staff passwords, we obtained a master password file directly from the agency and used password cracking software to test the passwords. This allowed us to conclude on the strength of the passwords, but does not simulate how a hacker would need to breach an agency firewall and other security controls to get to the same file.

We also evaluated each agency's comprehensive IT security management process. Best practices suggest that agencies should use a systematic process to help identify and prevent potential security breaches. That process, described in more detail on page 18, requires that agency officials regularly assess IT security risks, develop policies and controls to mitigate those risks, and monitor those controls to ensure they are effective.

FINDINGS RELATED TO SPECIFIC IT SECURITY CONTROLS

Most Agencies Had Weak Controls to Help Ensure Strong and Secure Staff Passwords

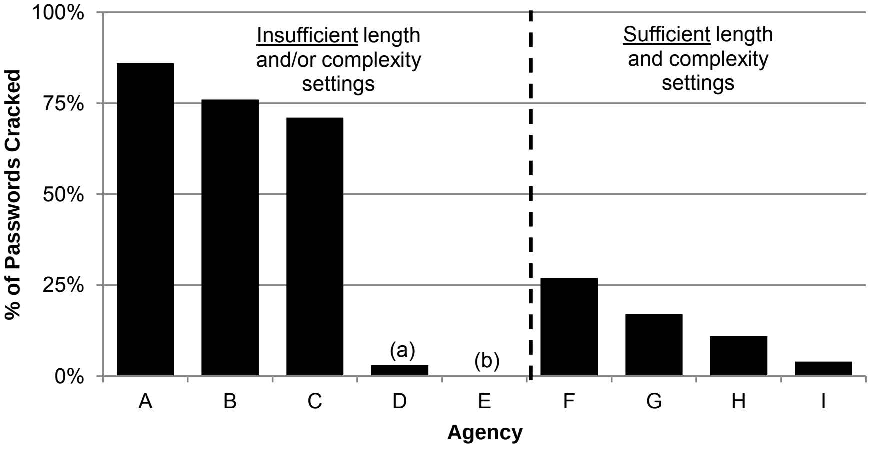
Using passwords to control access to networks and computers is inherently risky because it is relatively easy to crack many passwords. Despite the risk, passwords remain the most common form of security because they are far less expensive to use than other secure alternatives such as thumbprint identification.

To evaluate how well each agency managed passwords, we compared their password polices and settings to best practices and attempted to crack staff passwords. Password settings are controlled by IT staff and are used to establish minimum requirements for strong and secure passwords. We only tested passwords staff used to login to their computers, and not passwords used to access other agency applications or systems.

We cracked a significant number of passwords in six agencies because staff did not create strong passwords. To crack passwords, we collected each agency's encrypted password file and tested the strength of those passwords using free password cracking software available on the Internet.

A summary of agency password settings and the percent of cracked passwords is shown in ***Figure 1-1*** below.
As the figure shows, we cracked significantly fewer passwords in agencies with strong settings. We also found that:

Figure 1-1
Password Settings and Crack Rates for All Audited Agencies



(a) Despite having incorrect settings, the agency's crack rate is low likely because other agency applications require strong passwords. As a result, users may be using the same (stronger) password for both the network and the special application, or may have become accustomed to creating strong passwords even though the settings do not require them.
(b) We did not attempt to crack user passwords at this agency because its network configuration required us to test each user's password one at a time.

Source: LPA analysis of agency passwords settings and password crack results.

- **Five agencies had insufficient password settings to help ensure strong passwords.** To help ensure password strength, passwords must be sufficiently long and complex. Complexity settings require that passwords use a combination of uppercase letters, lowercase letters, numbers and special characters. Although most systems can be set to require lengthy passwords that use at least three of the four types of characters, five agencies did not have adequate length or complexity settings, including one agency that had neither setting.

- **The majority of passwords we cracked that met proper length and complexity requirements were constructed in a way that made them easy to crack**. That is because even complex passwords that use at least 8 characters and different types of characters can be easily cracked if they are built in a predictable fashion. Without proper training, it is more likely that staff might create passwords that appear strong, but are not. Examples of passwords we cracked included "Computer1", "password1!", and "Bluebird1". ***Figure 1-2*** on page 11 provides more information on constructing strong passwords.

Most agencies did not have adequate settings to help ensure passwords were adequately secured. In addition to making passwords stronger, password settings can also help secure those passwords from outside attacks. We found several problems with those settings in most of our selected agencies.

- **Seven agencies had not adequately configured settings to force staff to effectively change their passwords.** These agencies had weak or missing settings to force staff to frequently change and not recycle their password. Some agencies also failed to force staff to change the default password assigned to them when they started working with the agency. These weaknesses represent a threat to cracking passwords and to the agency itself.

- **Eight agencies used weak encryption to store passwords, which made them easier to crack.** In Microsoft Windows, passwords are stored in the computer in an encrypted format. There are two forms of encryption that can be used to protect user passwords. One is older, weaker, and much easier to crack while the other is newer and more secure. The weaker encryption may be needed at times to accommodate older software applications within an agency. However, only four of the eight agencies that used the older, weaker encryption needed it to accommodate older applications. Three agencies had no business reason to expose their passwords to greater risk and one agency was not sure if the weaker encryption was necessary.

- **Four agencies had not properly configured settings to lock out users after several failed attempts to log on.** Accounts should be set to automatically lock after several failed attempts to prevent a hacker from continuously trying to hack a user account. Two agencies had no lockout settings, which would allow a hacker unlimited attempts to crack passwords.

Two agencies further compromised passwords by failing to train staff that it is not acceptable to share passwords. Passwords serve not only as a means to gain access to an agency's network, but also as a form of identification to track what each user did while on the agency's network. If more than one person has access to a password, it is difficult to assign responsibility for inappropriate usage or actions. To ensure a password can uniquely identify a user, it is a best practice that staff should keep it strictly confidential. We identified two agencies that did not enforce this standard.

- **In one agency, supervisors knew the passwords of those working for them and IT staff kept a list of all staff user names and passwords.** If users changed their password, they were instructed to tell their supervisor and IT staff what the new password was. Although this agency used several passwords for different systems, sharing passwords creates significant risk to both the agency and individual employees that confidential data may be breached or inappropriate behavior may occur.

- **Another agency inappropriately trained staff that it was okay to share their password with IT staff.** IT staff should use their own user name and password when helping to fix another user's computer. Although it might be more convenient, they never need the user's password to do their work.

Figure 1-2
Some Passwords That Seem Complex May Be Easy To Crack

One of the important best practices for passwords is to require complex passwords be at least eight characters in length. Complex passwords include a combination of three of the four types of characters on the keyboard—uppercase letters, lowercase letters, numbers, and special characters. Such passwords are considered complex because it takes a long time for a hacker to try every combination of characters—even with password cracking software. However, complexity assumes that the passwords are created in a random and unpredictable manner.

Unfortunately, most users do not create random passwords, instead placing uppercase letters, numbers and special characters in predictable places. Studies have shown that when people use uppercase letters in passwords, they tend to place them at the beginning of the password. Conversely, they tend to place numbers and special characters, at the end of the password. People also tend to use only those special characters that are on the top row of the keyboard, avoiding characters such as brackets, quotation marks, and semicolons.

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

The key to creating strong passwords is moving numbers or special characters to the middle of the password. The following are a few typical examples of passwords that meet the complexity requirements (each incorporates proper length and three of the four types of characters), but are relatively easy to crack because of where the numbers and special characters have been placed. A stronger example of a similar password is also shown:

Weak Password	Strong Password
$apple43	app$le43
Thinking43	thin$king43
$orange43	ora$nge43
Monkey02	moN02key

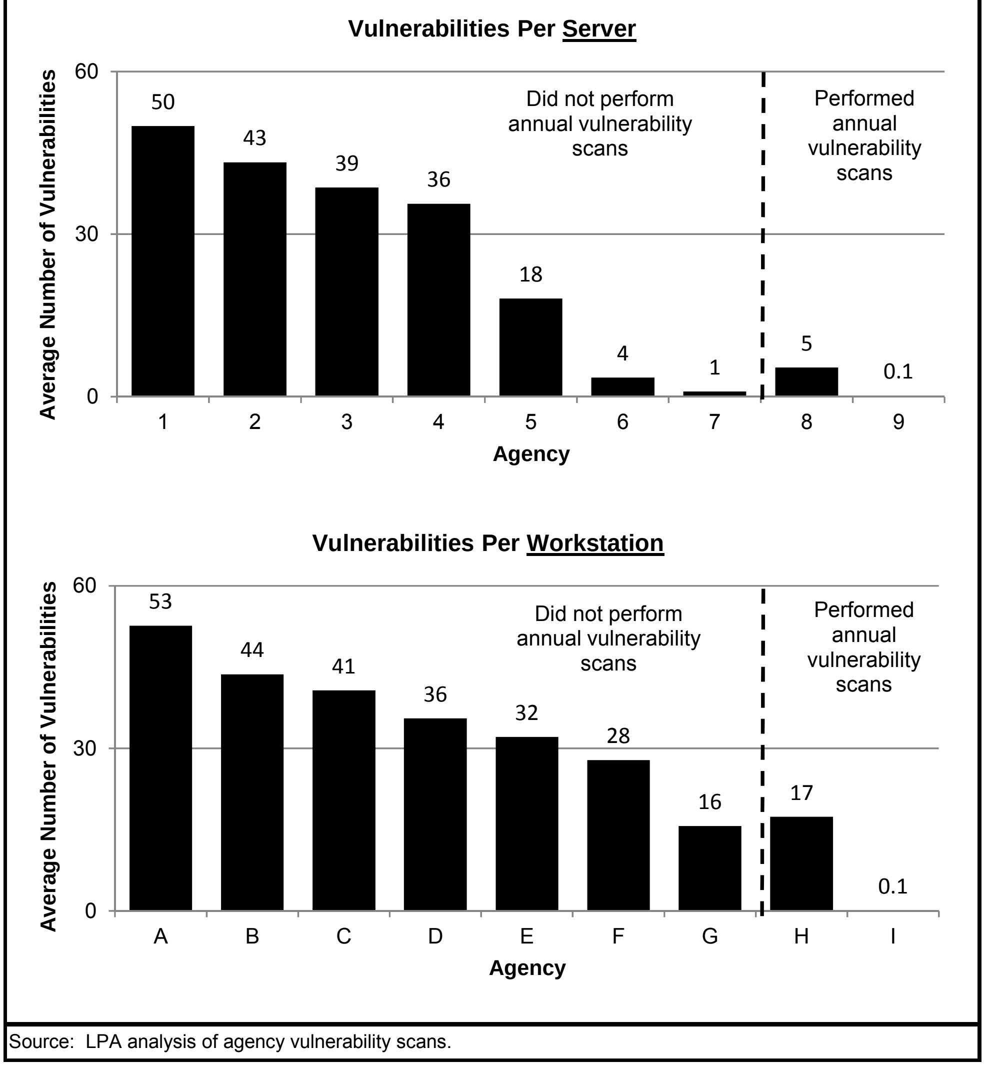
Almost All Agencies Did a Poor Job of Patching Software Vulnerabilities for Both Workstations and Servers

Over time, vulnerabilities in computer software are discovered that could allow someone to break into or otherwise harm an agency's network. Software manufacturers are constantly developing "patches" for these vulnerabilities as they are discovered. A basic function of each agency's IT staff is to install those patches to keep the agency's software and systems up to date and secure.

We used a vulnerability scanner which looks for unpatched software to identify how well IT staff patched high-risk vulnerabilities. We excluded certain types of unpatched vulnerabilities from our analysis, including low-risk patches, patches that had only recently been made available, and patches that were incompatible with an agency's software applications.

As we have found in previous audits, most agencies had a significant number of unpatched software vulnerabilities. Ideally, we would expect agencies to completely eliminate all high-risk software vulnerabilities, but realize that expectation is not very realistic. Not counting recent, low-risk, or incompatible patches, we looked for an average of three or fewer vulnerabilities per machine. ***Figure 1-3*** below summarizes the average number of vulnerabilities for each agency. As the figure shows, very few agencies had vulnerabilities below our expected threshold.

Figure 1-3
Average Software Vulnerabilities for
Audited Agencies' Servers and Workstations



Source: LPA analysis of agency vulnerability scans.

Having unpatched software applications is not a new problem for the state. Our 2009 and 2011 IT security audits evaluated these vulnerabilities across a total of 10 agencies. In both audits, we identified agencies with numerous software vulnerabilities across servers and workstations.

Agencies had much more difficulty patching non-Microsoft vulnerabilities than Microsoft vulnerabilities on workstations. Agencies had an average of five unpatched Microsoft vulnerabilities, compared to an average of 25 unpatched non-Microsoft vulnerabilities. Non-Microsoft companies are not as proactive as Microsoft in notifying users about when new patches become available, and many agencies did not have software that could automatically apply non-Microsoft patches to employee workstations.

The two agencies that performed annual vulnerability scans typically had fewer vulnerabilities on both servers and workstations. As ***Figure 1-3*** on page 12 shows, those agencies had far fewer vulnerabilities than most of the agencies that did not perform scans.

In addition to the vulnerabilities shown in the figure, some agencies had unpatched vulnerabilities due to old systems and applications. While these vulnerabilities were excluded from our analysis because they cannot be successfully fixed in the short run, vulnerabilities in older systems still present an ongoing security risk to the agency that should be addressed in the long run. As such, they are one reason an agency should try to upgrade legacy systems and applications as soon as reasonably possible.

The Office of Information Technology Services (OITS) recently negotiated a statewide license for vulnerability scanning software. As of October 2012, OITS negotiated a statewide license with Sophos that makes vulnerability scanning software available to all state agencies at a discounted rate. This software could potentially provide a cost effective means to help agencies ensure that software patches have been applied correctly.

Most Agencies Did Not Adequately <u>Train Staff</u> on IT Security Issues

Agency staff represent one of the most significant risks to an agency's security. That is because they may intentionally or inadvertently expose the agency's network or data to unauthorized individuals. Annual security awareness training teaches staff how to keep confidential data and the agency network safe from attacks and is required under the state's ITEC standards. This helps reduce the risk that staff will disclose, expose to attack, or abuse confidential information.

Seven agencies failed to provide adequate training on an annual basis. In reviewing the content of agencies' security awareness training, we found several problems:

- **Four agencies did not provide any security awareness training to staff.** Agency staff primarily reported that training was not provided because they were waiting for the Office of Information Technology Services or other agencies to develop the training.

- **Two agencies provide some training, but failed to address all of the key security topics.** ITEC requires that state agencies train staff on 12 security topics such as passwords, viruses, and physical security. Two agencies were missing one of the required 12 topics.

- **One agency did not train the majority of its staff on an annual basis.** ITEC requires agencies to provide security awareness training to new hires within 90 days, and annual training to all staff. Only about 30% of staff in this agency reported receiving such training within the last year.

Even agencies that provided regular security training had staff who did not fully understand several critical IT security risks. We surveyed all staff in each agency to determine how well they understood IT security risks. Based on responses to that survey, staff did not fully understand risks in three areas.

- **Many employees did not fully understand how to create strong passwords and that passwords should not be shared with anyone.**

- **Many employees did not recognize the threat of viruses from email attachments or links.**

- **Some employees did not understand that viruses can be transferred from portable devices when they are physically connected to their computer.**

Only the Department of Education took steps to help ensure staff fully understood what they had been taught. The department quizzed staff to identify security topics that needed more emphasis, and IT staff annually updated the training based partly on quiz results. The other eight agencies either did not monitor security awareness training at all, or not in a way that could help refine the training.

OITS has developed centralized security awareness <u>training</u> but agencies are not aware of it. About three years ago, the Kansas Enterprise Security Office (now part of OITS) developed security awareness training and made it available on its website. However, none of our audited agencies were using the available training. Furthermore, two agencies reported that they were waiting for OITS to develop training and were not aware of the training already available. We did not fully evaluate the training but our brief review found that it was time intensive.

None of the Agencies Had Fully Developed and Tested a <u>Continuity of Operations Plan</u>

A continuity of operations plan (COOP) is important because it provides a roadmap for an agency to reestablish operations after an emergency such as a tornado, fire, flu pandemic, or large-scale hardware failure. The COOP includes information about the agency's essential functions, staff roles in an emergency, and alternate operating facilities. Without a comprehensive and tested COOP, an agency will likely fail to reestablish operations in a timely manner during an emergency.

Only one agency had fully developed the five sections of its continuity of operations plan that we reviewed. A COOP covers many areas, but we limited our review to the five we thought were most important. These included:

- <u>Roles and responsibilities</u>—covers who is responsible for certain actions in the event of an emergency.
- <u>Alternative facilities</u>—covers where staff will perform work in the event the primary location is damaged, destroyed, or not available.
- <u>Mission essential functions</u>—prioritizes which agency functions are first to be restored after an emergency.
- <u>Succession plan</u>—lists the order of succession for key agency staff and their position.
- <u>Alert Notification Procedures</u>—lists the procedure the agency will use to notify staff of what action needs to be done and when.

Only the Board of Indigents' Defense Service had adequately developed all five areas. Five of the audited agencies had not sufficiently developed two or more areas, with alert notification procedures being the most common.

None of the agencies routinely tested the quality and usefulness of their continuity of operations plans. Routine testing is a good way to assess the quality of a COOP and to determine how well staff understand what they should do in the event of an emergency. Seven of the nine agencies had never tested their COOP. The other two agencies tested it during our audit, but had not tested it in the past few years.

While Most Agencies Adequately Controlled Their <u>IT Inventory</u>, Four Agencies Were Missing or Had Lost Track of Computers

Losing a piece of IT hardware (including workstations, laptops, and servers) increases the agency's risk that sensitive or confidential data will be compromised. Maintaining an accurate inventory and routinely verifying the physical existence of the items it lists helps ensure all computer hardware is accounted for.

We compared agency inventory records to randomly selected IT equipment in each agency to identify any discrepancies.

Five of the nine agencies were in possession of all IT hardware we looked for. Those agencies included:

- Board of Indigents' Defense Services
- Department of Corrections
- Department of Labor
- Department of Revenue
- State Treasurer's Office

While some of these agencies may have had a few minor issues with their inventories, such as inaccurate equipment locations and missing inventory tags, they were able to account for all of the IT equipment we looked for.

Three agencies had lost track of some IT equipment and one was missing four computers. Based on an onsite check of agency IT inventory we found:

- **The Juvenile Justice Authority had no inventory of IT equipment and had not kept track of about 200 computers in its closed Atchison facility.** Agency officials had no IT inventory, but did create one specifically for this audit. However, during our fieldwork we identified about 200 computers at their closed Atchison facility which had been stored there since 2009 and were not included of this new inventory. As an added precaution, we evaluated several of those computers to ensure they did not contain any confidential information.

- **The Department of Wildlife, Parks, and Tourism was missing four computers and had one computer in its possession that was not in its IT inventory.** We randomly selected 31 computers listed on the agency's inventory. Agency officials could not locate four of them. At this point the computers are presumed to be lost. Furthermore, we identified one computer that was in the agency's possession, but not included in the agency's inventory. Officials cited poor inventory procedures and a lack of training as the reason for these missing computers. They also told us that the computers did not contain confidential information.

- **The Department of Education had four computers and the Department of Commerce had one computer in the agency's possession that was not in the IT inventory.** Because the department's inventory was incomplete, officials are unable to determine whether some equipment is missing

Four agencies did not independently check the inventory on an annual basis to ensure the agency had all required IT hardware. The state's ITEC standards require an agency to review and update its inventory at least annually. The Juvenile Justice Authority, the Department of Education, and the Department of Corrections did not conduct annual inventory checks. While the Department of Wildlife, Parks, and Tourism checked its inventory annually, it relied on staff to self-report computer equipment in their possession. That increases the chance that missing equipment will not be reported, either intentionally or accidentally

The state's IT and accounting policies have different inventory requirements, creating confusion for several agencies. The Statewide Management Accounting and Reporting Tool (SMART) and ITEC both have inventory requirements. The SMART system requires all agencies to inventory all equipment worth $5,000 or more. This includes IT equipment, but the relatively high threshold would exclude most agency computers. On the other hand, ITEC requires all IT equipment be inventoried, regardless of value. The differences in the requirements are due to the different purposes of the inventories—the SMART inventory is used to tally the value of all state assets, while the ITEC inventory is intended to prevent the loss of data stored on any computer equipment.

These competing requirements caused some internal coordination problems in some agencies. For example, the Department of Education's Fiscal Services and Operations Division maintained and checked all inventory over $5,000 because of SMART requirements but only spot checked items under $5,000, which included most staff computers. Department staff reported being unaware that ITEC required annual inventories of all IT hardware.

We Found Only a Few Problems with Network Access Points, Which Were Largely Controlled By the Office of Information Technology Services

To access an agency's network, staff use either a wired connection that runs through a switch or a wireless connection (Wi-Fi). Switches should be locked in secure rooms to ensure only authorized staff can access them. Wi-Fi should be limited to those that need access, and the data should be encrypted to ensure it is securely transmitted.

The Office of Information Technology Services (OITS) generally provides agencies with network switches and Wi-Fi access, but agencies can supplement OITS services in some cases.

To determine if agency switches and Wi-Fi were secure, we inspected the physical security around switches and the security settings of wireless access points that were accessible within the agency.

Two agencies had switches located in unsecured areas that could be accessed by staff and agency guests. Two of nine agencies had switches located in staff common areas such as break rooms and open office space, which could allow unauthorized personnel to easily access the agency network. One agency managed its own switches outside of OITS control. However, the other agency's switches were serviced by OITS so both the agency and OITS should have been aware of the weak security.

Only one agency had any unsecured Wi-Fi access points. One agency had multiple Wi-Fi access points that used weak encryption to protect the data being transmitted. As a result, it would be easier for hackers to gain access to the agencies network and data. These access points were managed by the agency and not by OITS, which generally uses a much stronger encryption.

FINDINGS RELATED TO AGENCIES' OVERALL MANAGEMENT OF IT SECURITY

Agencies Should Have a Comprehensive Security Management Process to Develop and Enforce Strong IT Security Controls

Although much of our work was focused on specific security controls, effective IT security involves more than patching software and adopting security policies. Effective IT security is the result of a cyclical and dynamic security management process.

An IT security management process includes four components that help the agency develop and enforce strong security controls. ***Figure 1-4*** on page 19 summarizes this process, which includes the following components.

- A comprehensive risk assessment—a preventative process designed to examine all risks to the agency, determine the likelihood and impact of those risks, and identify policies and controls that can be implemented to mitigate them.

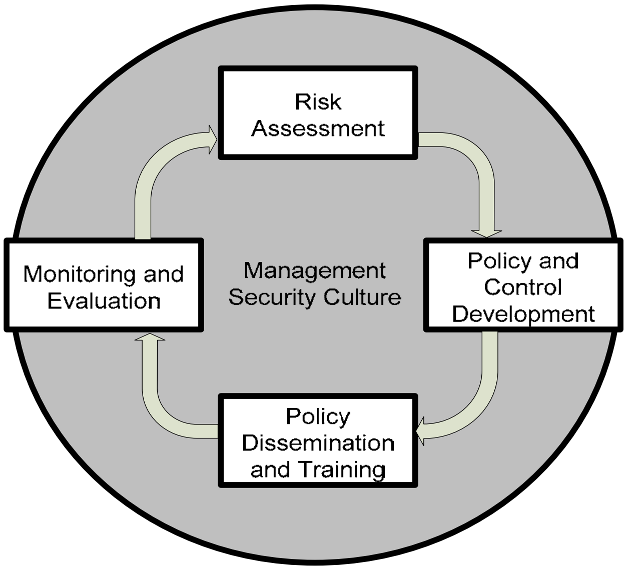
- Developing written policies and controls—a set of written policies and security controls used to help mitigate security risks.

- Disseminating policies and training staff—helps ensure that staff are aware of their responsibilities to help mitigate security risks.

- Monitoring and evaluating policies and controls—provides feedback to agency officials on whether current policies and controls are effective.

In addition, a security-conscious management culture is a critical part of the security management process. As ***Figure 1-4*** on the next page shows, the management security culture encompasses all other components of the process. That is because IT security measures require agency resources to implement and monitor, and also because they often are seen as an inconvenience to agency staff. Without management support, the best intentions of IT staff or well developed security controls will likely be short lived.

Figure 1-4
IT Security Management Process


Risk Assessment
Policy and Control Development
Policy Dissemination and Training
Monitoring and Evaluation
Management Security Culture

Source: Adapted from Information Security Management Learning from Leading Organizations, GAO/AIMD-98-68, May 1998.

None of the Agencies Had a Fully Developed Security Management Process, but All Nine Had at Least Some Process Components

We evaluated each of the components of the security management process for our nine selected agencies.

None of the agencies had conducted a comprehensive risk assessment to identify, prioritize, and resolve IT security threats. Performing a comprehensive risk assessment helps agencies identify all possible IT security risks, and then prioritize which ones should be addressed first. We found that:

- **All agencies lack comprehensive risk assessments that are routine and agency wide.** As mentioned previously, a comprehensive risk assessment is a preventative process and includes staff from all business aspects of the agency. The goal is to identify risk, set security priorities that can minimize that risk, and reevaluate agency risks on regular basis.

- **However, many agencies conducted ad hoc risk assessments for specific IT projects.** These assessments were conducted as needed to identify risks for a single project or a specific security risk. While these risk assessments can be helpful, the limited scope and unscheduled nature is not adequate to assess and prioritize agency wide security needs.

None of the agencies had a complete set of policies to help establish and communicate agency accepted practices or expectations. We reviewed policy requirements established by the state Information Technology Executive Council (ITEC), the

National Institute of Standards and Technology (NIST), and used our judgment to determine which policies agencies should have to address IT security in the areas we reviewed. In all, we assessed 45 specific policy requirements or best practices in our selected agencies.

- **Six agencies did not meet at least two-thirds of the policy requirements we reviewed.** Agency results varied widely. The Department of Revenue met 76% of these requirements, which was the most of any of the nine agencies. Conversely, one agency had no approved IT security policies.

- **Agencies sometimes had adequate IT security practices that were not codified in written policies.** For example, one agency's IT staff performed annual inventory checks of all IT equipment but the agency did not have a policy that put that practice in writing. Without written policies, IT staff must rely on an informal transfer of knowledge from others. This process could lead to important information not being transferred, or worse, incorrect information being transferred.

- **IT staff in some agencies were unaware or unfamiliar with the state's IT policy requirements.** It is the responsibility of agency's IT staff is to be aware of and comply with all applicable state security requirements. However, this responsibility is made more difficult because the requirements developed by ITEC are lengthy and complex, which could make them difficult to understand. Further, as we found in a previous audit, ITEC does a poor job of communicating those requirements to state agencies.

Five agencies did not effectively disseminate policies to staff that needed to be aware of them. For example, one agency put its policies on its intranet but did not notify staff when new or revised policies were added. In another agency, officials thought their policies were on their intranet for staff to read, but were not able to find them when we asked to see them. Proper dissemination requires agencies to proactively educate staff about relevant security policies and changes. Strong IT security policies are only useful if staff are aware of them.

Very few agencies adequately monitored certain IT security areas to mitigate risks, including performing vulnerability scans. Monitoring is important because it helps management assess whether agency policies and security controls are being followed and are effectively mitigating risks. We reviewed agencies monitoring efforts for four specific controls and found:

- **Seven agencies did not perform vulnerability scans to identify missing software patches on servers or workstations.** As mentioned earlier, performing vulnerability scans is a very effective way to help ensure all servers and workstations are adequately patched.

- **Eight agencies did not monitor the effectiveness of security awareness training.** Testing staff knowledge helps to identify security topics that need more emphasis in future training.
- **None of the agencies had routinely tested a continuity of operation plans (COOP).** Testing a COOP through a live simulation or a tabletop exercise is a critical step to help ensure that the plan works as intended.
- **Four agencies did not conduct an independent annual inventory check of IT equipment.** Routine inventory checks help to ensure all computer hardware that may contain or be able to access confidential data is accounted for.

IT Security Controls Were Far Stronger at Agencies Where Management Made IT Security a Priority

To determine whether agency management created a strong IT security conscious culture, we surveyed all agency staff and reviewed each agency's security management process. We found that management's "tone at the top" had a clear effect on the strength of an agency's security controls.

Management at the State Treasurer's Office appears to plan and emphasize the importance of IT security, and generally had strong IT security controls. Management at this agency was clearly IT security conscious and set a strong "tone at the top" that emphasized the importance of IT security. The head of IT was regularly involved in statewide IT meetings, and 83% of staff thought IT security was a very high priority. In addition, IT staff were running quarterly vulnerability scans, an often resource-intensive process used to ensure workstations and servers were patched. As a result of these efforts and general support for IT security, the State Treasurer's Office had very few weaknesses in the IT security controls we reviewed.

Management at several agencies did not make IT security a priority and had weak or missing controls. One agency in particular did a poor job in all six specific security areas we evaluated in this audit, and met only 7% of the policy requirements we reviewed. Management reported spending very little time on IT security and did not demonstrate a commitment to creating and enforcing strong security controls. Not surprisingly, only about 20% of agency staff reported they thought IT security was a very high priority for the agency.

Conclusion

Our cumulative IT security audit work over the past five years reveals some chronic weaknesses in several important security controls. Those include software vulnerabilities, weak or vulnerable passwords, and incomplete continuity of operations plans. Some of these weaknesses, such as software vulnerabilities, represent a more immediate threat to the state's security. Others, such as a poorly developed continuity of operations plan are less pressing, but could have significant long-term consequences.

The problems we have identified are often a combined result of poor management support, a decentralized approach to IT security across the state, and poorly communicated and enforced state security standards. Because agency resources are limited, it is critical that agency management has a clear sense of what security risks they face, which are most important, and what steps they can reasonably take to address them. Additionally, both the Information Technology Executive Council (which sets the state's security standards) and the Office of Information Technology Services (which provides IT services to most of the Executive Branch) could improve the state's IT security by clearly communicating security standards and offering centralized security solutions in critical areas.

Recommendations for Executive Action

1. To help protect the agency's network and data, the nine agencies we reviewed should implement all recommendations provided to them in their respective confidential reports.

2. The Office of Information Technology Services should take the following actions:

   a. Review the centralized security awareness training to ensure it effectively covers all 12 ITEC required areas. Also, communicate the availability of the training to all state agencies, as well as the ITEC mandatory requirement to train all new employees with 90 days of hire and all employees annually.

   b. Communicate the availability of the vulnerability scanning software license to all state agencies and the ITEC mandatory requirement to conduct annual vulnerability scans.

APPENDIX A

Scope Statement

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

State Agency Information Systems:
Reviewing Security Controls in Selected State Agencies (CY 2012)

Each year, most state agencies collect and process sensitive and confidential data in their computer systems, including citizen social security numbers, medical information, and income data. Some agencies are responsible for protecting millions of confidential records, which makes them a potentially enticing target for hackers.

Often, agencies use multiple security layers to protect data and computers from cyber or physical attack. Potential security layers include physical security, perimeter security, and host security. Because no one layer can protect an agency against all threats, it is important to have multiple controls that complement each other and are independently secure. Weak or missing layers can create cracks in the agency's overall security, which increases the risk for agency data to be compromised.

Currently, there is limited oversight of agencies' security controls to ensure that agencies are adequately protecting confidential data. The Kansas Information Technology Executive Council (ITEC) has developed guidance to assist state agencies in developing adequate security controls, but ITEC doesn't monitor or audit how well those controls are implemented. Consequently, agencies have a significant amount of autonomy in how they develop, apply, and monitor security controls.

The Legislative Post Audit Committee approved information system audits as an adjunct to the Division's compliance and control audits. This information system audit looks at seven important information technology security areas across a broad selection of state agencies.

This information security audit answers the following questions:

1. **Do selected state agencies have an adequate security management process to assess, manage, and monitor IT risks?**

2. **Do selected state agencies adequately control passwords?**

3. **Do selected state agencies provide adequate security awareness training to all staff?**

4. **Do selected state agencies adequately patch servers and workstations?**

5. **Do selected state agencies adequately secure network access points?**

6. **Do selected state agencies adequately inventory and track IT hardware?**

7. **Do selected state agencies have adequate policies and procedures for continuing operations in the event of an emergency?**

To answer these questions, we would perform an overall evaluation of each agency's security management process. Specifically, for each security area, we would review agencies' policies and procedures and compare them to state IT requirements and best practices. We would also interview agency officials and staff to determine how well policies and procedures are being followed in practice, and would survey agency staff to determine their knowledge of IT policies and procedures. Where possible, we would perform direct test work to determine whether agency actions in these security areas where achieving the intended results. We would perform additional work in these areas as necessary.

Estimated resources: 3 staff for 9 months (plus review)

Agencies Selected for Audit (2012)

1. Commerce, Department of
2. Corrections, Department of
3. Education, Department of
4. Juvenile Justice Authority
5. Labor, Department of
6. Revenue, Department of
7. State Board of Indigents' Defense Service
8. State Treasurer
9. Wildlife, Parks and Tourism, Department of

APPENDIX B

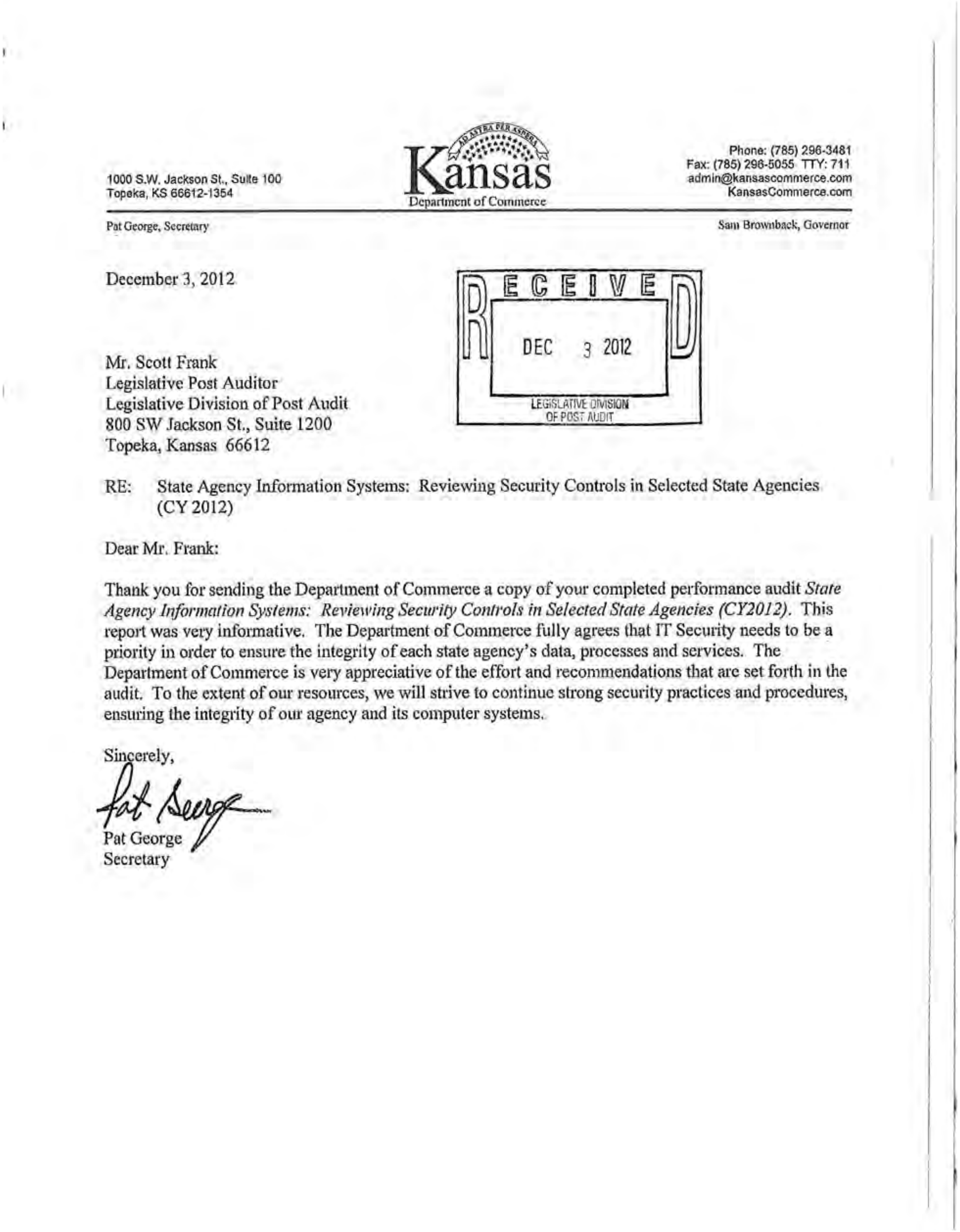
Agency Responses

On November 19 we provided draft copies of the public audit report to the nine audited agencies and the Office of Information Technology Services (OITS). Those responses are included as this appendix. Overall, the agencies concurred with the report's findings, conclusions, and recommendations.

We also provided each agency with a separate, confidential report to address agency specific problems we identified through our work. Because those responses contained specific IT security information that would jeopardize the agencies' security, we have not included those responses in this report.

In their confidential responses, agency officials generally concurred with our agency specific findings, conclusions, and recommendations. However, the Department of Commerce disagreed with a couple of findings. As a result we made a few minor changes to the final report.

Finally, all agencies have already started addressing many of our recommendations.



1000 S.W. Jackson St., Suite 100
Topeka, KS 66612-1354

Kansas
Department of Commerce

Phone: (785) 296-3481
Fax: (785) 296-5055 TTY: 711
admin@kansascommerce.com
KansasCommerce.com

Pat George, Secretary

Sam Brownback, Governor

December 3, 2012

Mr. Scott Frank
Legislative Post Auditor
Legislative Division of Post Audit
800 SW Jackson St., Suite 1200
Topeka, Kansas 66612

RE: State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2012)

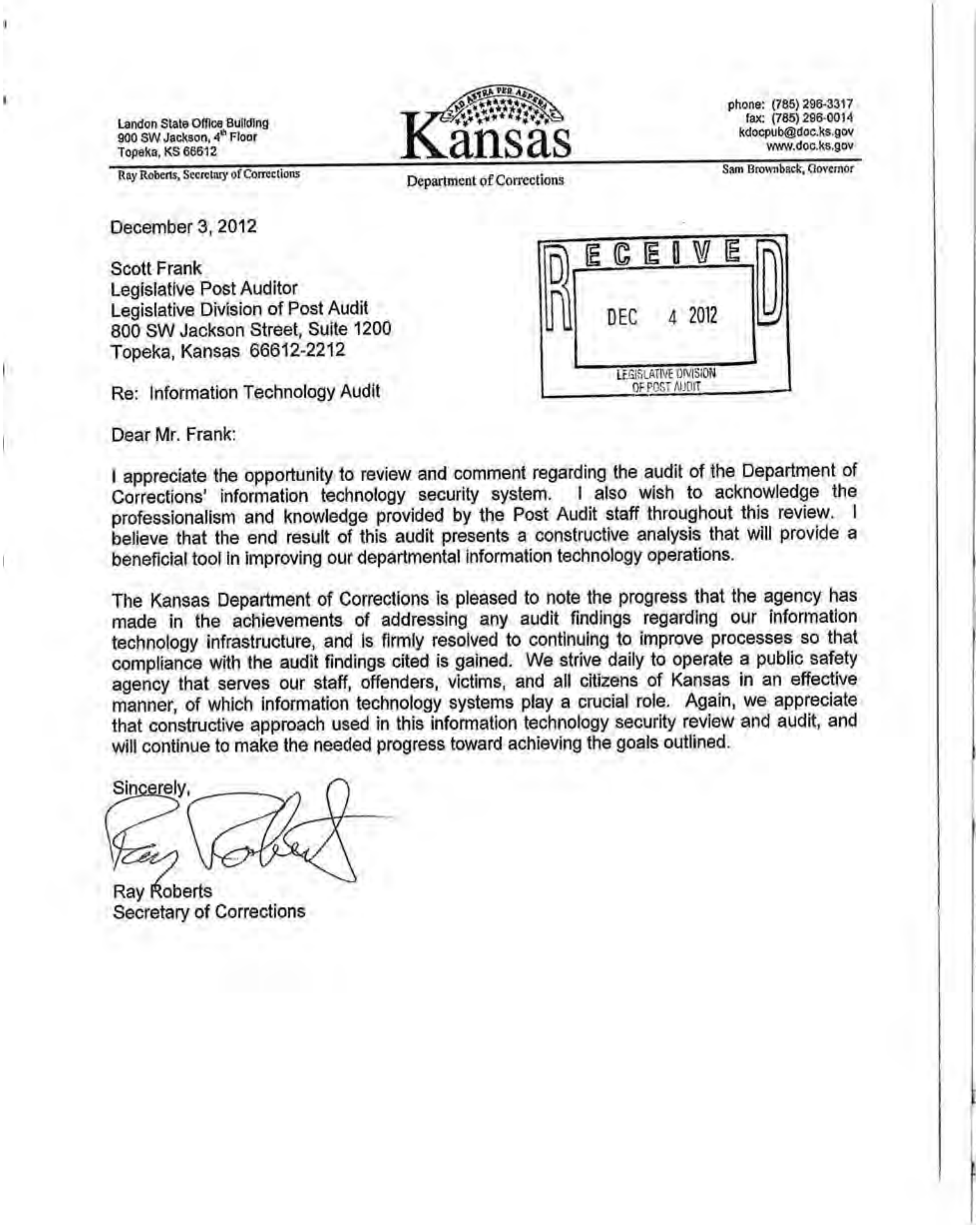
Dear Mr. Frank:

Thank you for sending the Department of Commerce a copy of your completed performance audit *State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY2012).* This report was very informative. The Department of Commerce fully agrees that IT Security needs to be a priority in order to ensure the integrity of each state agency's data, processes and services. The Department of Commerce is very appreciative of the effort and recommendations that are set forth in the audit. To the extent of our resources, we will strive to continue strong security practices and procedures, ensuring the integrity of our agency and its computer systems.

Sincerely,

Pat George

Pat George
Secretary



Landon State Office Building
900 SW Jackson, 4th Floor
Topeka, KS 66612

AD ASTRA PER ASPERA

Kansas

phone: (785) 296-3317
fax: (785) 296-0014
kdocpub@doc.ks.gov
www.doc.ks.gov

Ray Roberts, Secretary of Corrections

Department of Corrections

Sam Brownback, Governor

December 3, 2012

Scott Frank
Legislative Post Auditor
Legislative Division of Post Audit
800 SW Jackson Street, Suite 1200
Topeka, Kansas 66612-2212

Re: Information Technology Audit

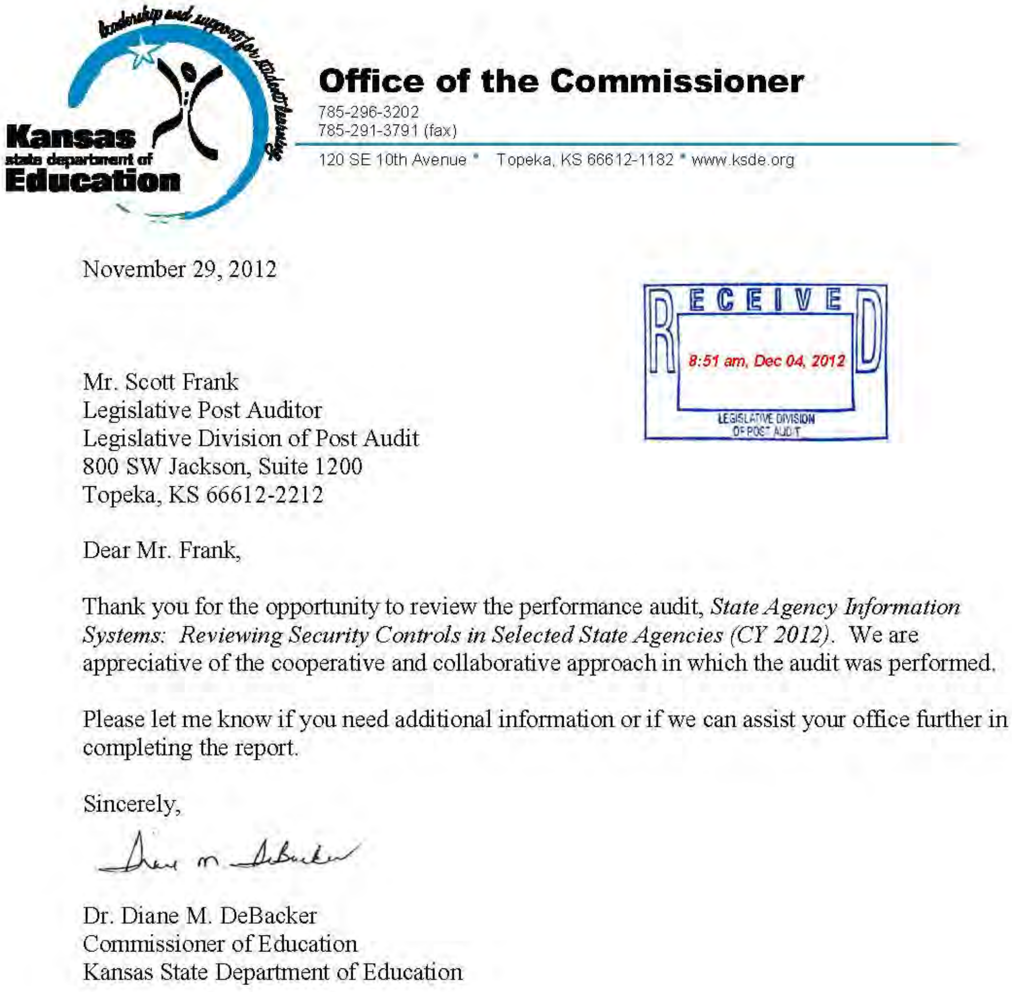
Dear Mr. Frank:

I appreciate the opportunity to review and comment regarding the audit of the Department of Corrections' information technology security system. I also wish to acknowledge the professionalism and knowledge provided by the Post Audit staff throughout this review. I believe that the end result of this audit presents a constructive analysis that will provide a beneficial tool in improving our departmental information technology operations.

The Kansas Department of Corrections is pleased to note the progress that the agency has made in the achievements of addressing any audit findings regarding our information technology infrastructure, and is firmly resolved to continuing to improve processes so that compliance with the audit findings cited is gained. We strive daily to operate a public safety agency that serves our staff, offenders, victims, and all citizens of Kansas in an effective manner, of which information technology systems play a crucial role. Again, we appreciate that constructive approach used in this information technology security review and audit, and will continue to make the needed progress toward achieving the goals outlined.

Sincerely,

Ray Roberts
Secretary of Corrections



leadership and support for student learning

Kansas
state department of
Education

Office of the Commissioner

785-296-3202
785-291-3791 (fax)

120 SE 10th Avenue • Topeka, KS 66612-1182 • www.ksde.org

November 29, 2012

Mr. Scott Frank
Legislative Post Auditor
Legislative Division of Post Audit
800 SW Jackson, Suite 1200
Topeka, KS 66612-2212

Dear Mr. Frank,

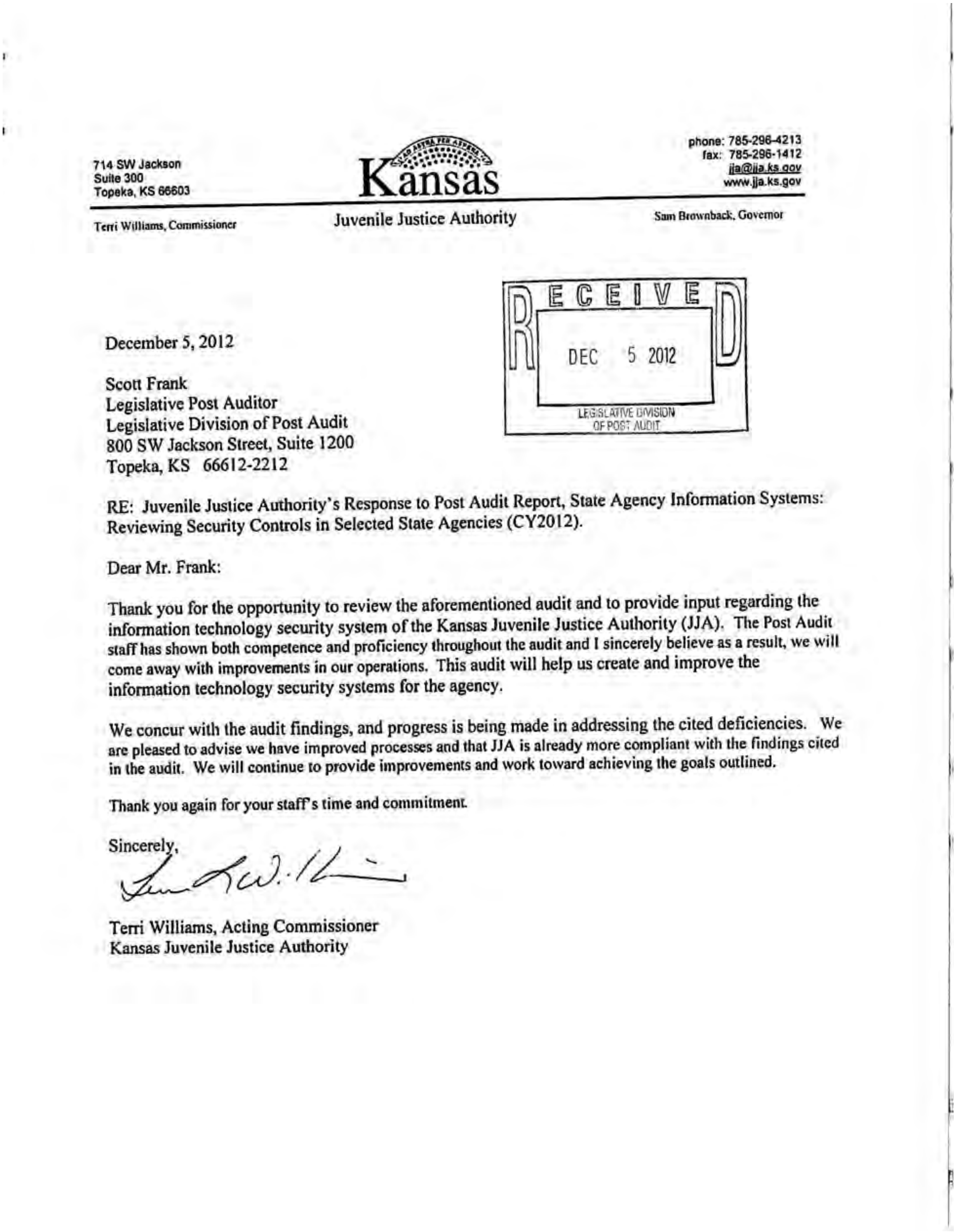
Thank you for the opportunity to review the performance audit, *State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2012)*. We are appreciative of the cooperative and collaborative approach in which the audit was performed.

Please let me know if you need additional information or if we can assist your office further in completing the report.

Sincerely,

Diane M. DeBacker

Dr. Diane M. DeBacker
Commissioner of Education
Kansas State Department of Education



714 SW Jackson
Suite 300
Topeka, KS 66603

Kansas

phone: 785-296-4213
fax: 785-296-1412
jja@jja.ks.gov
www.jja.ks.gov

Terri Williams, Commissioner

Juvenile Justice Authority

Sam Brownback, Governor

December 5, 2012

Scott Frank
Legislative Post Auditor
Legislative Division of Post Audit
800 SW Jackson Street, Suite 1200
Topeka, KS 66612-2212

RE: Juvenile Justice Authority's Response to Post Audit Report, State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY2012).

Dear Mr. Frank:

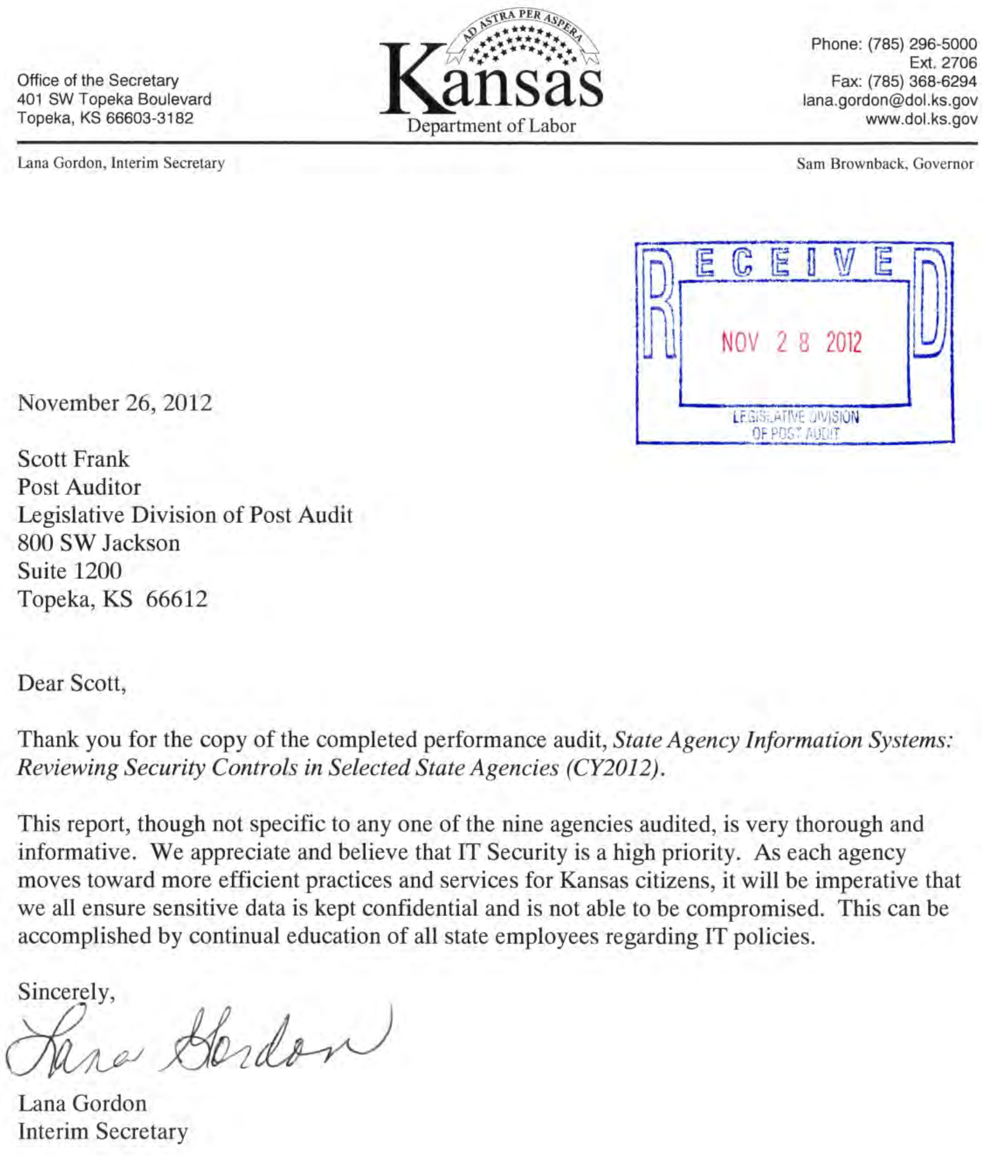
Thank you for the opportunity to review the aforementioned audit and to provide input regarding the information technology security system of the Kansas Juvenile Justice Authority (JJA). The Post Audit staff has shown both competence and proficiency throughout the audit and I sincerely believe as a result, we will come away with improvements in our operations. This audit will help us create and improve the information technology security systems for the agency.

We concur with the audit findings, and progress is being made in addressing the cited deficiencies. We are pleased to advise we have improved processes and that JJA is already more compliant with the findings cited in the audit. We will continue to provide improvements and work toward achieving the goals outlined.

Thank you again for your staff's time and commitment.

Sincerely,

Terri Williams, Acting Commissioner
Kansas Juvenile Justice Authority



Office of the Secretary
401 SW Topeka Boulevard
Topeka, KS 66603-3182

AD ASTRA PER ASPERA
Kansas
Department of Labor

Phone: (785) 296-5000
Ext. 2706
Fax: (785) 368-6294
lana.gordon@dol.ks.gov
www.dol.ks.gov

Lana Gordon, Interim Secretary

Sam Brownback, Governor

November 26, 2012

Scott Frank
Post Auditor
Legislative Division of Post Audit
800 SW Jackson
Suite 1200
Topeka, KS 66612

Dear Scott,

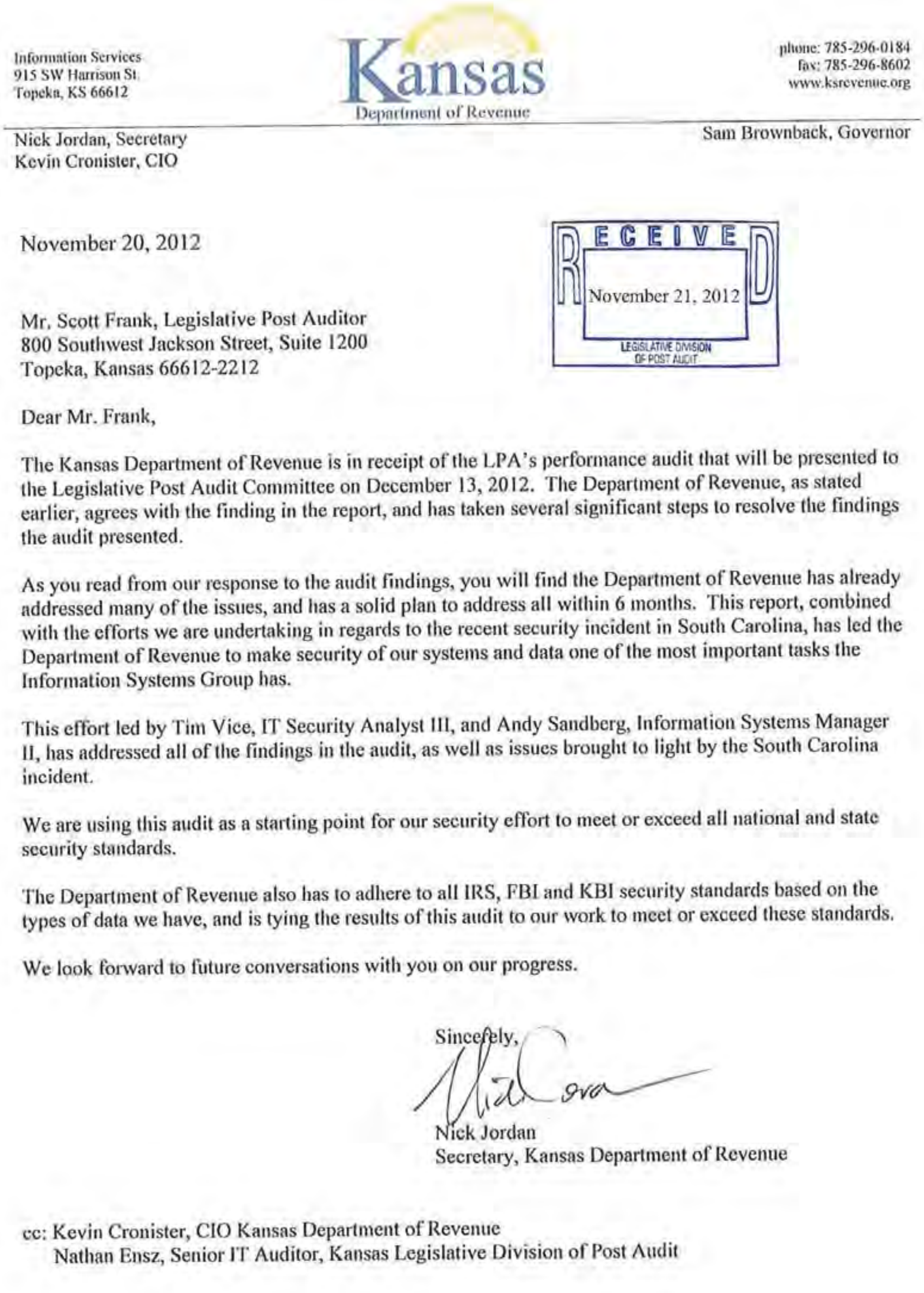
Thank you for the copy of the completed performance audit, *State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY2012)*.

This report, though not specific to any one of the nine agencies audited, is very thorough and informative. We appreciate and believe that IT Security is a high priority. As each agency moves toward more efficient practices and services for Kansas citizens, it will be imperative that we all ensure sensitive data is kept confidential and is not able to be compromised. This can be accomplished by continual education of all state employees regarding IT policies.

Sincerely,

Lana Gordon

Lana Gordon
Interim Secretary



Information Services
915 SW Harrison St.
Topeka, KS 66612

Kansas
Department of Revenue

phone: 785-296-0184
fax: 785-296-8602
www.ksrevenue.org

Nick Jordan, Secretary
Kevin Cronister, CIO

Sam Brownback, Governor

November 20, 2012

Mr. Scott Frank, Legislative Post Auditor
800 Southwest Jackson Street, Suite 1200
Topeka, Kansas 66612-2212

Dear Mr. Frank,

The Kansas Department of Revenue is in receipt of the LPA's performance audit that will be presented to the Legislative Post Audit Committee on December 13, 2012. The Department of Revenue, as stated earlier, agrees with the finding in the report, and has taken several significant steps to resolve the findings the audit presented.

As you read from our response to the audit findings, you will find the Department of Revenue has already addressed many of the issues, and has a solid plan to address all within 6 months. This report, combined with the efforts we are undertaking in regards to the recent security incident in South Carolina, has led the Department of Revenue to make security of our systems and data one of the most important tasks the Information Systems Group has.

This effort led by Tim Vice, IT Security Analyst III, and Andy Sandberg, Information Systems Manager II, has addressed all of the findings in the audit, as well as issues brought to light by the South Carolina incident.

We are using this audit as a starting point for our security effort to meet or exceed all national and state security standards.

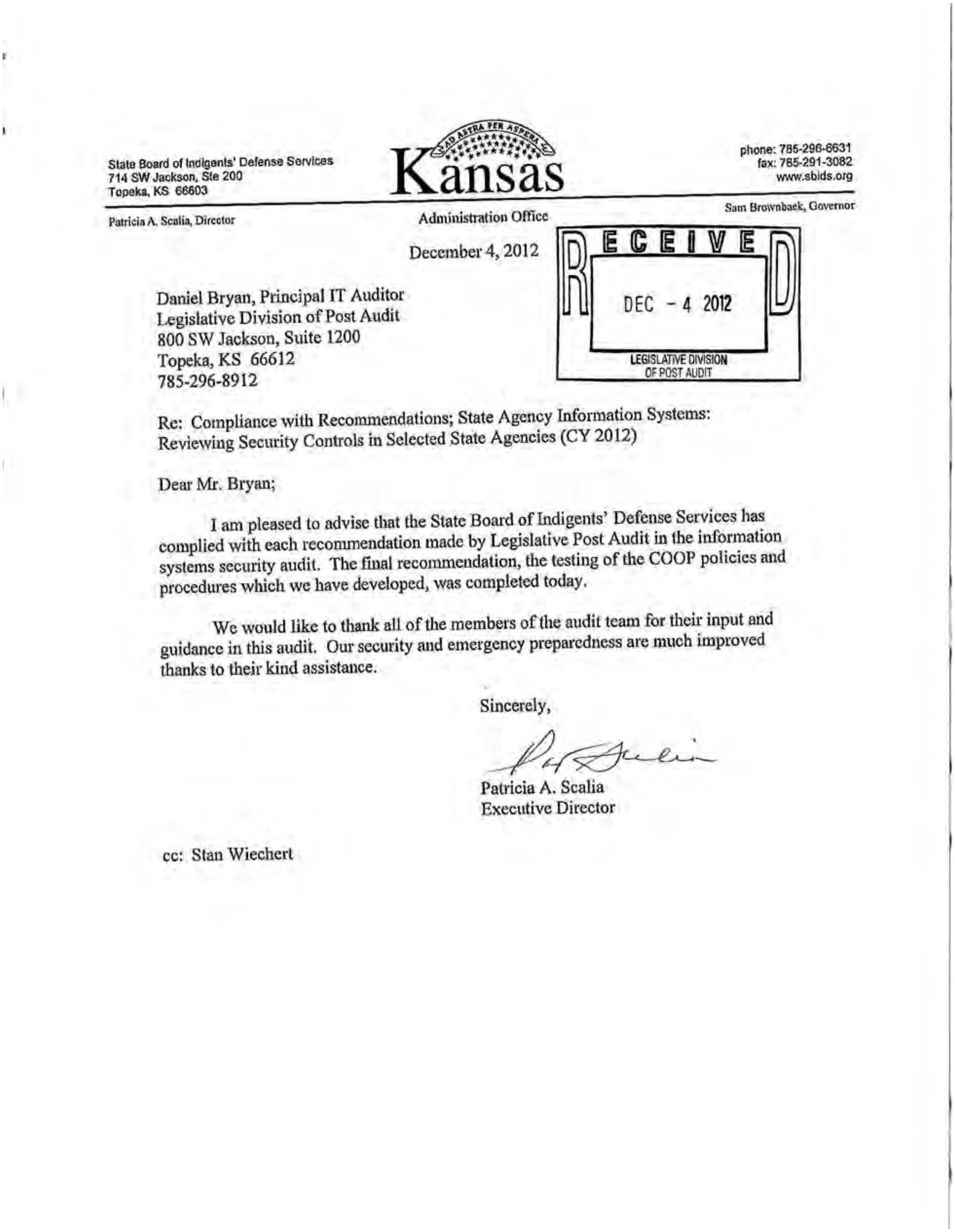
The Department of Revenue also has to adhere to all IRS, FBI and KBI security standards based on the types of data we have, and is tying the results of this audit to our work to meet or exceed these standards.

We look forward to future conversations with you on our progress.

Sincerely,

Nick Jordan
Secretary, Kansas Department of Revenue

cc: Kevin Cronister, CIO Kansas Department of Revenue
Nathan Ensz, Senior IT Auditor, Kansas Legislative Division of Post Audit



State Board of Indigents' Defense Services
714 SW Jackson, Ste 200
Topeka, KS 66603

AD ASTRA PER ASPERA
Kansas

phone: 785-296-6631
fax: 785-291-3082
www.sbids.org

Patricia A. Scalia, Director

Administration Office

Sam Brownback, Governor

December 4, 2012

Daniel Bryan, Principal IT Auditor
Legislative Division of Post Audit
800 SW Jackson, Suite 1200
Topeka, KS 66612
785-296-8912

Re: Compliance with Recommendations; State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2012)

Dear Mr. Bryan;

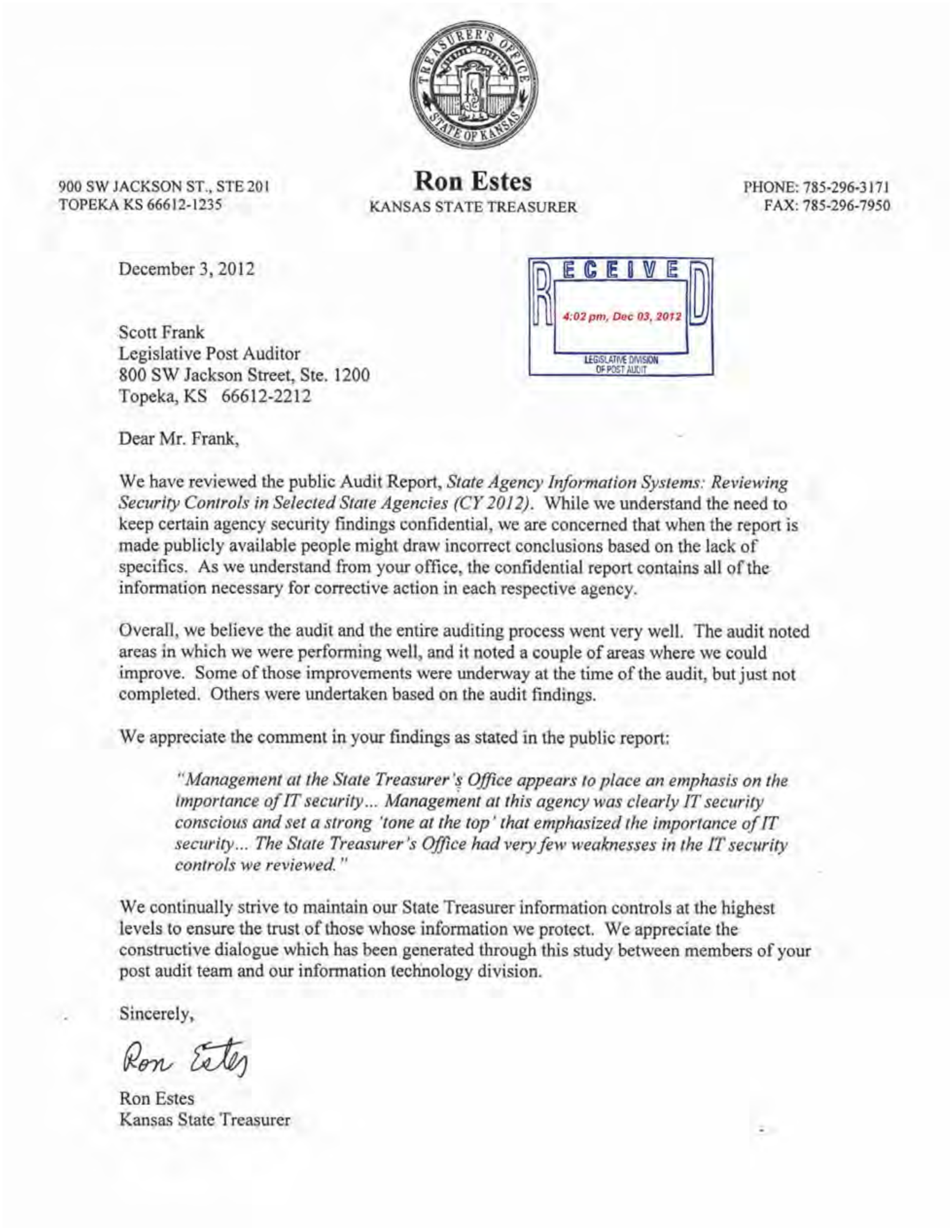
I am pleased to advise that the State Board of Indigents' Defense Services has complied with each recommendation made by Legislative Post Audit in the information systems security audit. The final recommendation, the testing of the COOP policies and procedures which we have developed, was completed today.

We would like to thank all of the members of the audit team for their input and guidance in this audit. Our security and emergency preparedness are much improved thanks to their kind assistance.

Sincerely,

Patricia A. Scalia
Executive Director

cc: Stan Wiechert



900 SW JACKSON ST., STE 201
TOPEKA KS 66612-1235

Ron Estes
KANSAS STATE TREASURER

PHONE: 785-296-3171
FAX: 785-296-7950

December 3, 2012

Scott Frank
Legislative Post Auditor
800 SW Jackson Street, Ste. 1200
Topeka, KS 66612-2212

Dear Mr. Frank,

We have reviewed the public Audit Report, *State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2012).* While we understand the need to keep certain agency security findings confidential, we are concerned that when the report is made publicly available people might draw incorrect conclusions based on the lack of specifics. As we understand from your office, the confidential report contains all of the information necessary for corrective action in each respective agency.

Overall, we believe the audit and the entire auditing process went very well. The audit noted areas in which we were performing well, and it noted a couple of areas where we could improve. Some of those improvements were underway at the time of the audit, but just not completed. Others were undertaken based on the audit findings.

We appreciate the comment in your findings as stated in the public report:

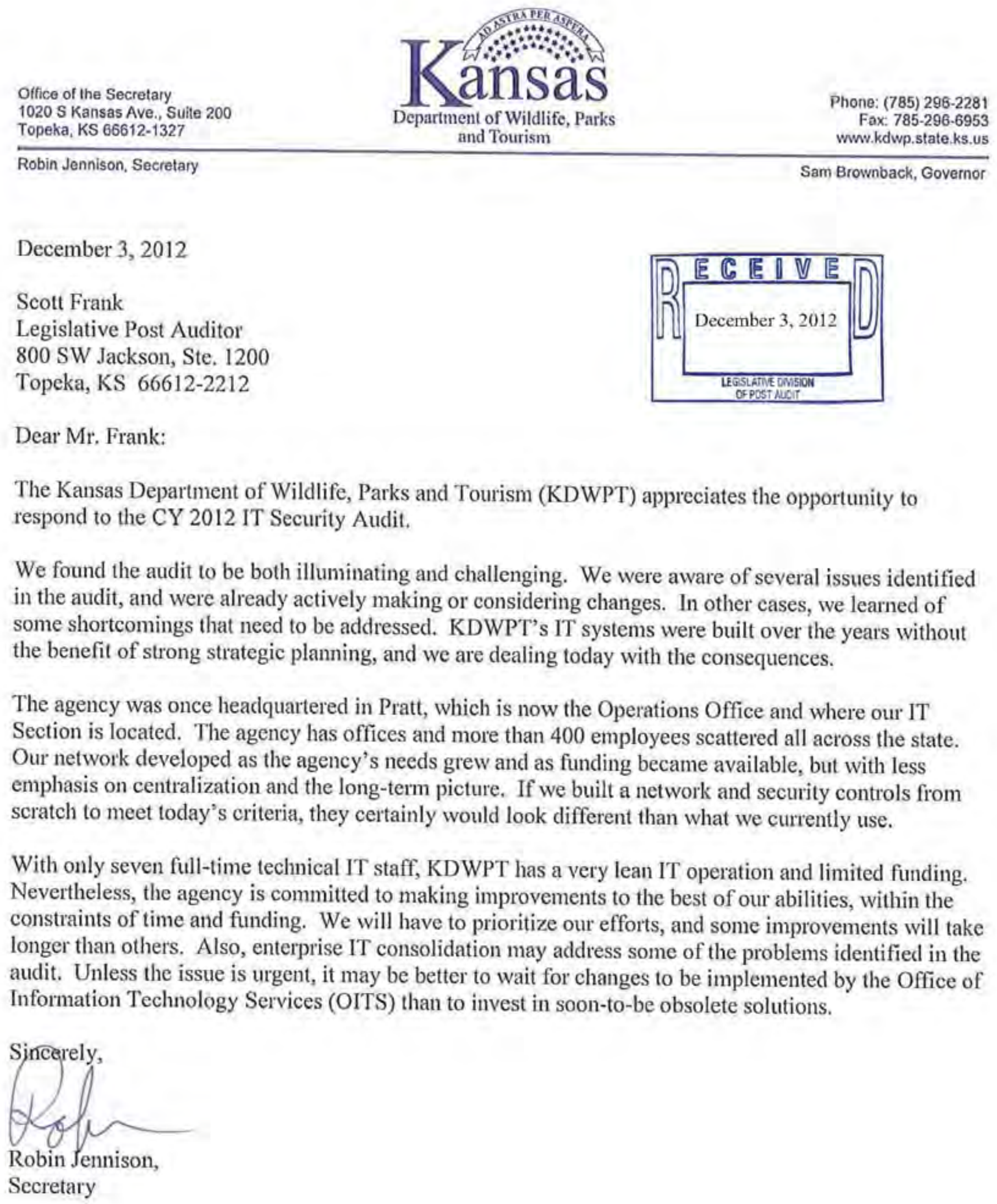
> *"Management at the State Treasurer's Office appears to place an emphasis on the importance of IT security... Management at this agency was clearly IT security conscious and set a strong 'tone at the top' that emphasized the importance of IT security... The State Treasurer's Office had very few weaknesses in the IT security controls we reviewed."*

We continually strive to maintain our State Treasurer information controls at the highest levels to ensure the trust of those whose information we protect. We appreciate the constructive dialogue which has been generated through this study between members of your post audit team and our information technology division.

Sincerely,

Ron Estes

Ron Estes
Kansas State Treasurer



Office of the Secretary
1020 S Kansas Ave., Suite 200
Topeka, KS 66612-1327

AD ASTRA PER ASPERA
Kansas
Department of Wildlife, Parks
and Tourism

Phone: (785) 296-2281
Fax: 785-296-6953
www.kdwp.state.ks.us

Robin Jennison, Secretary

Sam Brownback, Governor

December 3, 2012

Scott Frank
Legislative Post Auditor
800 SW Jackson, Ste. 1200
Topeka, KS 66612-2212

Dear Mr. Frank:

The Kansas Department of Wildlife, Parks and Tourism (KDWPT) appreciates the opportunity to respond to the CY 2012 IT Security Audit.

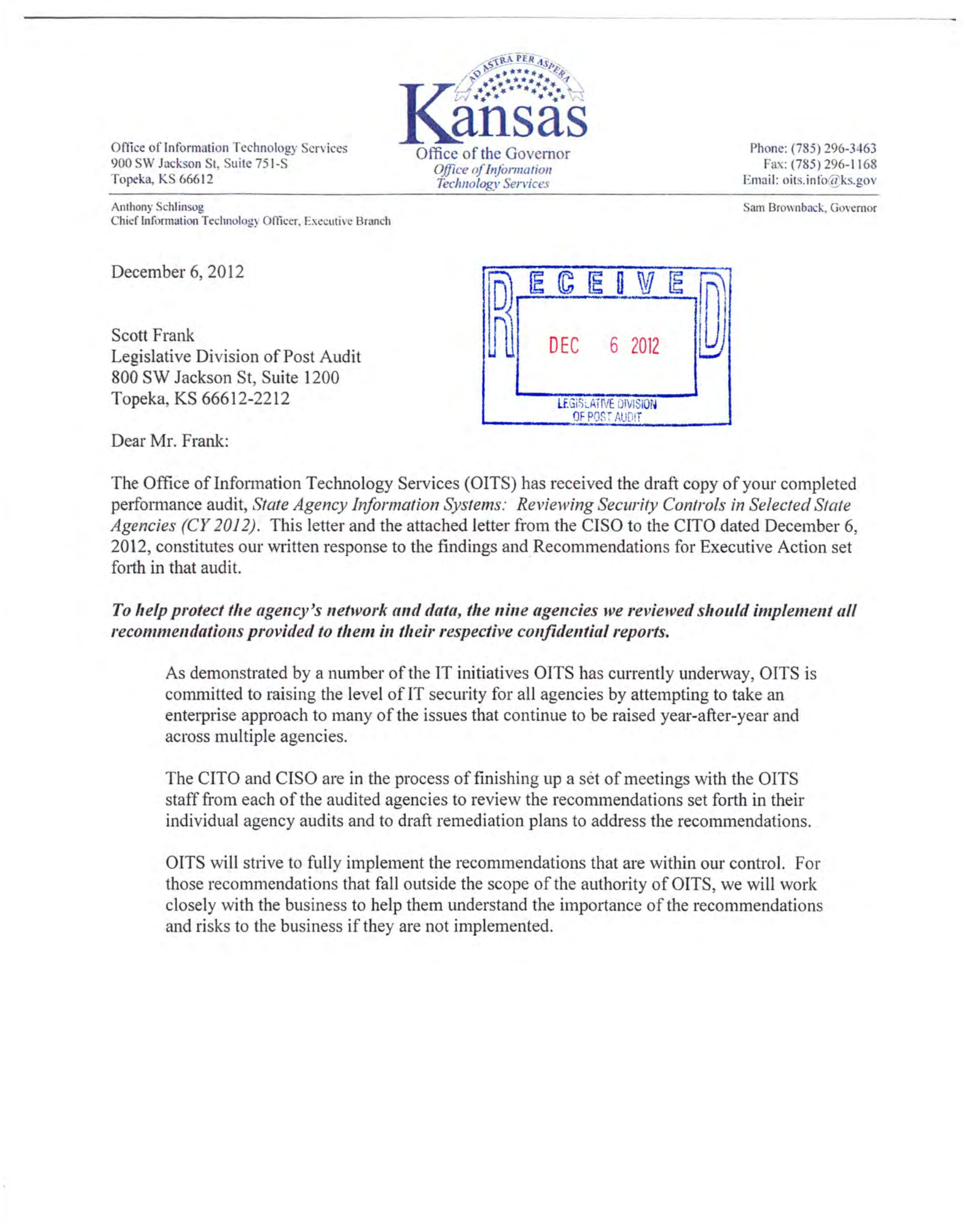
We found the audit to be both illuminating and challenging. We were aware of several issues identified in the audit, and were already actively making or considering changes. In other cases, we learned of some shortcomings that need to be addressed. KDWPT's IT systems were built over the years without the benefit of strong strategic planning, and we are dealing today with the consequences.

The agency was once headquartered in Pratt, which is now the Operations Office and where our IT Section is located. The agency has offices and more than 400 employees scattered all across the state. Our network developed as the agency's needs grew and as funding became available, but with less emphasis on centralization and the long-term picture. If we built a network and security controls from scratch to meet today's criteria, they certainly would look different than what we currently use.

With only seven full-time technical IT staff, KDWPT has a very lean IT operation and limited funding. Nevertheless, the agency is committed to making improvements to the best of our abilities, within the constraints of time and funding. We will have to prioritize our efforts, and some improvements will take longer than others. Also, enterprise IT consolidation may address some of the problems identified in the audit. Unless the issue is urgent, it may be better to wait for changes to be implemented by the Office of Information Technology Services (OITS) than to invest in soon-to-be obsolete solutions.

Sincerely,

Robin Jennison,
Secretary



AD ASTRA PER ASPERA

Kansas

Office of Information Technology Services
900 SW Jackson St, Suite 751-S
Topeka, KS 66612

Office of the Governor
Office of Information Technology Services

Phone: (785) 296-3463
Fax: (785) 296-1168
Email: oits.info@ks.gov

Anthony Schlinsog
Chief Information Technology Officer, Executive Branch

Sam Brownback, Governor

December 6, 2012

Scott Frank
Legislative Division of Post Audit
800 SW Jackson St, Suite 1200
Topeka, KS 66612-2212

Dear Mr. Frank:

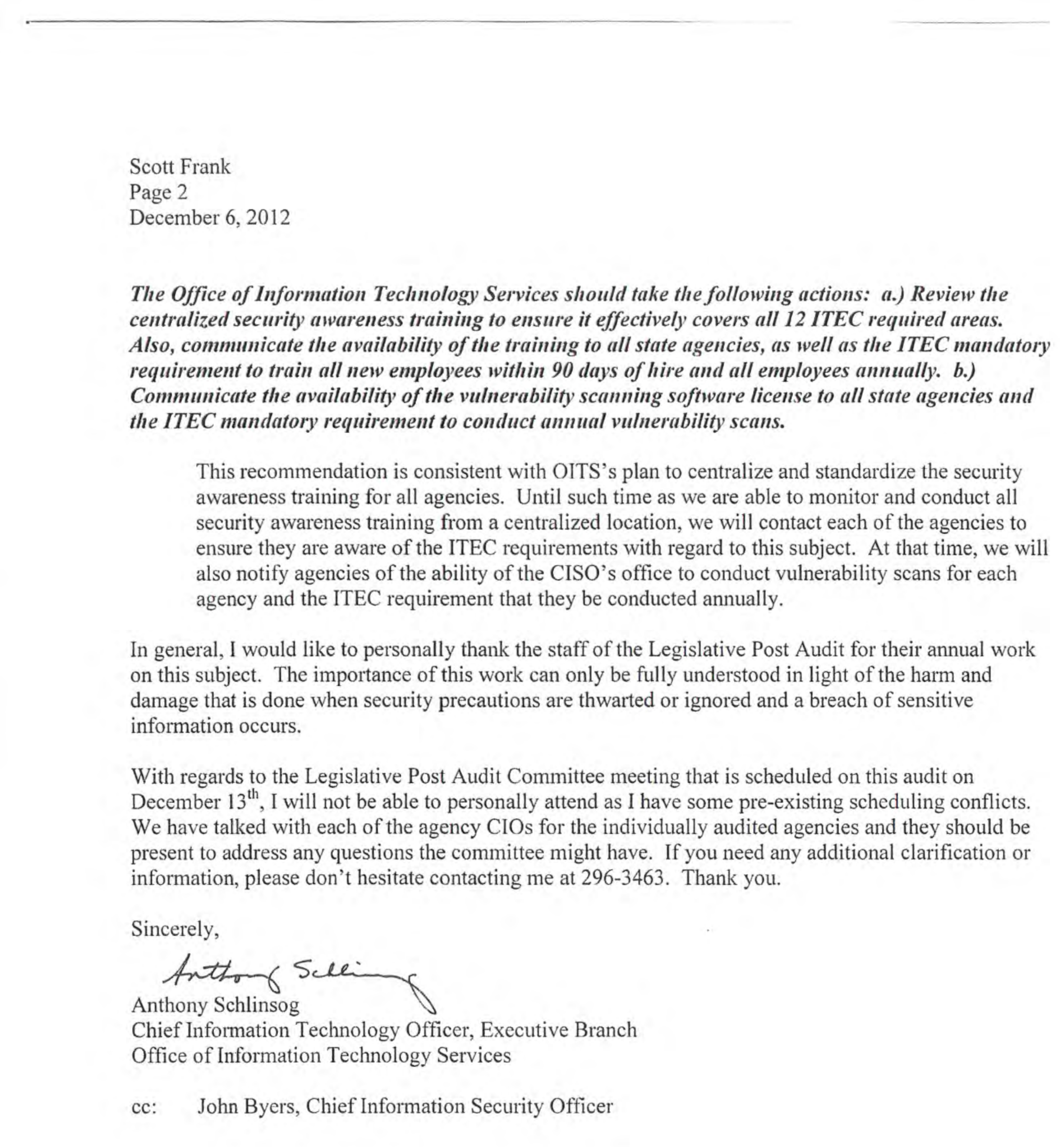
The Office of Information Technology Services (OITS) has received the draft copy of your completed performance audit, *State Agency Information Systems: Reviewing Security Controls in Selected State Agencies (CY 2012)*. This letter and the attached letter from the CISO to the CITO dated December 6, 2012, constitutes our written response to the findings and Recommendations for Executive Action set forth in that audit.

To help protect the agency's network and data, the nine agencies we reviewed should implement all recommendations provided to them in their respective confidential reports.

As demonstrated by a number of the IT initiatives OITS has currently underway, OITS is committed to raising the level of IT security for all agencies by attempting to take an enterprise approach to many of the issues that continue to be raised year-after-year and across multiple agencies.

The CITO and CISO are in the process of finishing up a set of meetings with the OITS staff from each of the audited agencies to review the recommendations set forth in their individual agency audits and to draft remediation plans to address the recommendations.

OITS will strive to fully implement the recommendations that are within our control. For those recommendations that fall outside the scope of the authority of OITS, we will work closely with the business to help them understand the importance of the recommendations and risks to the business if they are not implemented.



Scott Frank
Page 2
December 6, 2012

The Office of Information Technology Services should take the following actions: a.) Review the centralized security awareness training to ensure it effectively covers all 12 ITEC required areas. Also, communicate the availability of the training to all state agencies, as well as the ITEC mandatory requirement to train all new employees within 90 days of hire and all employees annually. b.) Communicate the availability of the vulnerability scanning software license to all state agencies and the ITEC mandatory requirement to conduct annual vulnerability scans.

> This recommendation is consistent with OITS's plan to centralize and standardize the security awareness training for all agencies. Until such time as we are able to monitor and conduct all security awareness training from a centralized location, we will contact each of the agencies to ensure they are aware of the ITEC requirements with regard to this subject. At that time, we will also notify agencies of the ability of the CISO's office to conduct vulnerability scans for each agency and the ITEC requirement that they be conducted annually.

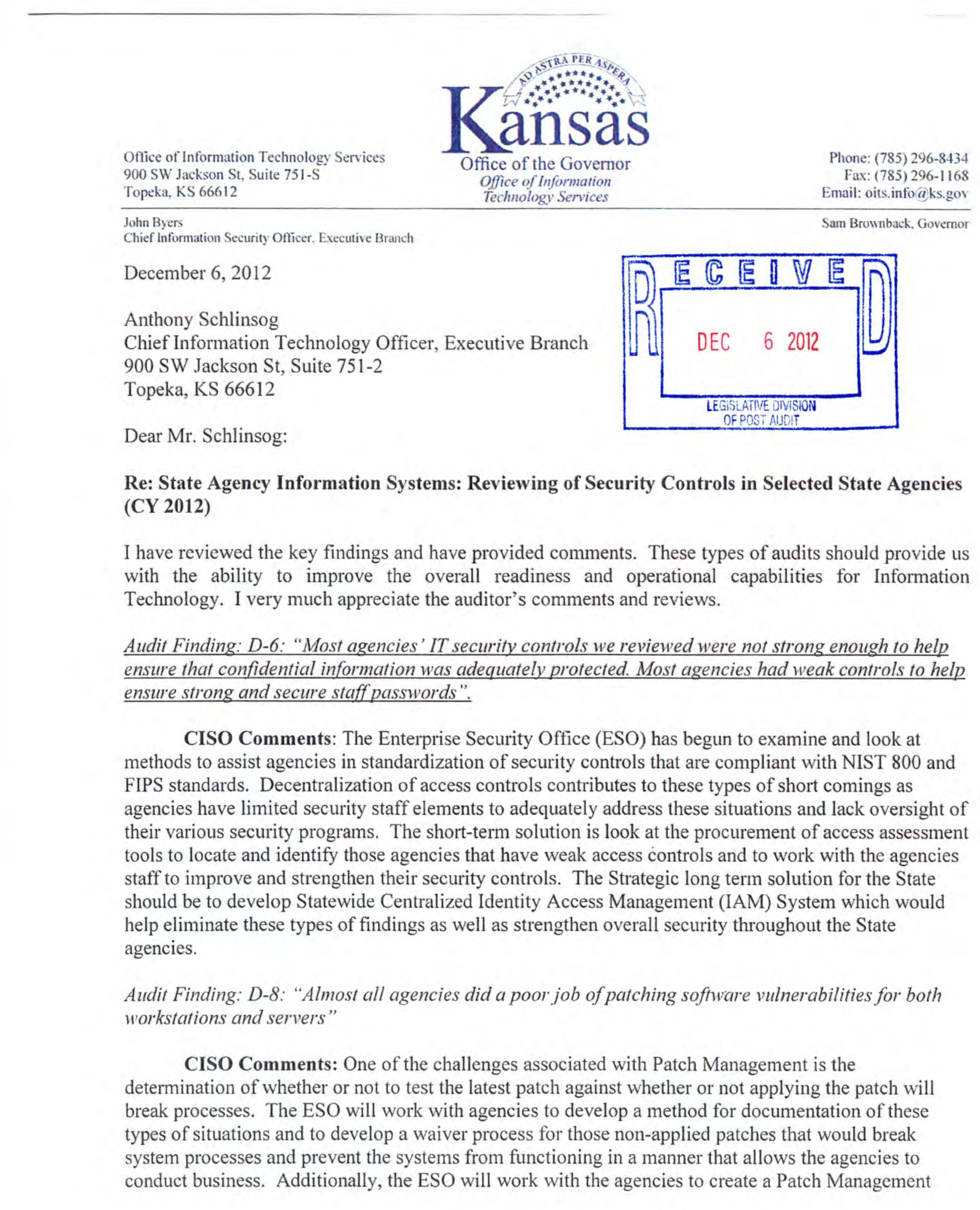
In general, I would like to personally thank the staff of the Legislative Post Audit for their annual work on this subject. The importance of this work can only be fully understood in light of the harm and damage that is done when security precautions are thwarted or ignored and a breach of sensitive information occurs.

With regards to the Legislative Post Audit Committee meeting that is scheduled on this audit on December 13th, I will not be able to personally attend as I have some pre-existing scheduling conflicts. We have talked with each of the agency CIOs for the individually audited agencies and they should be present to address any questions the committee might have. If you need any additional clarification or information, please don't hesitate contacting me at 296-3463. Thank you.

Sincerely,

Anthony Schlinsog
Chief Information Technology Officer, Executive Branch
Office of Information Technology Services

cc: John Byers, Chief Information Security Officer



AD ASTRA PER ASPERA

Kansas

Office of Information Technology Services
900 SW Jackson St, Suite 751-S
Topeka, KS 66612

Office of the Governor
Office of Information
Technology Services

Phone: (785) 296-8434
Fax: (785) 296-1168
Email: oits.info@ks.gov

John Byers
Chief Information Security Officer, Executive Branch

Sam Brownback, Governor

December 6, 2012

Anthony Schlinsog
Chief Information Technology Officer, Executive Branch
900 SW Jackson St, Suite 751-2
Topeka, KS 66612

Dear Mr. Schlinsog:

Re: State Agency Information Systems: Reviewing of Security Controls in Selected State Agencies (CY 2012)

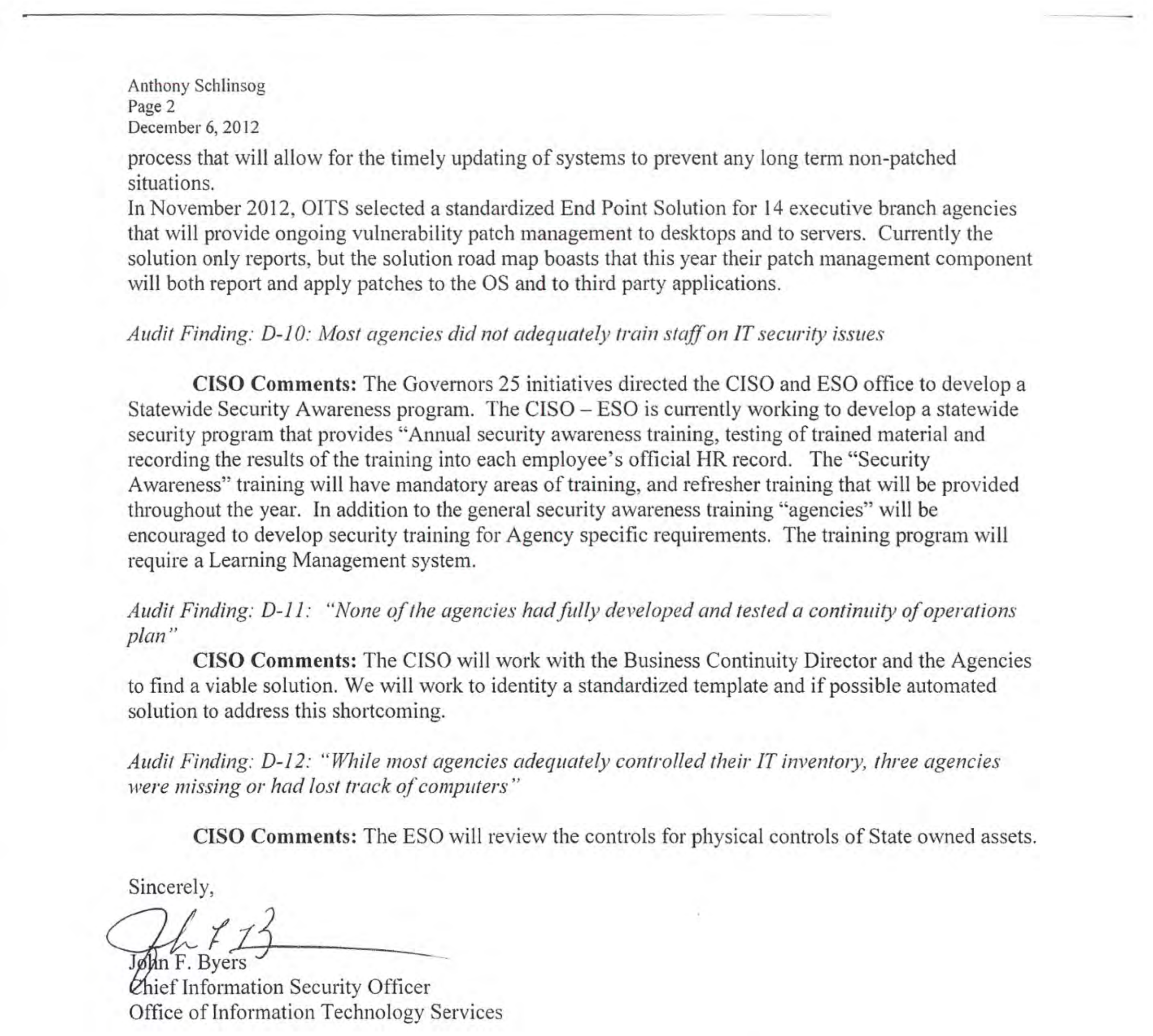
I have reviewed the key findings and have provided comments. These types of audits should provide us with the ability to improve the overall readiness and operational capabilities for Information Technology. I very much appreciate the auditor's comments and reviews.

Audit Finding: D-6: "Most agencies' IT security controls we reviewed were not strong enough to help ensure that confidential information was adequately protected. Most agencies had weak controls to help ensure strong and secure staff passwords".

CISO Comments: The Enterprise Security Office (ESO) has begun to examine and look at methods to assist agencies in standardization of security controls that are compliant with NIST 800 and FIPS standards. Decentralization of access controls contributes to these types of short comings as agencies have limited security staff elements to adequately address these situations and lack oversight of their various security programs. The short-term solution is look at the procurement of access assessment tools to locate and identify those agencies that have weak access controls and to work with the agencies staff to improve and strengthen their security controls. The Strategic long term solution for the State should be to develop Statewide Centralized Identity Access Management (IAM) System which would help eliminate these types of findings as well as strengthen overall security throughout the State agencies.

Audit Finding: D-8: "Almost all agencies did a poor job of patching software vulnerabilities for both workstations and servers"

CISO Comments: One of the challenges associated with Patch Management is the determination of whether or not to test the latest patch against whether or not applying the patch will break processes. The ESO will work with agencies to develop a method for documentation of these types of situations and to develop a waiver process for those non-applied patches that would break system processes and prevent the systems from functioning in a manner that allows the agencies to conduct business. Additionally, the ESO will work with the agencies to create a Patch Management



process that will allow for the timely updating of systems to prevent any long term non-patched situations.
In November 2012, OITS selected a standardized End Point Solution for 14 executive branch agencies that will provide ongoing vulnerability patch management to desktops and to servers. Currently the solution only reports, but the solution road map boasts that this year their patch management component will both report and apply patches to the OS and to third party applications.

Audit Finding: D-10: Most agencies did not adequately train staff on IT security issues

CISO Comments: The Governors 25 initiatives directed the CISO and ESO office to develop a Statewide Security Awareness program. The CISO – ESO is currently working to develop a statewide security program that provides "Annual security awareness training, testing of trained material and recording the results of the training into each employee's official HR record. The "Security Awareness" training will have mandatory areas of training, and refresher training that will be provided throughout the year. In addition to the general security awareness training "agencies" will be encouraged to develop security training for Agency specific requirements. The training program will require a Learning Management system.

Audit Finding: D-11: "None of the agencies had fully developed and tested a continuity of operations plan"

CISO Comments: The CISO will work with the Business Continuity Director and the Agencies to find a viable solution. We will work to identity a standardized template and if possible automated solution to address this shortcoming.

Audit Finding: D-12: "While most agencies adequately controlled their IT inventory, three agencies were missing or had lost track of computers"

CISO Comments: The ESO will review the controls for physical controls of State owned assets.

Sincerely,

John F. Byers
Chief Information Security Officer
Office of Information Technology Services