John Keel, CPA
State Auditor

An Audit Report on

Selected Information Technology Controls at the Winters Data Centers

July 2011

Report No. 11-033

State Auditor's Office

John Keel, CPA
State Auditor

An Audit Report on

Selected Information Technology Controls at the Winters Data Centers

SAO Report No. 11-033
July 2011

Overall Conclusion

Weaknesses in the Health and Human Services Commission's (Commission) logical and physical access controls over information technology at the Winters Data Centers could result in damage to equipment or unauthorized access to and the loss of confidential data and systems.

Health and human services agencies rely on mission-critical systems housed at the Winters Data Centers to carry out their responsibilities. The weaknesses auditors identified increase the risk of unauthorized access to or loss of confidential data.

While the Commission has comprehensive information security policies and procedures, it does not enforce those policies and procedures consistently. It also does not comply with Texas Administrative Code requirements for passwords, user access, and disaster recovery plan testing. On at least 70 percent of the databases and servers that auditors tested, the Commission's password implementation did not meet information security standards established for state data centers.[1]

Background Information

Under the requirements of House Bill 1516 (79th Legislature, Regular Session), in 2006 the Department of Information Resources contracted with IBM to migrate existing automated systems at several state agencies into consolidated data centers.

IBM then formed Team for Texas, a group of contractors that was required to perform ongoing operations and maintenance and to provide disaster recovery services from March 2007 through August 2014.

This audit focused on information technology controls at the Winters Data Centers, which encompass four distinct data centers that host health and human services agencies information resources. The Winters Data Centers include:

- Three data centers (Southeast, Northwest, and Texas Integrated Eligibility Redesign System or TIERS) under the responsibility of the Commission.
- One data center (Southwest) managed by the Department of State Health Services.

Team for Texas provides ongoing operations and maintenance for the servers in the above data centers, but the Commission and health and human services agencies are still responsible for ensuring the security of their information technology.

The Commission does not adequately monitor vendors that provide certain operation and maintenance services at the Winters Data Centers. The outsourcing of certain operation and maintenance services to vendors, combined with the Commission's organizational structure, has resulted in significant challenges. For example:

- A system of shared responsibilities for information technology now exists among vendors, the Commission, and health and human services agencies. Staff at the Commission and health and human service agencies have not fully embraced those shared responsibilities. The complex system of responsibilities requires greater oversight by the Commission and health and human services agencies.

[1] See additional details on those standards in Chapter 1 of this report.

This audit was conducted in accordance with Texas Government Code, Section 321.0132.

For more information regarding this report, please contact Ralph McClendon, Audit Manager, or John Keel, State Auditor, at (512) 936-9500.

- The outsourcing of certain services, coupled with a lack of oversight by the Commission and health and human services agencies, has resulted in instances in which staff were unaware of services and user accounts on their mission-critical systems.

While vendors perform certain services at the Winters Data Centers, this does not relieve the Commission or the health and human services agencies of their responsibility for ensuring that data and systems are properly secured.

Key Points

Auditors identified weaknesses in user access, physical security, and disaster recovery planning.

User Access. The Commission does not adequately secure access to servers, databases, and systems. For example, auditors identified weaknesses in password settings, weaknesses in user access management, and the absence of a regular user access review process.

Physical Security. Physical security controls at the Winters Data Centers are inadequate. For example, at the beginning of this audit, the doors for two of the data centers within the Winters Data Centers were not locked because they did not have working security card readers (the Commission corrected that issue after auditors brought it to the Commission's attention). In addition, the process for reviewing the appropriateness of physical access to the Winters Data Centers is ineffective, and one fire suppression system has not passed inspection.

Disaster Recovery Planning. Disaster recovery plans for the Winters Data Centers are inadequate. System documentation does not contain sufficient detail to facilitate recovery of systems and data; however, data backups are scheduled and routinely performed.

The weaknesses auditors identified increase the risk of service interruption and loss or theft of data.

Any of the weaknesses individually places data and systems at risk. When combined, these weaknesses significantly increase the risk that services could be interrupted and the data could be unintentionally or deliberately lost.

The weaknesses auditors identified could affect systems that were not audited.

This audit focused on seven mission-critical systems that are housed at the Winters Data Centers, but the weaknesses auditors identified could affect other systems that were not audited. Auditors selected the seven systems based on a risk assessment of mission-critical systems. The seven systems are used by the Commission, the Department of Aging and Disability Services, and the Department of State Health Services.

To minimize the risk associated with public disclosure, this report does not identify the systems audited, but auditors provided the Commission and health and human services agencies with detailed audit results and other less significant issues separately in writing.

Summary of Management's Response

The Commission agreed with the recommendations in this report.

Summary of Objectives, Scope, and Methodology

The audit objectives were to:

- Determine whether selected information technology controls at the Winters Data Centers operate to protect and support the information technology assets of the State's health and human services agencies.
- Determine whether selected information technology controls at selected health and human services agencies operate to protect state information technology assets.

The audit scope included the health and human service agency facilities where state technology assets are located, with a focus on the Winters Data Centers facilities in the Austin health and human services complex. The scope of this audit specifically covered information technology systems located on servers at the Winters Data Centers based on a risk assessment of confidential information in the systems and whether the system was identified by the agency as critical to operations. Audit work included a review of logical security controls related to user access and passwords; a review of physical security controls at the Winters Data Centers; and controls related to disaster recovery plans, operations, and security training at selected health and human services agencies. The Department of Assistive and Rehabilitative Services and the Department of Family and Protective Services were not included in logical security controls work because those agencies did not identify systems as critical in the Winters Data Centers.

The audit methodology included conducting an assessment of logical security controls for seven systems housed in the Winters Data Centers by verifying the appropriateness of user access, assessing the strength of password controls, and assessing the process for periodic user access reviews. Auditors interviewed staff at the Commission, health and human services agencies, the Department of Information Resources, and the Texas Facilities Commission. Auditors also conducted multiple walkthroughs of the Winters Data Centers to assess physical security, environmental security, and alternate and uninterruptible power supply. Auditors also verified the capability of the Commission to meet state disaster recovery requirements for systems that are housed in the Winters Data Centers.

This audit did not rely on agency data for the purpose of making conclusions. However, auditors used data from the State Data Center Centralized Master Database to assess risk at the Winters Data Centers.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

The Commission Does Not Adequately Secure User Access to Servers, Databases, and Systems

Auditors identified significant weaknesses in the Health and Human Services Commission's (Commission) controls at all access levels audited for the seven systems tested. Those weaknesses place the audited systems at risk of unauthorized access and loss of data. The 7 systems audited are supported by 25 servers and 10 databases, and auditors identified weaknesses in user access and passwords at the server, database, and system levels.

While auditors identified significant weaknesses in user access, they identified no weaknesses in segregation of duties in controls related to access.

Chapter 1-A

The Commission Does Not Consistently Ensure That Password Controls Are Adequate

Significant weaknesses in access controls exist at all levels tested. Controlling access is necessary for any information resource. If unauthorized entities gain access to data and systems, this can harm the confidentiality, integrity, and availability of data and systems and may result in loss of service, loss of trust, and liability.

For the servers, databases, and systems tested, auditors identified instances in which password requirements did not meet the standards established by Commission policies, Texas Administrative Code requirements, and state data center information security controls (see text box). Those weaknesses exist because of software limitations and a lack of adequate oversight and enforcement of policies and standards. Specifically:

Summary of Information Security Standards

- Title 1, Texas Administrative Code, Chapter 202, specifies security standards for all state agencies.
- The Commission's *Enterprise Information Security Standards and Guidelines* specifies standards for all authorized users (including contractors and agency staff) of health and human services information resources.
- Team for Texas's *Information Security Controls for State of Texas Data Center Services* specifies security standards, policies, and controls.

- **Server Level.** The Commission's enforcement of its password policies across servers has been inconsistent. Of the 25 servers tested:
  - Twenty-one servers (84.0 percent) have weak password settings.
  - One server (4.0 percent) does not have any default password settings. That server has 68 user accounts, 37 of which do not enforce password requirements. Of those 37 user accounts, 21 have no access limitations and no password requirements. The remaining 16 user accounts have no password requirements, but the user has to be physically present at the server to log in.

- Three servers (12.0 percent) comply with password policies; one of those three servers meets best practices but does not comply with Commission policy.

The Commission also has filed six exceptions to waive compliance with some of the password requirements on server accounts related to the systems audited. Four of the exceptions expired in April 2011 and two are pending approval. Exceptions are an acknowledgement that weak password controls exist. The approval of an exception does not mitigate the risk that passwords could be compromised. The Commission's exception documents state that "there is an increased risk of the password being compromised if this exception is granted. If this were to happen, an attacker could temporarily disable these systems." The exception documents also note that "user accounts which use weak passwords are more susceptible to brute force attack."

- **Database Level.** The Commission has not enforced its password standards across databases. Of the 10 databases associated with the systems tested, 7 do not meet the Commission's password standards.

- **System Level.** Controls for six of the seven systems tested complied with standards for password composition. The remaining system tested met the specific standard for changing passwords after a certain time period, but it did not comply with other password standards.

Recommendation

The Commission should ensure that password controls for servers, databases, and systems comply with policies, Texas Administrative Code requirements, and state data center information security controls.

Management's Response

HHSC, in collaboration with DADS and DSHS, will develop and implement procedures to ensure that password controls for servers, databases, and systems comply with policies, Texas Administrative Code requirements, and state data center information security controls. Areas that these processes will address include, but are not limited to, strong, complex passwords and password expiration. These processes will reduce or eliminate the need for information security control (ISEC) exceptions.

Estimated Completion Date:

Procedures will be in place no later than December 30, 2011

Title of Responsible Person:

Deputy CIO, HHSC

Chapter 1-B

The Commission Does Not Promptly Disable Accounts with Inappropriate Access

The Commission has not disabled some accounts with inappropriate access to systems under its direct control in a timely manner. In addition, the Commission has not demonstrated adequate oversight of vendors that manage accounts on servers and databases. Inadequate management of server, database, and system accounts places data at risk of misuse, loss, or theft.

Certain "privileged" accounts associated with individuals whose employment has been terminated and contractor staff who are no longer providing services are still active on the servers, databases, and systems. In addition, multiple users share generic accounts, which removes accountability for a particular user's actions. For example:

Privileged Accounts

A privileged account should be assigned to the system administrator who is responsible for maintaining a server. These accounts have the highest privileges on the server.

- **Server Level.** Of the 1,277 privileged accounts tested, auditors identified 116 accounts with inappropriate access. For example, as of March 2011, 40 individuals whose employment had been terminated as long ago as April 2007 still had active privileged accounts on at least 1 of the 25 servers tested. In addition, 25 former Team for Texas[2] contractors whose services had been terminated as long ago as July 2007 still had 67 active privileged accounts on 22 of the 25 servers tested.

- **Database Level.** The 10 databases associated with the systems audited had 47 privileged accounts. Of those 47 accounts, auditors identified 5 inappropriate accounts that affected 3 databases:

  - One account was assigned to a contractor whose services had been terminated in May 2009.

  - One current employee had an inappropriate privileged account on a

Inappropriate Accounts

For purposes of this audit, inappropriate accounts include:

- An account that belongs to an individual whose employment has been terminated or a vendor or contractor that is no longer providing services.
- A system account that is no longer required or used.
- An account with excessive access when compared to a user's job duties.
- A generic account shared by multiple users.

[2] Team for Texas is the group of contractors to which the Department of Information Resources outsourced certain operation and maintenance services at the Winters Data Centers.

database.

- Three generic accounts were shared by employees and multiple vendors.

- **System Level.** Of the 337 accounts with administrator roles that auditors tested, 12 user accounts were assigned to individuals whose employment had been terminated or whose responsibilities had changed. In addition, six active system accounts tested were inappropriate because they were no longer being used.

Recommendations

The Commission should:

- Disable employees' and contractors' access promptly upon termination of employment or services.
- Ensure that user access privileges align with job duties, and promptly modify user access privileges when job duties change.
- Disable unused system accounts in a timely manner.
- Ensure that accounts are unique and are not shared.

Management's Response

HHSC will, in collaboration with DADS and DSHS, and in consultation with management at DADS State Supported Living Centers and DSHS State Hospitals, develop and implement procedures to disable employees' and contractors' access promptly upon termination of employment or services; ensure that user access privileges align with job duties and promptly modify users access privileges when job duties change; disable unused system accounts in a timely manner; and ensure that accounts are unique and are not shared.

Estimated Completion Date:

Procedures will be developed no later than September 30, 2011, and implemented no later than December 30, 2011

Title of Responsible Person:

Deputy CIO, HHSC

Chapter 1-C

The Commission Does Not Periodically Review User Access

Periodic review of user access is important in identifying possible unauthorized access. Lack of a strong user access review process increases the risk of unauthorized access to systems and creates an opportunity for fraud.

The Commission has a policy that requires account access levels to be reviewed for appropriateness at least every 12 months. The Commission's policies also require that all maintenance accounts and accounts established for employees, contractors, consultants, interns, and vendors be disabled immediately upon termination or completion of the contract period. However, the Commission does not consistently enforce those policies.

Auditors identified the following weaknesses in the user access review process:

- **Server Level.** The Commission does not have evidence that it regularly reviews user access for any of the 25 servers tested. For five servers tested, the Commission asserted that it regularly reviewed user access; however, it was unable to provide evidence of those reviews. Auditors identified user access issues on 23 of the 25 servers tested, including the 5 servers for which the Commission asserted it performed regular reviews.

- **Database Level.** The Commission does not regularly review user access for 8 of the 10 databases tested. For the two databases on which the Commission asserted that it conducted periodic reviews, the Commission could not provide evidence to support that assertion, and auditors were not able to obtain evidence of a periodic review; however, auditors did not identify user access issues on those two databases.

- **System Level.** The Commission does not regularly review user access for five of the seven systems tested; however, two of those five systems have mitigating controls for inactive accounts. While the Commission does review user access for two systems, one of those reviews was ineffective.

Recommendation

The Commission should conduct and document regular reviews of user accounts for all servers, databases, and systems and promptly disable all inappropriate accounts it identifies.

Management's Response

HHSC will, in collaboration with DADS and DSHS, develop and implement procedures for conducting and documenting regular reviews of user accounts

for all servers, databases, and systems, and will promptly disable all inappropriate accounts identified by reviews. Reviews will be completed at least annually.

Estimated Completion Date:

The first annual review will be completed no later than December 30, 2011

Title of Responsible Person:

Deputy CIO, HHSC

Chapter 2

The Commission Should Improve Physical Security and Environmental Controls at the Winters Data Centers

Improvements in both physical security and environmental controls at the Winters Data Centers are necessary to ensure that information technology assets are protected. Auditors identified weaknesses in the controls over physical access to the building and procedures to protect the Winters Data Centers from environmental hazards such as fire.

Data Centers within the Winters Data Centers

The Winters Data Centers include four separate data centers:

- The Southeast Data Center hosts mission-critical systems that support programs for the Health and Human Services Commission, the Department of Aging and Disability Services, and the County Information Resources Agency.
- The Northwest Data Center hosts mission-critical systems, including those that support clients in state hospitals and state-supported living centers.
- The Texas Integrated Eligibility Redesign System (TIERS) Data Center hosts the mission-critical integrated eligibility system that supports health and human services programs, such as the Supplemental Nutrition Assistance Program. Construction of the TIERS Data Center was completed in 2010.
- The Southwest Data Center hosts information resources for the Department of State Health Services.

The Texas Facilities Commission (TFC) provides a number of services to the Winters Data Centers, including maintenance and repair services, ensuring the delivery of utilities, physical security, and managing the security card access system that grants individuals physical access. According to a Commission internal audit report, the Commission is responsible for coordinating with the TFC and communicating facility needs to both health and human services agencies' decision makers and the TFC.

The Commission has an interagency contract with the TFC, but that contract does not adequately define the physical security responsibilities of each agency (see Appendix 3 for the interagency contract). The absence of a detailed agreement outlining the responsibilities for providing specific services, combined with a lack of management oversight, may have contributed to the weaknesses in physical security and environmental controls discussed below.

The Commission should improve physical security at the Winters Data Centers.

The process for reviewing the appropriateness of physical access to the Winters Data Centers is ineffective. Health and human services agencies perform periodic reviews of physical access, but they do not always ensure that the TFC removes access in a timely manner. For example, in September 2010, the Department of State Health Services requested the removal of access for 39 security cardholders; however, 8 of those security cardholders still had access as of April 2011.

In addition, the health and human services agencies responsible for monitoring physical access to the Winters Data Centers were unable to obtain reports of user access for their areas of responsibility from December 2010 to March 2011 because of deficiencies in the security card access system. As a result, for four months, those agencies were unable to determine whether individuals who were no longer employed still had access to the Winters Data Centers.

Auditors also were unable to obtain from the TFC or the Commission's Winters Data Centers manager a complete list of individuals with security card access to the Winters Data Centers. The security cardholder list that auditors obtained more than a month after their initial request was incomplete and contained inaccurate information. For example, one data center manager was not included on the list of individuals with access, and auditors identified several individuals for whom the list specified an incorrect agency as their employer. Commission and agency staff also do not review the security card information in the access system to ensure its accuracy, which could result in inappropriate access being granted.

The process for removing individuals who no longer need access to the Winters Data Centers also is not effective. Three (9.4 percent) of 32 individuals tested whose employment had been terminated still had physical access to the Winters Data Centers. In addition, one former contractor still had physical access to the Winters Data Centers.

At the beginning of this audit, the doors for two of the data centers within the Winters Data Centers were not locked because two security card readers that controlled access were not working. The security card readers were repaired after auditors brought this matter to the Commission's attention. The Commission and the TFC use a work order system to track any reported repair requests. According to the TFC, the malfunctioning security card readers were not reported or entered into the work order system after the problem was identified, and there was not a record of the repair of those security card readers. This suggests that the work order system is not used consistently, which could result in a physical security issue not being addressed.

The Commission should improve environmental controls at the Winters Data Centers.

Monitoring and inspection of the fire suppression systems and handheld fire extinguishers at the Winters Data Centers is inadequate. At the time of this audit, handheld extinguishers in all of the data centers within the Winters Data Centers had not been inspected in more than a year.

The fire suppression system for one of the data centers within the Winters Data Centers has been disconnected since August 2010, when it failed inspection. In addition, a safety inspection report from the State Fire Marshal's office dated February 2011 indicated that the fire suppression systems in the Northwest Data Center and Southeast Data Center each had a "red tag"[3] dated August 2010. According to the TFC's property manager, fire suppression systems in those two data centers have not been tested because the health and human services agencies do not want to schedule the down time necessary to conduct a test.

[3] According to Title 28, Texas Administrative Code, Section 34.722 (a), a red tag indicates that a fire protection system has an impairment that constitutes an emergency impairment as defined by the National Fire Protection Association.

Auditors requested a copy of the most recent fire inspection of the Winters Data Centers. The only inspection report provided, which was dated August 2010, included an inspection of only the Northwest Data Center. No fire inspections reports were available for the other data centers within the Winters Data Centers. Commission facilities management staff are not notified when fire inspections are conducted at the Winters Data Centers.

Certain controls partially mitigate the weaknesses discussed above.

The weaknesses in physical security and environmental controls discussed above are partially mitigated by the following:

- Security guards for the Winters Data Centers receive mandatory training in security policies and procedures.

- The process for granting visitor access to the Winters Data Centers is effective and working as intended. Auditors observed this process during multiple visits and also tested a sample of visitor logs covering a one-year period. However, Commission management does not review the visitor logs as required by the Commission's policy.

- To compensate for the lack of a fire suppression system, security guards are required to physically inspect the Northwest Data Center every two hours for signs of a fire.

Recommendations

The Commission should:

- Ensure that its interagency contract with the TFC describes the specific services for which each agency is responsible with regard to the Winters Data Centers.

- Work with all health and human services agencies and the TFC to conduct and document routine periodic reviews of security cardholders with physical access to the Winters Data Centers. This review should include a determination of the appropriateness of each security cardholder's access.

- Review whether the initial establishment of security cardholder access for the Winters Data Centers is performed in accordance with documentation authorizing that access.

- Ensure that handheld fire extinguishers at the Winters Data Centers are inspected regularly and that a copy of the inspection report is provided to management.

- Evaluate the benefit of testing the fire suppression systems in the Winters Data Centers that are red-tagged to determine whether the systems are working as intended, or quantify the cost of making necessary repairs.

- Implement a process to review the visitor logs for the Winters Data Centers as required by Commission policy.

Management's Response

1. The existing interagency contract for the Winters Data Center will expire on August 31, 2011. As Facility Management and Leasing collaborates with the Texas Facilities Commission to execute a new interagency contract, it will ensure that the contract includes a detailed statement of responsibilities.

2. Facility Management and Leasing has assigned an interim on-site Property Manager to Building C. A new Property Manager position is posted and closes June 20, 2011. When that position is filled, the incumbent will be assigned to Building C as the permanent on-site facility manager. The Property Manager will be responsible for coordinating administration of the security card process with Texas Facilities Commission, including periodic reviews of cardholders and ensuring that changes to security access are done in a timely manner.

3. The Property Manager will ensure that changes made to security access reflect what has been approved on Form 9124.

4. The Property Manager will, with the assistance of Texas Facilities Commission, ensure fire extinguishers are inspected and properly tagged and that any replacements or repairs are completed in a timely manner.

5. The Property Manager will work with the Texas Facilities Commission to evaluate testing of red-tagged fire suppression systems and report the results of those evaluations or tests to management.

6. The Property Manager will periodically review the visitor logs to ensure visitors sign out when leaving the building. The Property Manager will work with the Texas Facilities Commission to ensure that security guards inform visitors at sign-in that they must sign out when leaving.

Estimated Completion Date:

1. September 1, 2011

2. August 1, 2011

3. August 1, 2011

4. *August 1, 2011*

5. *August 1, 2011*

6. *August 1, 2011*

Title of Responsible Person:

Director of Facility Management and Leasing

Chapter 3

Weaknesses in Disaster Recovery Planning and the Use of Outdated Software Could Impair the Commission's Ability to Recover from an Interruption in Services

The Commission should strengthen and test disaster recovery plans for the Winters Data Centers.

While the Commission routinely backs up the seven systems audited, significant weaknesses in disaster recovery planning for the Winters Data Centers could make it challenging for the Commission and health and human services agencies to recover from an interruption in service. The 7 systems audited were considered mission-critical, and the agencies that use these systems specified that these systems must be recovered within 72 hours.

Contractual Requirement for Disaster Recovery Plans

The contract between the Department of Information Resources and Team for Texas required that all systems with a disaster recovery plan be tested annually by Team for Texas and the agency.

Title 1, Texas Administrative Code, Section 202.24

(a) (4) Disaster Recovery Plan—Each state agency shall maintain a written disaster recovery plan for major or catastrophic events that deny access to information resources for an extended period. Information learned from tests conducted since the plan was last updated will be used in updating the disaster recovery plan. The disaster recovery plan will:

(A) Contain measures which address the impact and magnitude of loss or harm that will result from an interruption;

(B) Identify recovery resources and a source for each;

(C) Contain step-by-step implementation instructions;

(D) Include provisions for annual testing.

Disaster recovery plan testing. Although the Texas Administrative Code requires annual testing, none of the health and human services agencies' disaster recovery plans for the seven systems audited had been tested in a planned and controlled environment during fiscal years 2009, 2010, and 2011.

Disaster recovery plan review and approval. The contract between the Department of Information Resources and Team for Texas does not require Team for Texas to obtain health and human services agency review or approval of a disaster recovery plan. There also is no formal process for involving health and human services agencies in each plan's annual update, review, and approval process.

While the contract does not require agency review and approval, the Texas Administrative Code requires agencies to test and update disaster recovery plans. In addition, the disaster recovery plans specify responsibilities for both Team for Texas and the health and human services agencies, and they contain a section for both parties to sign to approve the plans. However, none of the health and human services agencies' disaster recovery plans that auditors reviewed had been approved by agency personnel. Furthermore, information technology staff at three health and human services agencies did not know that Team for Texas had updated their disaster recovery plans[4] until auditors informed them. Two health and human services agencies were in the process of reviewing and approving their updated disaster recovery plans.

Communication and content of disaster recovery plans. Auditors also observed a lack of communication and understanding between Team for Texas and the health and human services agencies about the purpose and content of a

[4] This included a total of four disaster recovery plans at three health and human services agencies (including two disaster recovery plans for the Commission: one at the enterprise level and another at the agency level).

disaster recovery plan. Agencies expect disaster recovery plans to include step-by-step instructions. In contrast, Team for Texas's disaster recovery plans document high-level procedures to perform in the event of a disaster, but they do not include instructions specific to the recovery of the system or server for which a disaster recovery plan is written.

Team for Texas relies on technical documentation in the technical recovery guide in each server's run book (run books contain information necessary to perform day-to-day operations and to respond to emergency situations). The disaster recovery plans specifically refer the user to the technical recovery guide contained in the run books. Auditors reviewed the server run books for each system tested and identified the following:

- Sixteen of the 25 servers tested had no run book or had run books that were incomplete.
- Technical recovery guides do not contain sufficient detail to fully recover servers.

As owners of the systems and the data, the Commission and the health and human services agencies should be involved in the review, approval, and testing of the disaster recovery plans for their systems.

The Commission should address the use of outdated software that is no longer supported by the vendor.

Software that vendors no longer support is referred to as "end-of-life" software. Using end-of-life software is a risk because, in addition to the absence of product support, the vendor ceases offering patches to fix bugs, and malicious codes specifically target unsupported and unpatched operating systems. Any vulnerabilities related to unsupported software create the risk of loss of data, unauthorized data access, or system unavailability. Those risks are in addition to the ongoing risk of malware attacks that systems face each day. Some of the password weaknesses discussed in Chapter 1 were caused by the lack of functionality associated with relying on outdated software.

For the servers and databases tested during this audit:

- Nine (36.0 percent) of 25 servers tested have operating system software that is no longer supported by the vendor.
- Four (40.0 percent) of 10 databases tested are no longer supported by the vendor.

The risks associated with end-of-life software—coupled with the weaknesses in access controls discussed in Chapter 1 and weaknesses in physical security and environmental controls discussed in Chapter 2—significantly increase the risk that services could be interrupted and that data maintained in systems could be lost or stolen. Lack of disaster recovery plan testing and inadequate

technical documentation could impair the ability to recover from an interruption in services.

Recommendations

The Commission should:

- Ensure that each health and human services agency has a comprehensive disaster recovery plan that it tests annually.
- Coordinate with the Department of Information Resources and the data center services vendor to modify procedures and require agencies to review and approve their disaster recovery plans.
- Ensure that each server has a technical recovery guide with sufficient information to recover not only the server, but also the systems and data residing on the server.
- Develop and implement a plan for the replacement of software that is no longer supported by the vendor. This process should include coordination with the Department of Information Resources and the data center services vendor and the prioritization of mission-critical systems.

Management's Response

1. HHSC will ensure that each health and human services agency has a comprehensive disaster recovery plan that it tests annually.

2. HHSC, in consultation with DADS and DSHS, will coordinate with the Department of Information Resources and the data center services vendor to modify procedures and will require agencies to review and approve their disaster recovery plans.

3. HHSC, in consultation with DADS and DSHS, will ensure that each server has a technical recovery guide with sufficient information to recover not only the server, but also the systems and data residing on the server.

4. HHSC will, in consultation with DADS and DSHS, develop and implement a plan to review the software portfolio and identify software that is no longer supported by the vendor. The process will include coordination with the Department of Information Resources and the data center services vendor and will prioritize mission-critical systems. Replacement of software will be: (a) dependent on available funding and (b) contingent on the availability of sufficient hardware resources to support required testing and remediation.

Estimated Completion Date:

1. December 30, 2011

2. December 30, 2011

3. December 30, 2011

4. Processes for review of software lifecycle, in coordination with the Department of Information Resources and the data center services vendor, will be included as part of data center services governance and the new data center services contract. Data center services governance is in place now and has a process for maintaining a list of supported infrastructure software, and for updating the list when software becomes obsolete. HHSC will develop and implement a plan to review the non-data center services software items no later than December 30, 2011.

Title of Responsible Person:

Deputy CIO, HHSC

Appendices

Appendix 1

Objectives, Scope, and Methodology

Objectives

The objectives of this audit were to:

- Determine whether selected information technology controls at the Winters Data Centers operate to protect and support the information technology assets of the State's health and human services agencies.
- Determine whether selected information technology controls at selected health and human services agencies operate to protect state information technology assets.

Scope

The audit scope included the health and human service agency facilities where state technology assets are located, with a focus on the Winters Data Centers facilities in the Austin health and human services complex. The scope of this audit specifically covered information technology systems located on servers at the Winters Data Centers based on a risk assessment of confidential information in the systems and whether the system was identified by the agency as critical to operations. Audit work included a review of logical security controls related to user access and passwords; a review of physical security controls at the Winters Data Centers; and controls related to disaster recovery plans, operations, and security training at selected health and human services agencies. The Department of Assistive and Rehabilitative Services and the Department of Family and Protective Services were not included in logical security controls work because those agencies did not identify systems as critical in the Winters Data Centers.

Methodology

The audit methodology included conducting an assessment of logical security controls for seven systems housed in the Winters Data Centers by verifying the appropriateness of user access, assessing the strength of password controls, and assessing the process for periodic user access reviews. Auditors interviewed staff at the Health and Human Services Commission (Commission), health and human services agencies, the Department of Information Resources, and the Texas Facilities Commission. Auditors also conducted multiple walkthroughs of the Winters Data Centers to assess physical security, environmental security, and alternate and uninterruptible power supply. Auditors also verified the capability of the Commission to

meet state disaster recovery requirements for systems that are housed in the Winters Data Centers.

This audit did not rely on agency data for the purpose of making conclusions. However, auditors used data from the State Data Center Centralized Master Database to assess risk at the Winters Data Centers.

Information collected and reviewed included the following:

- Enterprise-wide information technology inventory ranked by risk.
- Incident reports for all health and human services agencies.
- List of servers with confidential information and their locations.
- Information security policies and procedures for health and human services agencies.
- Risk assessments and disaster recovery plans.
- List of litigation.
- State Fire Marshal's inspection report for the Winters Data Centers.
- Fire inspection report for the Winters Data Centers.
- Report of security card access for the Winters Data Centers.
- Security training.
- Visitor sign in/sign out policies and procedures.
- Screenprints from systems, servers, and databases with user access/password settings.
- Controlled penetration tests for health and human services agencies.
- Backup reports from the data center services' Web portal.

Procedures and tests conducted included the following:

- Conducted interviews with staff from the health and human services agencies, the Department of Information Resources, and the Texas Facilities Commission.
- Conducted walk-throughs of the Winters Data Centers.
- Tested privileged user access to systems.
- Tested the security card access list for Winters Data Centers.

- Reviewed disaster recovery plans for completeness.
- Reviewed server run books and technical guides for completeness.
- Evaluated operating systems and software for end-of-life concerns.
- Reviewed backup procedures and schedules.
- Reviewed hardware asset reports.

Criteria used included the following:

- The Texas Administrative Code.
- The Health Insurance Portability and Accountability Act.
- Internal Revenue Service Publication 1075.
- Health and Human Services Enterprise Information Security Standards and Guidelines (EISSG).
- National Institute of Standards and Technology, Special publication 800-53.
- Control Objectives for Information and Related Technology (COBIT) 4.1, IT Governance Institute.

Project Information

Audit fieldwork was conducted from January 2011 through May 2011. 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.

The following members of the State Auditor's staff performed the audit:

- Cyndie Holmes, CISA (Project Manager)
- Kathy Aven, CIA, CFE (Assistant Project Manager)
- Kenneth Manke
- Darcy Melton, MSA
- Anca Pinchas, CPA, CIDA
- Barrett Sundberg, CIA, MPA

- Serra Tamur, MPAff, CISA, CIA
- Dennis Ray Bushnell, CPA (Quality Control Reviewer)
- Ralph McClendon, CISSP, CCP, CISA (Audit Manager)

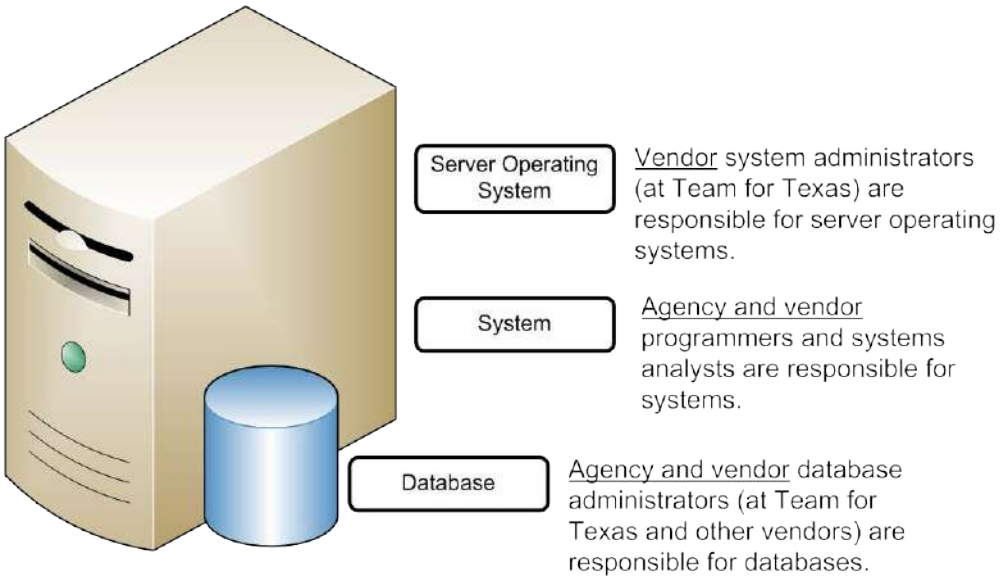
Appendix 2

Shared Responsibility for Server Operating Systems, Systems, and Databases Audited

As Figure 1 shows, agencies and vendors share responsibility for the server operating systems, systems, and databases audited.

Figure 1

Shared Responsibility for Server Operating Systems, Systems, and Databases Audited



Notes:

- Systems and the databases they use are located either on the same servers or on separate servers, depending on the architecture.
- Every server has an operating system.

Source: Developed by auditors based on information that the Health and Human Services Commission provided.

Appendix 3

Interagency Contract Between the Health and Human Services Commission and the Texas Facilities Commission

The interagency contract regarding the Winters Data Centers between the Health and Human Services Commission and the Texas Facilities Commission is presented below.

HHSC Contract No. 529-10-0019-00001

TFC Contract No: 10-005-000 IAC

INTERAGENCY COOPERATION CONTRACT
BETWEEN
TEXAS FACILITIES COMMISSION
AND
HEALTH AND HUMAN SERVICES COMMISSION

This Interagency Cooperation Contract (Contract) is entered into by and between the Texas Facilities Commission (TFC) and the Health and Human Services Commission (Receiving Agency), pursuant to the authority granted by and in compliance with the provisions of "The Interagency Cooperation Act," TEX. GOV'T CODE ANN. §§ 771.001 to 771.010 (Vernon 2004 & Supp. 2008).

SECTION I. STATEMENT OF WORK TO BE PERFORMED.

1.01. **SCOPE OF SERVICES.** (a) TFC shall provide the following security services for the John H. Winters Building, 701 West 51st Street, Austin, Texas (Property):

(i) unarmed security guard services;

(ii) maintenance of closed circuit security camera system and intercom system;

(iii) maintenance to the external card access badge readers;

(iv) agency identification photographs, access cards and supplies for same;

(v) custodial services; and

(vi) cabling.

SECTION II. BASIS FOR COMPUTING REIMBURSABLE COSTS.

2.01. Payments made to TFC shall be for actual security services estimated by TFC in cooperation with Receiving Agency, developed from TFC's expenditure records for Fiscal Year 2008 and Fiscal Year 2009.

2.02. Exceptional costs related to services requested by Receiving Agency above and beyond that contemplated by this Contract may be recovered by TFC on a cost basis. Security badge and related items will be charged as follows:

(i) HID Proximity Card: $5.77 each;

(ii) Sticky Back Card: $2.49 each;

(iii) Plain White Card: $2.49 each;

(iv) Retractable Reels: $1.80 each; and,

(v) Lanyard: $0.77 each.

Page 1 of 5

2.03. Funds received by TFC shall only be used to cover cost of services and resources provided to Receiving Agency. Any funds not used will be returned to agency of origin at the end of the fiscal year. In the event that Receiving Agency requests services beyond those covered by the contract, TFC will provide an estimate and agreement letter for the requested service and Receiving Agency agrees to be liable for such costs upon agreement with and acceptance of the estimate.

SECTION III. CONSIDERATION.

3.01. **CONTRACT AMOUNT.** The total amount of this Contract shall not exceed One Million Five Hundred Twenty-six Thousand and No/100 Dollars ($1,586,000.00) for providing the services required to fulfill the terms of this Contract. For Fiscal Year 2010, the Receiving Agency agrees to pay TFC an amount not-to-exceed the sum of Seven Hundred Ninety-three Thousand and No/100 Dollars ($793,000.00) and for Fiscal Year 2011, the Receiving Agency agrees to pay TFC an amount not-to-exceed the sum of Seven Hundred Ninety-three Thousand and No/100 Dollars ($793,000.00).

3.02. In the event that actual maintenance and facility management and/or utility expenditures are in excess of the above-described amounts, TFC will seek reimbursement from Receiving Agency for same. If actual costs for contracted services by private vendors are less than the maximum contract amount, TFC will return any amount that exceeds actual costs to Receiving Agency.

SECTION IV. PAYMENT FOR SERVICES.

4.01. **PAYMENT.** An Interagency Transaction Voucher or Invoice (ITV) for the services to be performed under the Contract will be prepared by TFC at the beginning of each fiscal year.

Receiving Agency shall reimburse TFC within thirty (30) days from receipt of an ITV or invoice. If payment by Receiving Agency is not paid within thirty (30) days, TFC may cancel the Contract without further notice to Receiving Agency, and Receiving Agency shall remain liable for all actual costs incurred by TFC in delivering services under this Contract.

4.02. **UNIFORM STATE ACCOUNTING SYSTEM (USAS).** To the extent possible, interagency payments involving only treasury funds will be processed as paperless document transfers in the USAS system subject to audit by the Fund Accounting Division of the Comptroller's Office. Payments from treasury funds for deposit into local bank accounts will be processed in USAS through the paperless purchase vouchers process. Interagency payments received from local funds for deposit into the State Treasury must be submitted according to policies and procedures for USAS deposits.

4.03. **REIMBURSEMENT.** Reimbursements with funds contained in the State Treasury shall be made via USAS funds transfers, with Receiving Agency initiating the transfers. TFC will provide Receiving Agency with all the necessary USAS coding elements. Reimbursement with funds outside the State Treasury shall be made by Receiving Agency issuing warrants for payment to TFC.

All reimbursements must be made through the use of local funds or drawn on the appropriated item(s) or account(s) of Receiving Agency from which the agency would ordinarily make expenditures for similar services or resources. Reimbursements will be credited to the appropriation year in which the expenses were incurred.

To comply with HB 1, 80th Leg., R.S., Art. IX, pg. IX-27, Sec. 6.08, entities making payments from funding sources other than General Revenue Fund appropriations, shall remit an additional amount equal to 29.91% of direct labor costs, to cover the cost of the benefits.

SECTION V. TERM OF CONTRACT.

5.01. **TERM.** This Contract shall be effective as of September 1, 2009, and shall terminate on August 31, 2011.

5.02. **DISPUTE RESOLUTION.** The parties agree to use good-faith efforts to decide all questions, difficulties, or disputes of any nature that may arise under or by this Contract; provided however, nothing in this paragraph shall preclude either party from pursuing any remedies as may be available under Texas law.

SECTION VI. FUNDING.

6.01. **NO DEBT.** This Contract shall not be construed as creating any debt on behalf of the State of Texas and/or Receiving Agency and/or TFC in violation of TEX. CONST. Art. III, § 49. In compliance with TEX. CONST. Art. VIII, § 6, it is understood that all obligations of TFC hereunder are subject to the availability of state funds. If such funds are not appropriated or become unavailable, this Contract may be terminated. In that event, the parties shall be discharged from further obligations, subject to the equitable settlement of their respective interests accrued up to the date of termination.

SECTION VII. FORCE MAJEURE.

7.01. **FORCE MAJEURE. Except as otherwise provided, neither TFC nor Receiving Agency is liable to the other for any delay in, or failure of performance, of a requirement contained in this Contract caused by force majeure. The existence of such causes of delay or failure shall extend the period of performance until after the causes of delay or failure have been removed, provided the non-performing party exercises all reasonable due diligence to perform. Force majeure is defined as acts of God, war, strike, fires, explosions, or other causes that are beyond the reasonable**

control of either party and that by exercise or due foresight, such party could not reasonably have been expected to avoid, and which, by the exercise of all reasonable due diligence, such party is unable to overcome. Each party must inform the other in writing with proof of receipt within three (3) business days of the existence of such force majeure.

SECTION VIII. MISCELLANEOUS PROVISIONS.

8.01. **INDEPENDENT CONTRACTOR.** It is further mutually understood and agreed that Receiving Agency is contracting with TFC as an independent contractor.

8.02. **INCORPORATION BY REFERENCE.** Incorporated by reference the same as if specifically written herein are the rules, regulations, and all other requirements imposed by law, including but not limited to compliance with those applicable rules and regulations of the State of Texas and the federal government, all of which shall apply to the performance of the services under this Contract.

8.03. **GOVERNING LAW AND VENUE.** This Contract shall be governed and construed in accordance with the laws of the State of Texas. **VENUE OF ANY SUIT BROUGHT FOR BREACH OF THIS CONTRACT SHALL BE FIXED IN ANY COURT OF COMPETENT JURISDICTION IN TRAVIS COUNTY, TEXAS;** provided, however, the foregoing shall not be construed as a waiver of sovereign immunity by either party.

8.04. **SEVERANCE.** Should any one or more provisions of this Contract be held to be void, voidable, or for any reason whatsoever of no force and effect, such provision(s) shall be construed as severable from the remainder of this Contract and shall not affect the validity of all other provisions of this Contract, which shall remain of full force and effect.

8.05. **HEADINGS.** The headings contained in this Contract are for reference purposes only and shall not in any way affect the meaning or interpretation of this Contract.

8.06. **NOTICES.** Any notice required or permitted to be delivered under this Contract shall be deemed delivered when deposited in the United States mail, postage prepaid, certified mail, return receipt requested, addressed to TFC or Receiving Agency, as the case may be, at the addresses set forth below:

TFC:
Texas Facilities Commission
1711 San Jacinto Blvd.
P.O. Box 13047
Austin, Texas 78711-3047
Attention: James Barrington
Phone: (512) 463-3565
Fax: (512) 236-6179

Receiving Agency: Health and Human Services Commission
4900 N. Lamar
Austin, Texas 78751
Attention: C. J. Adams
Phone: (512) 424-6553
Fax: (512) 424-6641

Notice given in any other manner shall be deemed effective only if and when received by the party to be notified. Either party may change its address for notice by written notice to the other party as herein provided.

8.07. **ENTIRE AGREEMENT.** This Contract constitutes the entire agreement of the parties. No other agreement, statement, or promise that is not contained in this Contract shall be binding except a subsequent written amendment to this Contract signed by both parties.

THE UNDERSIGNED do hereby certify that: (1) the services specified above are necessary and essential and are properly within the statutory functions and programs of the affected agencies of State Government, (2) the proposed arrangements serve the interest of efficient and economical administration of those agencies, and (3) the services, supplies or materials contracted for are not required by Section 21 of Article 16 of the Constitution of Texas to be supplied under contract to the lowest responsible bidder.

TFC certifies that it has the authority to enter into this Contract by virtue of the authority granted in TEX. GOV. CODE ANN., §§2165.007 and 2165.056.

Receiving Agency further certifies that it has the authority to enter into this Contract by virtue of the authority granted in TEX. GOV. CODE ANN., Chapter 771.

TEXAS FACILITIES COMMISSION

Edward L. Johnson
Executive Director

Date: 6-17-2009

Approved as to Form:

G.C.

Dir.

HEALTH AND HUMAN SERVICES COMMISSION

By: Albert Hawkins

Title: Exec. Commissioner

Date: 7-22-09

Appendix 4

Related State Auditor's Office Work

Related State Auditor's Office Work		
Number	**Product Name**	**Release Date**
09-051	An Audit Report on the Department of Information Resources and State Data Center Consolidation	August 2009
08-038	An Audit Report on the Department of Information Resources and the Consolidation of the State's Data Centers	June 2008
08-030	An Audit Report on the Department of Information Resources and Security of the State's Data Centers	April 2008

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Joe Straus III, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas "Tommy" Williams, Member, Texas Senate
The Honorable Jim Pitts, House Appropriations Committee
The Honorable Harvey Hilderbran, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Health and Human Services Commission

Mr. Thomas Suehs, Executive Commissioner

Department of Aging and Disability Services

Mr. Chris Traylor, Commissioner

Department of State Health Services

Dr. David L. Lakey, Commissioner