John Keel, CPA
State Auditor

An Audit Report on

The Department of Information Resources and Security of the State's Data Centers

April 2008

Report No. 08-030

State Auditor's Office

John Keel, CPA
State Auditor

An Audit Report on

The Department of Information Resources and Security of the State's Data Centers

SAO Report No. 08-030
April 2008

Overall Conclusion

The two largest data centers involved in the Department of Information Resources' (Department) state data center consolidation project have control environments capable of protecting state agency systems and safeguarding confidential state data to meet all state and federal requirements. These two data centers—the Austin Data Center and the San Angelo Data Center—are considered the primary data centers and will eventually house the data and systems of the 27 agencies involved in the data center consolidation project. Team for Texas, a group of firms with a $145 million annual contract with the Department, selected the Austin Data Center and the San Angelo Data Center as the final locations for all consolidated data center services.

As of January 2008, only one agency's systems and data had been consolidated; the systems and data of the remaining 26 agencies involved in the data center consolidation project had not been fully consolidated at either of the two primary data centers.

Background Information

The Department of Information Resources entered into a contract with IBM and a group of subcontractors that are collectively referred to as Team for Texas. The contract requires Team for Texas to provide data center services under Texas Government Code, Chapter 2054 (specifically pursuant to House Bill 1516, 79th Legislature, Regular Session). The firms that comprise Team for Texas include:

- IBM (implementation and operations).
- Unisys (facilities operations).
- Pitney Bowes and Xerox (print and mail services).
- Other firms that play smaller roles in Team for Texas (for example, Dell Inc. and AT&T).

These firms are working to move data center operations that are currently located at state agencies to the two primary data centers in Austin and San Angelo. These firms will support data center services for a total of 27 state agencies.

Auditors identified weaknesses in controls at smaller data centers that are involved in the data center consolidation project. For example:

- Reviews of the logs of physical access to server rooms at the Winters Data Center in Austin are incomplete. This may prevent compliance with the U.S. Internal Revenue Service's guidelines for protecting federal tax information. [1]

[1] The U.S. Internal Revenue Service's Publication 1075 (which provides tax information security guidelines for federal, state, and local agencies and entities), Section 5.6.3.3 Audit and Accountability, requires state agencies to develop policy and procedures to detect unauthorized access to federal tax information.

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 processes and procedures at the Winters Data Center for erasing confidential data from tape media are inadequate. Documented processes and procedures are required by the U.S. Health Insurance Portability and Accountability Act (HIPAA).

- A State Fire Marshal inspection of the fire suppression and alarm systems at the Winters Data Center could not confirm that these systems were functional.

- Key card readers at the Winters Data Center and the Network Security Operations Center are not installed or are not functioning properly for some doors to server rooms. This increases the risk of unauthorized physical access to agency servers and data in those server rooms.

Team for Texas also manages the data centers currently located at individual agencies. However, Team for Texas has addressed only certain aspects of security at agency data centers and continues to rely on pre-existing agency processes and physical security at agency data centers for other critical aspects until agency systems are consolidated at one of the primary data centers. As a result, security risks that existed at agency data centers prior to the data center consolidation project will continue to exist until those risks are addressed or until agencies' systems are consolidated into one of the primary data centers.

In addition, Team for Texas has not maintained current disaster recovery plans for each data center. Its contract with the Department does not require Team for Texas to prepare a final disaster recovery plan for the primary data centers until three months after the first agency goes through the consolidation process at one of the primary state data centers. Team for Texas has collected 17 existing agency disaster recovery plans and developed new disaster recovery plans for 6 agencies. Until all agency disaster recovery plans are developed and updated for the current environment, agencies could lose the ability to conduct business if their disaster recovery plans are not adequate.

Summary of Management's Response

The Department agrees with the recommendations in this report, and it provided the following summary of its responses:

> *The Department agrees with the recommendations in the report and appreciates the SAO's assessment that the two primary state data centers are sound and secure facilities. The Department acknowledges the risks in the current environment and suggests that the impetus for the data center services program stems from these risks. The SAO's findings support the data center services program and the Department's objective to migrate in-scope operations to environments with higher levels of security and access controls.*
>
> *The Department will continue to work with agencies and the Team for Texas to address risks in the current data center environment while consolidating*

operations to the Austin Data Center and San Angelo Data Center. The Department will use a methodical consolidation process to enable agencies to efficiently migrate to the new environment without introducing additional risks through undue haste.

Detailed management responses are included in the Detailed Results section of this report, and an overall response from the Department is presented in Appendix 3.

Summary of Objective, Scope, and Methodology

The audit objective was to determine whether the information technology general controls, such as organizational, security, general operations, and disaster recovery controls, at the state data centers under the scope of Team for Texas's contract with the Department are operating effectively to protect state information technology assets and support state agency operations.

The audit scope covered control environments that existed as of January 2008 at the Austin Data Center, the Network Security Operations Center in Austin, the San Angelo Data Center, and the Winters Data Center in Austin. It is important to note that the scope of this audit did not include application controls or aspects of operating system security that are not managed centrally.

The audit methodology included visits to selected data centers to assess physical security, environmental security, alternate and uninterruptible power supply, logical security procedures for consolidated systems, backup procedures, network and firewall security, hardware disposal, and disaster recovery. Auditors also verified the capability of data centers to meet state and federal data security requirements, including the U.S. Internal Revenue Service's security guidelines; HIPAA requirements; and information security standards in Title 1, Texas Administrative Code, Chapter 202.

Auditors communicated details of information technology weaknesses and other less significant issues separately to the Department.

Contents

Detailed Results

Appendices

Detailed Results

Chapter 1

Two of Four State Data Centers Audited Have Weaknesses in Security Controls

Auditors visited the four largest state data centers and identified weaknesses in security controls at two of them: the Winters Data Center in Austin and the Network Security Operations Center in Austin. The other two data centers audited—the Austin Data Center and the San Angelo Data Center—are capable of protecting systems and safeguarding confidential data after agency data center operations are consolidated at those data centers. However, security risks that existed at agency data centers prior to the data center consolidation project will continue to exist until they are corrected or until agencies' systems are consolidated at the Austin Data Center or the San Angelo Data Center.

State of Texas Data Centers and the Data Center Consolidation Project

As of January 2008, many of the 27 agencies involved in the data center consolidation project still operated automated systems from their own agency locations. Four data centers maintain systems for multiple agencies: the Winters Data Center in Austin, the Network Security Operations Center in Austin, the Austin Data Center, and the San Angelo Data Center.

Team for Texas's long-term plan is to move the systems and data for all 27 agencies involved in the data center consolidation project to the two primary data centers: the Austin Data Center and the San Angelo Data Center.

This report refers to agency data centers and primary data centers to distinguish between the different types of data centers. Agency data centers and systems are currently operated by Team for Texas at agencies' facilities but will be consolidated into one of the primary data centers in accordance with Team for Texas's contract with the Department of Information Resources. Some agencies have systems and data stored at the San Angelo Data Center but still need to complete Team for Texas's consolidation process.

The weaknesses identified at two state data centers highlight the differences in the level of standardization and controls between (1) the data centers that will be reduced in functionality as part of the data center consolidation project and (2) the two primary data centers in Austin and San Angelo that will be expanded as part of the data center consolidation process. (See text box for details on the data center consolidation project.) Team for Texas, a group of firms with a $145 million annual contract with the Department of Information Resources (Department), has developed policies and procedures that, if implemented, will provide adequate physical security controls at the two primary data centers in Austin and San Angelo.

Auditors reviewed security controls at both primary data centers and determined that state systems and data were adequately protected at those data centers. In addition, security safeguards and controls at the primary data centers are capable of meeting the wide range of security requirements of the 27 agencies involved in the data center consolidation project, including the following key safeguards:

- Encryption of federal tax information across public networks to protect confidential data.
- Access to duplicate or redundant sources of power and an uninterruptible power supply to keep data centers functioning in the event of a power

outage. The San Angelo data center also maintains a backup generator in addition to having access to a backup power grid.

- Scheduled backup routines to prevent loss of data in the event of hardware or software failure.

However, as of January 2008, only one agency (the Library and Archives Commission) had consolidated its servers and data at one of the two primary data centers to fully benefit from the standardized control environment at those data centers. Team for Texas may use some of the controls at other agency data centers involved in the data center consolidation project while also using outdated processes and procedures that agency staff developed prior to the data center consolidation project. The lack of standardization in controls across agency data centers creates a fragmented control environment for the 27 agencies involved in the data center consolidation project.

The Department, agencies, and Team for Texas have not taken responsibility for the administration of security at agency data centers as required by Title 1, Texas Administrative Code, Section 202.21. Instead, Team for Texas is relying on processes and procedures that agencies established for physical and logical security prior to the commencement of its contract with the Department. As a result, risks that may have existed prior to the data center consolidation project will continue to exist at agencies until they are corrected or until Team for Texas consolidates each agency's systems and data into a primary data center that offers standardized controls.

Chapter 1-A

The Winters Data Center Lacks Certain Security Controls

Auditors noted multiple weaknesses in controlling physical access to confidential data at the Winters Data Center. The Winters Data Center has three separate server rooms that house systems and data for many of the health and human services agencies. This data is subject to several state and federal security requirements. The most stringent of these are the security requirements in the U.S. Internal Revenue Service's Publication 1075 and the U.S. Health Insurance Portability and Accountability Act (HIPAA). The following weaknesses may prevent the Winters Data Center from consistently complying with these requirements:

- The Winters Data Center lacks processes and procedures to ensure that staff log removable tapes and erase those tapes as required by HIPAA regulations [Title 45, Code of Federal Regulations, Section 164.310(d)(2)(ii)].

- The Winters Data Center lacks processes and procedures to ensure that staff periodically review access logs from one server room for indications

of unusual activities or suspected violations as required by U.S. Internal Revenue Service Publication 1075, Section 5.6.3.3. It is important to note that the U.S. Internal Revenue Service inspected four systems located at the Winters Data Center and concluded that the server room containing those systems met minimum protection standards. The weaknesses that the State Auditor's Office identified, however, existed in other parts of the Winters Data Center.

- A magnetic key card reader on one exterior door of the Winters Data center had been removed, which limits the ability of data center staff to control access to that data center and to periodically review physical access logs as required by HIPAA regulations [Title 45, Code of Federal Regulations, Section 164.310(a)(2)(ii)].

Any weaknesses that existed before Team for Texas's contract with the Department commenced may still exist. Team for Texas has only partly assessed overall security risks and it omitted key controls such as physical and environmental security as discussed in Chapter 2. However, Team for Texas is not tasked with the responsibility to improve security procedures or controls at the Winters Data Center. Instead, Team for Texas continues to run the Winters Data Center using the security procedures and policies that were in effect prior to the Department's commencement of the data center consolidation project.

In addition, auditors identified other controls that can be improved to further protect agency systems and data, but these controls are not required by state or federal law:

- The fire suppression systems and fire alarm systems in two of the three server rooms at the Winters Data Center may not be functional. A State Fire Marshal inspection of the fire suppression and fire alarm systems indicated that these systems were impaired and may not be operational if a fire occurred.

- Visitor access logs for the Winters Data Center are inaccurate and incomplete. Auditors determined that unauthorized employees signed in for visitors, which enabled visitors to enter restricted areas.

- A loading dock at the Winters Data Center is not always secured due to an equipment malfunction.

The agencies that have systems and data at the Winters Data Center are primarily health and human services agencies, which are scheduled last on the data center consolidation project plan. As a result, many of these weaknesses could continue to exist until the scheduled conclusion of the data center consolidation project in December 2009 (or longer if the project is delayed).

Auditors determined that the following key controls were adequate at the Winters Data Center:

- Safeguards to prevent loss of power.
- Procedures to maintain backup copies of critical data.
- Access to the Internet through a single portal that is restricted by firewalls and is protected by intrusion prevention systems to reduce the risk of cyber attacks.

A summary of key controls at the Winters Data Center is available in Appendix 2.

Chapter 1-B

The Network Security Operations Center in Austin Lacks Certain Security Controls

Auditors identified multiple weaknesses in controlling physical access to server rooms at the Network Security Operations Center in Austin. This data center contains state agencies' systems and data that must be secured according to the U.S. Social Security Administration's information system security guidelines and HIPAA.

The following security weaknesses may limit the Network Security Operations Center from complying with security requirements:

- A door to one server room at the Network Security Operations Center was not locked during auditors' visit. This could allow physical access to agency servers. In addition, access to server room doors is automatically logged via key cards, but data center staff are not required to review the logs. HIPAA regulations [Title 45, Code of Federal Regulations, Section 164.310(a)(2)(ii)] require that physical access controls be implemented to prevent unauthorized physical access, tampering, and theft of protected health information.
- The Network Security Operations Center lacks policies and procedures to address security incidents as required by HIPAA regulations [Title 45, Code of Federal Regulations, Section 164.308(a)(6)].
- The Network Security Operations Center has not developed a policy to provide staff with security awareness training as required by HIPAA regulations [Title 45, Code of Federal Regulations, Section 164.308(a)(5)].
- The Network Security Operations Center lacks documented shut down procedures for agency systems as required by National Institute of Standards and Technology Special Publication 800-53.

Multiple entities use the Network Security Operations Center to store data and conduct operations. For example, Department staff monitor the networks at that data center, and four contractors support agency systems at that data center. This data center houses systems for at least 22 state agencies, but only 8 of those agencies are involved in the data center consolidation project. The large number of entities operating at this data center increases the risk that confidential data could be exposed due to the security weaknesses described above. However, auditors did not determine that breaches of security had occurred.

Auditors determined that the following controls were adequate at the Network Security Operations Center:

- Monitoring of environmental risks (for example, fire, water, and temperature).
- Safeguards to prevent loss of power.
- Procedures to maintain backup copies of critical data.
- Processes to erase or destroy data on hardware before disposal.
- Access to the Internet through a single portal that is restricted by firewalls and is protected by intrusion prevention systems to reduce the risk of cyber attacks.

A summary of key controls at the Network Security Operations Center is available in Appendix 2.

Chapter 1-C

The Two Primary Data Centers Have Critical Security Controls

Controls at the two primary data centers—the Austin Data Center and the San Angelo Data Center—adequately protect state systems and data. The primary data centers are the two largest data centers involved in the data center consolidation project and Team for Texas plans to move each agency's systems to one of these two data centers.

As of January 2008, nine agencies' systems were located at the San Angelo Data Center, but Team for Texas had not completed the consolidation process for those agencies' systems. Northrop Grumman, the Department's former contractor for the San Angelo Data Center operated this data center until September 1, 2007. Auditors reviewed security controls at this data center and determined that systems and data were adequately protected. In addition, auditors verified the existence of key controls for the Library and Archives Commission, the only agency whose systems had been fully consolidated at the Austin Data Center as of January 2008.

Auditors determined that the following controls were adequate at both the Austin Data Center and the San Angelo Data Center:

- Physical security controls to prevent unauthorized access to hardware and network equipment.
- Monitoring of environmental risks (for example, fire, water, and temperature).
- Safeguards to prevent loss of power.
- Controls to prevent unauthorized electronic access to data.[2]
- Procedures to maintain backup copies of critical data.
- Processes to erase or destroy data on hardware before disposal.

The two primary data centers are capable of protecting and safeguarding confidential data.

The Austin Data Center and San Angelo Data Center are capable of protecting systems and safeguarding confidential data after agency data center operations are consolidated. Auditors verified that these data centers have key controls to protect agency systems, including the following critical safeguards:

- These two data centers comply with numerous state and federal requirements that auditors tested (see Appendix 2 for a list of these requirements). In addition, auditors reviewed documentation from the U.S. Internal Revenue Service's inspection of certain security controls at the Austin Data Center. That inspection determined that the Austin Data Center meets minimum standards to protect federal tax information.
- These two data centers have access to redundant power grids for power redundancy. In addition, the San Angelo Data Center maintains a backup generator to provide a third source of power.
- These two data centers make routine backups of agency systems and data and store the backups at off-site vendors.
- These two data centers encrypt network traffic when it travels between the data centers across virtual private networks, and they segregate this information according to agency systems.
- These two data centers control Internet access through a single portal that is restricted by firewalls and is protected by intrusion prevention systems to reduce the risk of cyber attacks.

[2] Auditors did not review application controls or aspects of operating system security.

Auditors also determined that the Austin Data Center and the San Angelo Data Center are capable of complying with state and federal requirements with which agency data centers currently must comply. For example, the San Angelo Data Center stores federal tax information for the Office of the Attorney General, and Team for Texas plans to use the Austin Data Center as a disaster recovery location for this same data. This data must be restricted in accordance with special safeguards published by the U.S. Internal Revenue Service[3], and those safeguards are among the most restrictive requirements for data involved in the data center consolidation project. Auditors verified that both data centers are capable of complying with those safeguards.

Recommendations

The Department should:

- Require Team for Texas or agencies to address control weaknesses at the Winters Data Center and the Network Security Operations Center.
- Conduct a security analysis at each of the 26 agencies' data centers whose operations have not been consolidated to determine whether critical security controls are present.

Management's Response

The Department agrees with the recommendations and is taking measures to address security controls at the Network Security Operations Center. The Department has installed a security system that automatically logs access to all server room doors via key cards and will update the appropriate policies and procedures to ensure its security controls are compliant with the appropriate HIPAA and NIST regulations.

Estimated completion date: April 30, 2008

Title of responsible person: Network Security Operations Center Manager

The Department will work with Team for Texas and the Health and Human Services Commission to review security controls at the Winters Data Center. The Department has hired a Risk, Security and Facilities Specialist who will collaborate with Team for Texas and the Health and Human Services Commission to identify cost-effective compensating protections that could be implemented prior to consolidation.

[3] See U.S. Internal Revenue Service Publication 1075, *Safeguards for Protecting Federal Tax Returns and Return Information*.

Estimated completion date: August 31, 2008

Title of responsible person: Risk, Security and Facility Specialist

The Department required Team for Texas to complete a security analysis for logical security and develop statewide standards regarding security settings and controls for operating systems and software tools. The process included gathering baseline data on current security controls, assessing the gap between baseline data and agreed to settings, identifying threats, and communicating known vulnerabilities in the environment. The Department received and accepted this analysis on December 21, 2007. Based on the assessment, Team for Texas developed a project plan to resolve gaps, threats, and vulnerabilities for in-scope operations prior to consolidation. The Department received the project plan on March 12, 2008. The Department, Team for Texas, and the agencies are currently implementing changes to achieve the enterprise standards over the next six months.

Estimated completion date: Phased implementation to be completed by December 31, 2008

Title of person responsible: Data Center Services Manager

The Department is committed to assessing other security risks, including physical, environmental and network security risks, in agency data centers. The Department will work with agencies to gather data on the current environment, review risks and risk mitigation strategies against consolidation timelines, and develop a process to appropriately address any outstanding issues. The Department will develop a prioritized plan to assess the physical, environmental, and logical risks to information resources at each of the 26 unconsolidated agencies' data centers. This assessment will identify threats, vulnerabilities, impact of disruption, and remediation responsibilities.

Estimated completion date: August 31, 2008

Title of person responsible: Data Center Services Manager

Pursuant to HB 1788, 80th Legislative Session, the Department also assesses security controls through a compliance review. All agencies are required to document compliance with security and other information resources-related statutes, rules and standards for the Information Resources Deployment Review (IRDR). The Department reviews the information submitted in the IRDR and requires agencies to submit a corrective action plan for each non-compliant area. The Department submits these responses and action plans to the State Auditor and Legislative Budget Board.

Estimated completion date: July 31, 2008

Title of responsible person: Information Resources Deployment Review Coordinator

Team for Texas Has Not Standardized Access Controls at Agency Data Centers

Team for Texas has designed processes, policies, and procedures to standardize the safeguards that protect access to agency systems and data at the two primary data centers (the Austin Data Center and the San Angelo Data Center). However, according to Team for Texas's plans, it will implement these controls only after each system is consolidated at one of the primary data centers. As a result, the Department does not have assurance that the systems and data currently residing at agency data centers are protected with standardized access controls.

Some weaknesses in security controls may still exist at agency data centers.

As of January 2008, the Library and Archives Commission was the only agency to complete Team for Texas's consolidation process. Agency data centers operated by Team for Texas at agencies' facilities still have controls to protect their systems (those controls were implemented by agency staff prior to the data center consolidation project). However, any access control weaknesses at the agency data centers that existed before Team for Texas assumed responsibility on March 31, 2007, will continue to exist until those agencies' systems are consolidated at a primary data center.

Team for Texas has not implemented standardization of password management and user account management at agency data centers. Although Team for Texas has developed processes, policies, and procedures to prevent unauthorized logical access to state systems and data, it has not implemented the majority of those controls at agency data centers. As discussed below, Team for Texas also has not standardized other access controls across agency data centers.

Some security threats may not be identified and may continue to exist until agencies' systems are consolidated at one of the primary data centers.

Neither Team for Texas nor the Department monitors security or user account management at agency data centers. Team for Texas is required to perform a security baseline review of agency environments, document security gaps, and develop plans to resolve security gaps. However, in fulfilling this requirement, Team for Texas addresses only certain aspects of security at agency data centers. Specifically, Team for Texas has assessed the following security controls at many agency data centers:

- Operating system configurations.
- Application and database configurations.
- Disaster recovery planning.

- Network security controls for certain types of network hardware.

However, Team for Texas continues to rely on pre-existing agency processes and physical security at agency data centers for other critical aspects. Team for Texas, agencies, and the department do not provide comprehensive monitoring of the following:

- Physical access controls for hardware.
- Environmental exposures and controls.
- Comprehensive network infrastructure.
- Security risk management.

Many of these critical aspects may be performed by the Department or agencies until agency systems are consolidated at one of the primary data centers. The fragmentation of control and lack of comprehensive monitoring create a risk that some security threats may not be identified and may continue to exist until agencies' systems are consolidated at one of the primary data centers. As of January 2008, some agencies were not scheduled to complete the consolidation process until December 2009.

Auditors identified the following weaknesses at agency or primary data centers:

- User account management practices are inconsistent across agency data centers and between systems within the same agency data center.
- Security awareness training to communicate security policies to employees is inconsistent across agency data centers and the Austin Data Center.
- Agency and primary data centers use inconsistent incident response procedures, emergency plans, and shut-down procedures. Therefore, the Department cannot ensure that data centers use a standardized response in the event of a security incident or emergency.

The Department has not standardized network controls or firewall configurations.

Firewall policies and configurations are not consistent between network devices at each of these data centers. However, auditors reviewed network and firewall security policies and procedures at each of the four data centers visited and did not identify any significant weaknesses that would compromise the security of those data centers. The Department is responsible for controlling access to the Capitol Area Network (CAPnet, the data communications network that agency data centers use to transfer information and access the Internet). Team for Texas is responsible for controlling access

to primary data center networks, and agencies are responsible for controlling access to agency data center networks, each of which connects to CAPnet. If each network device that connects to CAPnet had similar security configurations this could help to ensure that an acceptable security level is maintained for CAPnet.

Recommendations

The Department should:

- Coordinate with agencies that have data centers in the scope of the data center consolidation project to assess risks at each agency data center to determine whether significant risks expose data to unauthorized access or modification. If an agency identifies significant risks, the agency should work to correct or mitigate these risks during this transition period.

- Establish minimum security policies for network devices and periodically test firewall security to verify compliance with these policies.

- Ensure that all agency systems involved in the data center consolidation project receive periodic network scans and penetration tests to monitor network security across the networks that carry agency data.

- Coordinate with state agencies' internal and external auditors on future audits to continue to review the agencies' logical control environments until their systems have been consolidated at one of the two primary data centers.

Management's Response

The Department agrees with these recommendations and strongly supports comprehensive risk assessments for all state agencies. Through the aforementioned security analyses, the Department, participating agencies, and the Team for Texas will address logical, physical, environmental and network security risks for the data centers in the contract.

Additionally, the Department integrated risk assessment into the TAC 202 security rules and the State Enterprise Security Plan (SESP). These rules and strategies address risk assessments as part of all business decisions affecting the security of information resources. The Department offers Information Security Awareness, Assessment, and Compliance (ISAAC), a risk assessment tool, to all agencies free of charge. ISAAC facilitates agency baseline risk analysis, vulnerability reduction of cyber assets, compliance, planning, and tracking of agency IT assets.

Estimated completion date: Ongoing

Title of responsible person: Chief Information Security Officer

The Department agrees that the state should establish minimum security policies for network devices and periodically test firewall security to verify compliance with these policies. The Department will revise and update TAC RULE §202.25 to reflect minimum security policies for network devices and require periodic testing of firewall security to verify compliance with these policies.

Estimated completion date: October 31, 2008 for establishment of policy, periodic testing is ongoing

Title of responsible person: Chief Information Security Officer

The Department will conduct periodic network scans and penetration tests to monitor network security across the networks that carry agency data.

Estimated completion date: Ongoing

Title of responsible person: Chief Information Security Officer

The Department will notify agency internal auditors of the SAO's recommendation and work with agency internal auditors and the SAO on any future data center audits.

Estimated completion date: May 1, 2008

Title of responsible person: Data Center Services Manager

Disaster Recovery Plans Have Not Been Developed for Data Centers

The Department has not ensured that a current disaster recovery plan is available for each data center, as required by Title 1, Texas Administrative Code, Section 202.24. Team for Texas has collected 17 existing agency disaster recovery plans and developed new disaster recovery plans for 6 agencies since the Team for Texas contract commenced on March 31, 2007. Team for Texas's contract with the Department requires it to collect and update disaster recovery plans that agencies used before the data center consolidation project. The Department has not worked with the agencies involved in the data center consolidation project to prioritize the order in which critical agency systems will be recovered if a disaster occurs. This creates a risk that critical agency systems could not be restored in a timely manner (or restored at all) if a disaster occurred in the interim period during which agency systems are being consolidated.

According to its contract with the Department, Team for Texas is not required to finalize disaster recovery plans for the two primary data centers in Austin and San Angelo until three months after some agency systems are consolidated at those data centers. As a result, as of January 2008, Team for Texas had not developed disaster recovery plans for the primary data centers. Instead, Team for Texas relies on disaster recovery plans that were in existence at the agencies before the data center consolidation project to help it recover from any disasters that could occur during the consolidation process. It is important to note that Team for Texas plans to make significant modifications to agency systems as part of the data center consolidation project, and comprehensive disaster recovery plans need to be in place to support these systems. The duration for which agency disaster recovery plans will need to be updated differs for each of the agencies due to the schedule for moving systems to one of the primary data centers.

Although it has updated disaster recovery plans for most agencies involved in the data center consolidation project, Team for Texas has tested only four agency plans since March 31, 2007, to ensure that it is capable of restoring agency operations. In addition, due to the nature of the consolidation process, significant changes could occur to agency systems that further increase the risk that pre-existing agency disaster recovery plans could become outdated, incomplete, or otherwise unusable. As of January 2008, Team for Texas did not plan to complete consolidation of some agency systems until December 2009.

Recommendations

The Department should:

- Develop interim disaster recovery plans for primary data centers for the period during which Team for Texas is consolidating agency systems.
- Ensure that disaster recovery plans exist and they are periodically tested for all agency systems throughout the entire duration of the data center consolidation project.
- Ensure that the Business Leadership Council for Technology [4] prioritizes the order in which critical agency systems will be recovered if a disaster occurs.
- Continuously monitor Team for Texas's progress in consolidating data centers, with the purpose of determining when significant changes to systems have occurred that require updates to disaster recovery plans.

Management's Response

The Department agrees with the recommendations. The Department has received an interim disaster recovery plan for the San Angelo Data Center from Team for Texas. This plan, initially developed by a prior vendor, was reviewed, validated, and updated after Team for Texas assumed operational responsibility for the center on August 31, 2007. Team for Texas is finalizing a disaster recovery plan for the Austin Data Center.

Estimated completion date: May 5, 2008

Title of person responsible: Data Center Services Manager

The Department requires Team for Texas to develop or update disaster recovery plans for the agencies in the data center services program. As this report states, all plans have been developed and 23 of these plans have been accepted by the agency. DIR is working with the three agencies to finalize the plans so all agencies will have complete disaster recovery plans.

Estimated completion date: April 30, 2008

Title of person responsible: Data Center Services Manager

[4] The Department's executive director chairs the Business Leadership Council for Technology. This council's members include agency heads or executive-level designees.

The Department has confirmed Team for Texas has completed or scheduled disaster recovery tests for the following agencies:

- *Completed*
  - *OAG-CS June 12, 2007*
  - *TXDOT July 23, 2007*
  - *TWC October 17 – 19, 2007*
  - *SOS February 8, 2008 (Table Top Exercise)*
  - *TABC March 25, 2008 (Table Top Exercise)*
- *Scheduled*
  - *TDCJ June 12, 2008*
  - *TWC August 11, 2008*
  - *TWC November 8, 2008*

The Department will continue to work with agencies and the Team for Texas to schedule additional tests, as appropriate, to ensure disaster recovery plans are periodically tested.

Estimated completion date: Ongoing

Title of person responsible: Data Center Services Manager

The Department convened the first meeting of the Business Leadership Council for Technology on February 22, 2008. At the next meeting scheduled for July 9, 2008, the Department will include a discussion about disaster recovery and begin to establish the guiding principles for setting the order of priority in which critical agency systems will be recovered if a disaster occurs.

Estimated completion date: November 30, 2008

Title of person responsible: Chief Technology Officer

The Department has confirmed that activities to update disaster recovery plans are included in agency transformation plans. As agencies transform (installing new tools and processes to facilitate migration to a primary state data center), disaster recovery plans will be revised as necessary. The Department will monitor Team for Texas's progress and ensure updates occur as needed.

Estimated completion date: Ongoing

Title of person responsible: Data Center Services Manager

Appendices

Appendix 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether the information technology general controls, such as organizational, security, general operations, and disaster recovery controls, at the state data centers under the scope of IBM's (the lead contractor for Team for Texas) contract with the Department of Information Resources (Department) are operating effectively to protect state information technology assets and support state agency operations.

Scope

The scope of this audit included the four largest data centers managed by the Department, each of which is included in the data center consolidation project. These data centers were: the Austin Data Center, the San Angelo Data Center, the Winters Data Center in Austin, and the Network Security Operations Center in Austin. The scope covered the time period from December 2007 through January 2008. It is important to note that the scope of this audit did not include application controls or aspects of operating system security that are not managed centrally.

Methodology

The audit methodology included interviewing Department personnel; interviewing Team for Texas staff; and reviewing network and firewall policies and configurations, disaster recovery planning documentation, the November 2006 Master Service Agreement signed by IBM and the Department, policies and procedures developed by Team for Texas, and security requirements related to information technology systems. Auditors also conducted walkthroughs of the four data centers in the audit scope to discuss and observe the general controls implemented.

Information collected and reviewed included the following:

- Master service agreement between IBM and the Department, signed on November 22, 2006.
- Policies and procedures developed by Team for Texas.
- Policies and procedures developed by agencies.
- Maps of computer networks at each data center visited.

- Disaster recovery planning documents developed by agencies.
- Draft disaster recovery planning documents for primary data centers developed by Team for Texas.
- State Fire Marshal inspection documents for each data center.
- U.S. Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification Text.
- U.S. Internal Revenue Service Publication 1075 "Safeguards for Protecting Federal Tax Returns and Return Information."
- Criminal Justice Information System security policy.
- U.S. Family Educational Rights and Privacy Act (FERPA).
- U.S. Social Security Administration requirements.
- Payment Card Industry (PCI) data security standards.
- Computer systems and networks at data centers.

Procedures and tests conducted included the following:

- Interviewed key staff from the Department and Team for Texas.
- Analyzed compliance with security requirements.
- Analyzed the implementation of policies and procedures related to change management and incident management.
- Observed and tested physical and logical access at data centers.
- Observed environmental controls at all data centers.
- Reviewed data center disaster recovery plans.
- Analyzed the effectiveness of network perimeter security controls through monitoring and periodic scanning.

Criteria used included the following:

- Master service agreement between IBM (the lead contractor for Team for Texas) and the Department, signed on November 22, 2006.
- Title 1, Texas Administration Code, Chapter 202.
- Team for Texas policies and procedures.
- Department policies and procedures.

- HIPPA Administrative Simplification Text.
- U.S. Internal Revenue Service Publication 1075 "Safeguards for Protecting Federal Tax Returns and Return Information"
- Criminal Justice Information System security policy.

Project Information

Audit fieldwork was conducted from December 2007 through January 2008. 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:

- Kels Farmer, CISA (Project Manager)
- Cyndie Holmes, CISA (Assistant Project Manager)
- Shelby Cherian, MBA (Information Systems Audit Team)
- Michelle DeFrance, MA
- Joe Kozak, CPA, CISA (Information Systems Audit Team)
- Serra Tamur, MPAff, CIA, CISA (Information Systems Audit Team)
- Worth Ferguson, CPA (Quality Control Reviewer)
- Ralph McClendon, CCP, CISA, CISSP (Audit Manager)

Audit team members from other state agencies:

- Carlos Contreras, MBA, CIA, CISA, CGAP, CCSA, Higher Education Coordinating Board
- Scott Coombes, JD, CISA, Commission on Environmental Quality
- Karin Faltynek, Department of Transportation
- Enrique Guerra, MBA, CIA, Texas Education Agency
- Brandy Meeks, CPA, CIA, Texas Youth Commission
- Emmanuel Nwokocha, MMIS, CISA, Department of Insurance

- Jack Rayburn, CDP, CCP, CISA, CISM, CFGM, Office of the Attorney General

Appendix 2

Summary of Key Controls at State Data Centers Audited

Table 1 summarizes auditors' assessment of key controls at the four data centers audited.

Table 1

Assessment of Key Controls at State Data Centers Audited				
Key Control	Austin Data Center	San Angelo Data Center	Winters Data Center in Austin	Network Security Operations Center in Austin
Building and perimeter are sound and secure. Rooms used for systems are constructed solidly; walls, floors, and ceiling allow no alternative methods of access.	Y	Y	N	N
Auxiliaries to systems (cabling, back-up power, transformers, fire suppression) are secure.	Y	Y	Y	Y
Physical access to systems and auxiliaries requires authorization and is monitored.	Y	Y	N	Y
Systems are protected from environmental hazards such as heat, cold, humidity, and flooding.	Y	Y	Y	Y
Building and systems rooms are designed to deter or prevent fire hazards.	Y	Y	Y	Y
Systems and personnel are protected from fire hazards.	Y	Y	N	Y
Data center has sufficient alternative power sources to maintain operation in the case of power spikes and short- and long-term outages.	Y	Y	Y	Y
Alternative power sources are maintained and tested regularly.	Y	Y	Y	Y
Data center has an effective process to authorize and monitor physical access to systems for only personnel that require physical access to systems.	Y	Y	N	Y
Data center follows policies for assigning logical access to systems such as unique user IDs, strong passwords, password expiration thresholds, and regular monitoring of access.	Y	Y	N	N
Data center actively protects systems from viruses and mal-ware.	Y	Y	Y	Y
Data center monitors systems for outside intrusion and has an appropriate process to investigate, stop, and report an attempted intrusion.	Y	Y	Y	Y
Data transmitted between the data center and an agency is encrypted while on public lines.	Y	Y	N/A	N/A
Systems at the data center are backed up on an appropriate schedule. Back-up media is tested, and data is capable of being retrieved if necessary.	Y	Y	Y	Y
Media used for secure data is disposed of in a way that prevents release of data (for example, destruction) through erasure.	Y	Y	N	Y
All media, including back-up media, used for secure data is stored in a secure location when not in use.	Y	Y	Y	Y

Assessment of Key Controls at State Data Centers Audited				
Key Control	Austin Data Center	San Angelo Data Center	Winters Data Center in Austin	Network Security Operations Center in Austin
Data center has a disaster recovery plan in place that will minimize interruption of service in the case of an emergency.	N	N	N	N
Data center's disaster recovery plan is tested at least annually and updated to reflect current needs of the data center.	N/A	N/A	N/A	N/A
Data center is materially compliant with the standards within the following laws, regulations, or organizations (N/A means the data center does not and will not store data related to the law, regulation, or organization):				
▪ U.S. Health Insurance Portability and Accountability Act (HIPAA).	Y	Y	N	N
▪ U.S Internal Revenue Service standards.	Y	Y	N/A	N/A
▪ Criminal Justice Information System standards.	Y	Y	N/A	N/A
▪ U.S. Family Educational Rights and Privacy Act (FERPA).	Y	Y	N/A	N/A
▪ Payment Card Industry standards.	Y	Y	N/A	N/A
▪ Federal requirements (Federal Information Security Management Act of 2002 and National Institute of Standards and Technology).	Y	Y	N	N/A
▪ Texas Administrative Code.	Y	Y	N	N

Appendix 3

Overall Management Response from the Department of Information Resources

TEXAS DEPARTMENT OF INFORMATION RESOURCES
P.O. Box 13564 ◆ Austin, TX 78711-3564 ◆ www.dir.state.tx.us
Tel: (512) 475-4700 ◆ Fax: (512) 475-4759

April 1, 2008

Mr. John Keel, CPA
State Auditor
State Auditor's Office
1501 N. Congress Ave.
Austin, TX 78701

Dear Mr. Keel,

The Department of Information Resources (Department) appreciates the SAO's recognition of the sound security controls in place at the two main state data centers and welcomes the opportunity to further improve data center operations for Texas. The Department concurs that the Austin Data Center, a hardened facility built to the state's specifications, and San Angelo Data Center, recently upgraded to better protect systems and data, have the capability to provide secure, reliable services for state agencies. This audit supports the state's direction to consolidate data center operations to upgrade service, security, and disaster recovery for agencies.

Implementation of audit recommendations will help improve the security of the state's critical systems in the current environment. The Department is committed to addressing audit findings and has already implemented a number of changes.

Because it may not be possible or cost effective to mitigate all risks in the current environment, the Department will also work with agencies to develop compensating controls and efficiently consolidate in-scope operations to the Austin Data Center and San Angelo Data Center. These operations host many of the state's most critical programs and services and, accordingly, the Department will work to balance speed of consolidation with the need for careful and deliberate planning. The Department will employ a structured process for consolidation to avoid introducing risk or disrupting the state's business.

The Department thanks the audit team for their professionalism and commitment to understanding the complexities of the data center services contract. The Department also thanks the SAO for the opportunity to provide feedback and comment on this report and welcomes further input on improving security controls in the state data center system.

Sincerely,

Brian S. Rawson
Chief Technology Officer
State of Texas

Copies of this report have been distributed to the following:

Legislative Audit Committee

The Honorable David Dewhurst, Lieutenant Governor, Joint Chair
The Honorable Tom Craddick, Speaker of the House, Joint Chair
The Honorable Steve Ogden, Senate Finance Committee
The Honorable Thomas "Tommy" Williams, Member, Texas Senate
The Honorable Warren Chisum, House Appropriations Committee
The Honorable Jim Keffer, House Ways and Means Committee

Office of the Governor

The Honorable Rick Perry, Governor

Department of Information Resources

Members of the Department of Information Resources Board
- Mr. Cliff Mountain, Chair
- The Honorable Charles Bacarisse
- Mr. Albert Betts
- Mr. Gary Gumbert
- Ms. Rosemary R. Martinez
- The Honorable Debra McCartt
- Mr. P. Keith Morrow
- Mr. Robert E. Pickering, Jr.
- Mr. Edward Serna
- Mr. William Wachel

Mr. Brian S. Rawson, Chief Technology Officer