



John Keel, CPA
State Auditor

A Follow-up Audit Report on The Issuance of Birth Certificates at the Department of State Health Services

December 20, 2012

Members of the Legislative Audit Committee:

The Department of State Health Services (Department) fully or substantially implemented 8 (57 percent) of 14 recommendations from *An Audit Report on the Department of State Health Services' Issuance of Birth Certificates* (State Auditor's Office Report No. 10-011, November 2009). (See text boxes for background information on the prior audit report and implementation status definitions.)

Of the eight recommendations fully or substantially implemented:

- The Department fully implemented two recommendations for ensuring that it issues birth certificates only to qualified applicants and maintaining application records for the required time frames.
- The Department fully implemented one recommendation to accurately record in its internal Remittance System the funds that its Vital Statistics Unit receives.
- The Department fully or substantially implemented three recommendations related to certain security-related policies and procedures.
- The Department substantially implemented two recommendations related to its information system controls for passwords and disaster recovery testing.

While the Department has made progress in implementing the prior audit recommendations, it should continue its efforts to improve controls related to (1) its monitoring of local registrars' compliance with applicable laws and regulations, (2) its compliance with its *Internal Security Manual*, and (3) reviewing user access to its Texas Electronic Registrar (TER) system. Specifically:

- The Department should strengthen its monitoring of local registrars by updating its policies and procedures, requiring local registrars to submit self-assessments, documenting its selection process for monitoring visits, and maintaining an accurate list of completed monitoring visits.
- The Department should ensure that its Vital Statistics Unit complies with policies and procedures related to the destruction of birth certificates and obtaining all required employee signatures for confidentiality and computer use agreements.

Background Information

In November 2009, the State Auditor's Office issued *An Audit Report on the Department of State Health Services' Issuance of Birth Certificates* (State Auditor's Office Report No. 10-011). Auditors selected all 14 recommendations in that report for follow-up based on Department of State Health Services (Department) management's original responses to the recommendations, the Department's subsequent self-reported recommendation implementation status and implementation dates, and the level of risk.

Implementation Status Definitions

Fully Implemented - Successful development and use of a process, system, or policy to implement a prior recommendation.

Substantially Implemented - Successful development but inconsistent use of a process, system, or policy to implement a prior recommendation.

Incomplete/Ongoing - Ongoing development of a process, system, or policy to address a prior recommendation.

Not Implemented - Lack of a formal process, system, or policy to address a prior recommendation.

- The Department should deactivate or update TER access for users with inappropriate access to that system and periodically review user access to TER to ensure that it appropriately restricts access based on each user’s job responsibilities.

The Department did not implement a prior recommendation to establish a process for monitoring or reviewing transactions processed using the “no fee” function in TER. (The no fee function is a function in TER that allows users to process a birth certificate request without assessing a fee.) The Department’s Vital Statistics Unit uses that feature primarily to correct errors, void requests, document client communications, and issue certificates for military and school purposes.

Auditors communicated other, less significant issues to the Department’s management separately in writing.

Table 1 provides additional details on the Department’s implementation of prior State Auditor’s Office recommendations.

Table 1

Status of Implementation of Prior Audit Recommendations				
No.	Recommendation	Implementation Status as Reported by the Department	Implementation Status as Determined by Auditors	Auditor Comments
1	The Department should develop a risk-based approach to monitoring local registrars to ensure that local registrars (1) issue birth certificates in accordance with applicable laws and regulations; (2) comply with all reporting requirements; (3) retain birth certificate-related records for at least three years in compliance with the State's record retention schedule; and (4) remit funds to the State as required by Texas Health and Safety Code, Section 191.022.	Fully Implemented	Incomplete/ Ongoing	<p>The Department developed policies and procedures for monitoring local registrars; however, it did not document its risk-based approach for selecting local registrars at which it will conduct monitoring visits. As a result, auditors were unable to determine whether the local registrars the Department visited in fiscal years 2011 and 2012 were high-risk registrars.</p> <p>In addition, not all of the Department’s processes and risk factors for selecting the local registrars at which it will conduct monitoring visits were incorporated into the Department’s policies and procedures. The Department also did not use all of the tools available to it in its risk assessment process.</p> <p>Specifically, the Department’s procedures require local registrars to submit self-assessments; however, the Department did not ensure that local registrars submitted those self-assessments, and it did not use the self-assessments that were submitted in its risk assessment process.</p> <p>The Department’s list of completed monitoring visits was not accurate. Auditors obtained the list of monitoring visits the Department reported it completed from March 1, 2010, through August 31, 2012, and selected a sample of 30. For 3 (10 percent) of the 30 monitoring visits tested, the Department had not conducted a monitoring visit. For the remaining 27 monitoring visits tested (90 percent), the Department had evidence to support that it reviewed the local registrars’ compliance with applicable laws and regulations.</p>
2	The Department should ensure that correct identification is attached to all applications and that all applications are signed by the requestor.	Fully Implemented	Fully Implemented	For all 30 applications auditors tested, the Department ensured that the applicant was qualified, that the applicant had attached the correct identification, and that the requestor had signed the application.

Status of Implementation of Prior Audit Recommendations				
No.	Recommendation	Implementation Status as Reported by the Department	Implementation Status as Determined by Auditors	Auditor Comments
3	The Department should ensure that all records are kept at least three years in compliance with the State's records retention schedule in Title 25, Texas Administrative Code, Section 181.28.	Fully Implemented	Fully Implemented	The Department had application records for all 30 applications that auditors tested.
4	The Department should ensure that the amounts entered into its internal Remittance System match the amounts remitted to the Office of the Comptroller of Public Accounts.	Fully Implemented	Fully Implemented	The Department has controls to ensure that it accurately records the funds its Vital Statistics Unit receives in its internal Remittance System. After the 2009 audit, the Department began using the services of a new third-party vendor for processing credit card remittances. Credit card remittances are now automatically uploaded to IRS to prevent data entry errors. All 30 remittances from fiscal years 2011 and 2012 that auditors tested were accurately entered into IRS and could be traced to the Uniform Statewide Accounting System.
5	The Department should ensure that its Vital Statistics Unit complies with its <i>Internal Security Manual</i> .	Fully Implemented	Incomplete/Ongoing	The implementation status of this recommendation is based on the Vital Statistics Unit's compliance with <i>Internal Security Manual</i> requirements in recommendations 6, 7, and 8 below. While the Department appropriately logged its issuance of security paper, it did not fully comply with documentation procedures for the destruction of birth certificates or for ensuring that all Vital Statistics Unit employees sign all required confidentiality and computer user agreements.
6	The Department should ensure that its Vital Statistics Unit complies with its documentation procedures for the destruction of birth certificate paper.	Fully Implemented	Incomplete/Ongoing	Auditors reviewed all 14 destruction reports completed in fiscal years 2011 and 2012. None of the destruction reports complied with all of the Department's requirements for the destruction of birth certificate paper. Specifically, of the 14 destruction reports tested: <ul style="list-style-type: none"> ▪ 13 (93 percent) did not include the document control numbers voided, the dates voided, or who voided the certificates. ▪ 4 (29 percent) did not have the required signature of the individual who shredded the certificates. ▪ 1 (7 percent) did not contain the date on which the certificate was voided.
7	The Department should ensure that its Vital Statistics Unit logs every issuance of security paper in the document log spreadsheet.	Fully Implemented	Fully Implemented	The Department's Vital Statistics Unit logged in the document control log spreadsheet the 31 security paper issuances that auditors tested.

Status of Implementation of Prior Audit Recommendations				
No.	Recommendation	Implementation Status as Reported by the Department	Implementation Status as Determined by Auditors	Auditor Comments
8	The Department should ensure that all Vital Statistics Unit employees sign all required confidentiality and computer use agreements.	Fully Implemented	Incomplete/ Ongoing	<p>The Department did not ensure that all Vital Statistics Unit employees signed all required confidentiality and computer user agreements. Specifically:</p> <ul style="list-style-type: none"> • Employees hired on or after September 1, 2010, that auditors selected for testing signed a confidentiality agreement on the day their employment began. However, the Department did not renew confidentiality agreements for its employees annually as required by its <i>Internal Security Manual</i>. • Employees hired on or after September 1, 2010, that auditors selected for testing signed a computer usage agreement on the day their employment began. However, the Department did not require employees to sign a new computer usage agreement annually as required by the <i>Internal Security Manual</i>. The Department required employees to complete computer usage training annually. Of the 28 employees auditors tested, 27 (96 percent) had renewed their computer usage training in a timely manner.
9	The Department should ensure that there is a review of the inventory report for accuracy before it is sent to management. The Department should also document this process in policies and procedures.	Fully Implemented	Substantially Implemented	The Department implemented a review process for the inventory report by having a second staff member conduct a count of the inventory. All inventory reports that auditors tested were reviewed by a second staff member. However, the review process was not documented in the Department's policies and procedures.
10	The Department should ensure that its Vital Statistics Unit complies with all security requirements in Title 25, Texas Administrative Code, Chapter 181, or update the security requirements in the Texas Administrative Code to reflect the Department's current security practices.	Substantially Implemented	Fully Implemented	The Department updated its solicitation for the procurement of security paper to comply with all security features required by the Texas Administrative Code. The vendor agreements the Department entered into in fiscal years 2011 and 2012 met all solicitation specifications.
11	The Department should ensure that its password controls for TER comply with the password guidelines and best practices.	Fully Implemented	Substantially Implemented	The Department strengthened its password controls for TER; however, the password expiration setting for TER does not comply with the Department's internal password guidelines. Additionally, although the Department considered establishing an account lockout feature for TER, it did not establish that feature.
12	The Department should establish a process to monitor and periodically review the use of TER's no fee function.	Fully Implemented	Not Implemented	The Department did not establish a process, nor does it monitor or periodically review transactions processed using the no fee function in TER.

Status of Implementation of Prior Audit Recommendations				
No.	Recommendation	Implementation Status as Reported by the Department	Implementation Status as Determined by Auditors	Auditor Comments
13	The Department should regularly review user access to TER, deactivate and update user access as users' job responsibilities change.	Fully Implemented	Incomplete/ Ongoing	<p>The Department has an informal process to submit employee terminations and transfers to its departments to review and make updates to TER access on a weekly basis. However, that process is not documented, and the Department did not have evidence to support that departments performed those reviews or deactivated or updated access as users' job responsibilities changed.</p> <p>Auditors reviewed user access for internal users for TER and external users with access to processes that the Department reported were restricted to internal users at the Department. Auditors determined that:</p> <ul style="list-style-type: none"> Twenty internal users reviewed had inappropriate access to TER data. Sixteen of those 20 were employees whose employment had been terminated or were employees who changed positions or had not accessed TER in more than 2 years. Three of those 20 were associated with generic accounts that were no longer necessary for business purposes. The last account was shared by multiple users. None of the external users that auditors tested had access to the three security processes that the Department considers to be most critical. However, 78 external users tested had access to processes in TER that the Department asserted were supposed to be restricted to internal Department employees. <p>Because TER does not have the ability to disable or lock user accounts, it is important for the Department to have compensating controls to help ensure that it reviews user accounts and updates them appropriately to prevent inappropriate access or changes to confidential data.</p>
14	The Department should work with Team for Texas at the Department of Information Resources to set up and conduct an annual test of its disaster recovery plan.	Fully Implemented	Substantially Implemented	<p>The Department performed a test of its disaster recovery plan for TER in September 2012. However, that test was conducted 23 months after the Department placed new servers into production for TER. Title 1, Texas Administrative Code, Chapter 202, requires those tests to be performed annually. In addition, the Department did not maintain supporting documentation for any data validation work it did to ensure that the application data was complete and that the system tested was successfully restored.</p>

Recommendations

The Department should:

- Strengthen its risk-based approach to monitoring local registrars by:
 - ♦ Updating its policies and procedures to reflect all risk factors it considers when selecting the local registrars at which it will conduct monitoring visits.
 - ♦ Requiring submission of and using local registrars' self-assessments in its risk assessment process.
 - ♦ Documenting its risk-based approach for selecting the local registrars at which it will conduct monitoring visits.
 - ♦ Ensuring that its list of completed monitoring visits at local registrars is accurate.
- Require its Vital Statistics Unit to comply with documentation procedures for the destruction of birth certificate paper.
- Require Vital Statistics Unit employees to sign all confidentiality and computer use agreements required by its policies and procedures.
- Require its Vital Statistics Unit to document its policies and procedures for reviewing inventory of security paper.
- Align its password expiration setting for TER with its internal password guidelines.
- Develop and implement a process to monitor and periodically review the use of TER's no fee function.
- Deactivate or update TER access for users with inappropriate access to that system. In addition, it should periodically review user access to TER to ensure that it appropriately restricts access based on each user's job responsibilities.
- Conduct and document tests of its disaster recovery plan annually as required by Title 1, Texas Administrative Code, Chapter 202.

The Department agreed with the above recommendations, and its management's responses are in the attachment to this letter.

Sincerely,

John Keel, CPA
State Auditor

Attachment

cc: Dr. Kyle Janek, Executive Commissioner, Health and Human Services Commission
Dr. David L. Lakey, Commissioner, Department of State Health Services



This document is not copyrighted. Readers may make additional copies of this report as needed. In addition, most State Auditor's Office reports may be downloaded from our Web site: www.sao.state.tx.us.

In compliance with the Americans with Disabilities Act, this document may also be requested in alternative formats. To do so, contact our report request line at (512) 936-9500 (Voice), (512) 936-9400 (FAX), 1-800-RELAY-TX (TDD), or visit the Robert E. Johnson Building, 1501 North Congress Avenue, Suite 4.224, Austin, Texas 78701.

The State Auditor's Office is an equal opportunity employer and does not discriminate on the basis of race, color, religion, sex, national origin, age, or disability in employment or in the provision of services, programs, or activities.

To report waste, fraud, or abuse in state government call the SAO Hotline: 1-800-TX-AUDIT.

Attachment

Section 1

Objective, Scope, and Methodology

Objective

The objective of this audit was to determine the implementation status of prior State Auditor's Office recommendations and evaluate whether management has taken corrective actions to address recommendations in *An Audit Report on the Department of State Health Services' Issuance of Birth Certificates* (State Auditor's Office Report No. 10-011, November 2009).

Scope

The scope of this audit included reviewing the implementation status of the Department of State Health Services' (Department) prior audit recommendations in *An Audit Report on the Department of State Health Services' Issuance of Birth Certificates* (State Auditor's Office Report No. 10-011, November 2009) from March 1, 2010, through August 31, 2012.

Methodology

The audit methodology included identifying and collecting information on the implementation of the prior audit recommendations. To determine the implementation status of the recommendations, auditors conducted interviews, reviewed the Department's policies and procedures, and performed selected tests and procedures.

Auditors assessed the reliability of Department data associated with local registrar monitoring visits; birth certificates issued, voided, and inventoried; and funds remitted by (1) reviewing query language used to extract data from the Department's automated system, (2) analyzing key data elements for completeness and reasonableness, and (3) interviewing Department employees knowledgeable about the data. Auditors determined that the data was sufficiently reliable for the purposes of this audit.

To determine the implementation status of prior recommendations, auditors selected and tested non-statistical samples. Specifically:

- Auditors selected 30 local registrar monitoring visits that Department field representatives had conducted since March 1, 2010. Auditors stratified the sample by region so that it included all regions.
- Auditors selected 30 birth certificates issued between September 1, 2010, and August 31, 2012. Auditors stratified the sample by unique remittance and application type so that it included all remittance and application types for testing applications and funds remitted, and to determine whether the

Department properly logged the security paper it used for the birth certificates.

- Auditors randomly selected 28 employees of the Department's Vital Statistics Unit to test whether they completed and signed confidentiality and computer usage agreements as required by the Department's *Internal Security Manual*.
- Auditors selected a sample of five monthly inventory reports for security paper to determine whether the Department reviewed them for accuracy before sending them to management. Auditors selected the most recent inventory report completed (in August 2012) and randomly selected four additional inventory reports for testing.

Because auditors did not use a statistical sample, findings cannot be generalized and may not represent the entire population of the Department's birth certificates issued, logged, and inventoried or funds remitted.

Information collected and reviewed included the following:

- *An Audit Report on the Department of State Health Services' Issuance of Birth Certificates* (State Auditor's Office Report No. 10-011, November 2009) and supporting audit documents.
- Department risk assessment procedures and surveys for monitoring local registrars.
- List of monitoring visits at local registrars that the Department completed from March 2010 through August 31, 2012.
- Department documentation of training provided to local registrars.
- Department policies and procedures for birth certificate applications and record retention.
- Birth certificates issued from September 1, 2010, through August 31, 2012, from the Department's Texas Electronic Registrar (TER) system and supporting documents for a selected sample.
- Department documentation to support reconciliations of amounts entered into its internal Remittance System.
- Internal security policies and procedures of the Department's Vital Statistics Unit.
- Birth certificates voided from September 1, 2010, to August 31, 2012, from TER and supporting documents for the sample selected.

- List of employees in the Department's Vital Statistics Unit from September 1, 2010, through August 31, 2012.
- Department confidentiality and computer use agreements for a selected sample.
- Vendor contract and bid information for security paper.
- Information that supported the Department's implementation of information technology recommendations, including Department security standard guidelines for passwords, screenshots to support TER password controls, and evidence to support annual disaster recovery tests for TER.

Procedures and tests conducted included the following:

- Interviewed management and key personnel at the Department.
- Tested a sample of local registrar monitoring visits that Department field representatives conducted since March 1, 2010, to determine whether the Department verified that local registrars complied with applicable laws and regulations.
- Tested a sample of birth certificate applications issued between September 1, 2010, and August 31, 2012, to determine whether the Department had adequate supporting documentation and whether it maintained applications in accordance with retention requirements.
- Tested a sample of funds remitted to the Department and the Office of the Comptroller of Public Accounts.
- Reviewed and tested policies and procedures from the Department's Vital Statistics Unit's *Internal Security Manual* related to birth certificate paper destruction, security paper logging, security paper inventory reviews, and employee confidentiality and computer use agreements.
- Reviewed Department security paper vendor agreement and supporting documentation for fiscal years 2011 and 2012 to determine whether required security features were included and to obtain evidence that the Department had tested the security features successfully.
- Reviewed user access controls for internal TER users and selected external TER users.
- Reviewed evidence of Department disaster recovery tests for TER performed in September 2012.

Criteria used included the following:

- Department policies and procedures, including:

- ♦ *Basic Issuance Manual.*
- ♦ *Internal Security Manual.*
- ♦ *Security Standard Guidelines for Passwords.*
- Title 25, Texas Administrative Code, Chapter 181.
- Title 1, Texas Administrative Code, Chapter 202.
- Texas Health and Safety Code, Chapter 191.
- *Federal Information System Controls Audit Manual (FISCAM I)*, GAO-09-232F version, U.S. Government Accountability Office, February 2009.

Project Information

Audit fieldwork was conducted from September 2012 through October 2012. 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:

- Stacey Williams, CGAP (Project Manager)
- Kendra Shelton, MAcy, CPA (Assistant Project Manager)
- Kristina A. Aguilar
- Ishani Baxi, CIDA
- Rachel Lynne Goldman, CPA
- Jacqueline M. Gomez
- Frances Anne Hoel, CIA, CGAP
- Ashlee C. Jones, MAcy, CFE, CGAP
- Kristin Alexander, MBA, CFE, CIA (Quality Control Reviewer)
- Nicole M. Guerrero, MBA, CIA, CGAP, CICA (Audit Manager)

Management's Responses

Recommendations

The Department should:

Strengthen its risk-based approach to monitoring local registrars by:

- *Updating its policies and procedures to reflect all risk factors it considers when selecting the local registrars at which it will conduct monitoring visits.*
- *Requiring submission of and using local registrars' self-assessments in its risk assessment process.*
- *Documenting its risk-based approach for selecting the local registrars at which it will conduct monitoring visits.*
- *Ensuring that its list of completed monitoring visits at local registrars is accurate.*

Management Response

The department agrees to strengthen the initial risk-based approach to monitoring local registrars. VSU Field Services Branch has begun to implement the recommendations for use in setting the next monitoring cycle. The department has already taken steps to ensure the accuracy of lists of completed monitoring visit lists.

Implementation Date: April 30, 2013

Responsible Party: Field Services Branch, Vital Statistics Unit and Director, Vital Statistics Unit

Require its Vital Statistics Unit to comply with documentation procedures for the destruction of birth certificate paper.

Management Response

The department agrees it should comply with documentation procedures for the destruction of birth certificate paper and has modified its operations to comply with documentation procedures going forward.

Implementation Date: January 31, 2013

Responsible Party: Manager, Request Processing Branch and Director, Vital Statistics Unit

Require Vital Statistics Unit employees to sign all confidentiality and computer use agreements required by its policies and procedures

Management Response

The department agrees with this recommendation and is currently taking actions to communicate to managers the importance of complying with policies and procedures that require all employees to sign confidentiality and computer use agreements within the specified time frame, and verify that all employees are in compliance.

Implementation Date: January 31, 2013

Responsible Party: Staff Services Officer, Vital Statistics Unit and Director, Vital Statistics Unit

Require its Vital Statistics Unit to document its policies and procedures for reviewing inventory of security paper.

Management Response

The department agrees with this recommendation and is currently taking action to improve documentation of procedures for reviewing this inventory.

Implementation Date: January 31, 2013

Responsible Party: Manager, Request Processing Branch and Director, Vital Statistics Unit

Align its password expiration setting for TER with its internal password guidelines.

Management Response

The department agrees with this recommendation and is currently taking actions to align password expiration setting for TER with internal password guidelines.

Implementation Date: April 30, 2013

Responsible Party: Manager, Electronic Registration, Vital Statistics Unit and Director, Vital Statistics Unit

Develop and implement a process to monitor and periodically review the use of TER's no fee function.

Management Response

DSHS last reviewed the use of the no fee functions in 2009. The department will establish a formal process, based upon the 2009 review, to develop standard periodic monitoring. Reviews currently conducted each month will be formalized to include documentation of monitoring use of the no fee function.

Implementation Date: January 31, 2013

Responsible Party: Manager, Request Processing Branch and Director, Vital Statistics Unit

Deactivate or update TER access for users with inappropriate access to that system. In addition, it should periodically review user access to TER to ensure that it appropriately restricts access based on each user's job responsibilities.

Management Response

The Department agrees that it is important to deactivate or update TER access for users. The department will develop and document more formal processes to periodically review and adjust user access.

Implementation Date: April 30, 2013

Responsible Party: Manager, Electronic Registration, Vital Statistics Unit and Director, Vital Statistics Unit

Conduct and document tests of its disaster recovery plan annually as required by Title 1, Texas Administrative Code, Chapter 202.

Management Response

The Department agrees with the importance of testing its disaster recovery plan annually. The department will develop a process to request annual testing and monitor vendor performance in conducting the test annually.

Implementation Date: January 31, 2013

Responsible Party: Director, Information Technology Section and Director, Vital Statistics Unit