State Auditor's Office

John Keel, CPA
State Auditor

An Audit Report on

Well-plugging within the Railroad Commission's Oil and Gas Regulation and Cleanup Program

July 2013

Report No. 13-040

State Auditor's Office
John Keel, CPA
State Auditor

An Audit Report on

Well-plugging within the Railroad Commission's Oil and Gas Regulation and Cleanup Program

SAO Report No. 13-040
July 2013

Overall Conclusion

The Railroad Commission (Commission) follows a process for prioritizing and recommending oil and gas wells for plugging that incorporates risk-based factors and complies with requirements in the Texas Natural Resources Code. As part of its Oil and Gas Regulation and Cleanup Program, the Commission creates annual plugging goals for its Oil and Gas Division's district offices (see the text box for additional information). The district offices follow the Commission's policies and procedures to prioritize wells eligible for plugging and recommend the specific wells that should be plugged.

> **Background Information**
>
> Through its Oil and Gas Division, the Railroad Commission (Commission) regulates the exploration, production, and transportation of oil and natural gas in Texas. To prevent pollution of the state's surface water and groundwater resources, the Commission has an Oil and Gas Regulation and Cleanup Program that is funded, in part, by financial assurances (cash, bonds, and letters of credit) that oil and gas operators provide. This audit focused on the process of selecting wells for plugging that the Commission performs through that program, and its collection of financial assurances.
>
> The Oil and Gas Division is headquartered in Austin and has nine district offices across the state (see Appendix 2). The district offices help ensure compliance with Commission rules by performing field inspections, witnessing well-plugging and testing, and investigating complaints and incidents.
>
> The Commission was appropriated $20,106,474 in fiscal year 2012 and $20,078,082 in fiscal year 2013 for oil and gas well-plugging. The Commission's operational goals were to plug 1,222 wells in fiscal year 2012 and 815 wells 2013. At the end of fiscal year 2012, the Commission reported that it had plugged, had contracts to plug, or had bid out the plugging of 1,162 wells.

The Commission also has effective processes and related controls to establish, maintain, and collect the financial assurances from oil and gas well operators that are required by Texas Natural Resources Code, Chapter 91. The financial assurances are cash, bonds, or letters of credit that operators provide and that fund the Commission's plugging of wells. However, the Commission should strengthen certain controls related to its financial assurance processes to help ensure that it can collect on those financial assurances before they expire. In 63 (98 percent) of the 64 cases that auditors tested, the Commission appropriately sent demands to collect on operators' financial assurances. However, in one instance the Commission did not collect on an operator's $25,000 letter of credit. In that instance, the letter of credit expired before the Commission determined that it should have collected on that letter of credit.

The Commission has adequate information technology security policies, user access policies, use of generic user id accounts, change management policies, password controls for applications, and physical security controls for its mainframe. However, the Commission should strengthen certain controls for its mainframe and Oilfield Cleanup (OFCU) application in the areas of review of user access,

This audit was conducted in accordance with Texas Government Code, Sections 321.0131 and 321.0132.

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

segregation of programmer duties, password controls for servers, and physical controls over the Commission's data center.

Auditors communicated less significant issues to Commission management separately in writing.

Key Points

The Commission follows a process for prioritizing and recommending oil and gas wells for plugging that incorporates risk-based factors.

District offices use a worksheet the Commission developed to determine the priority rating to assign to a well they recommend for plugging. Auditors tested the records for 121 wells recommended for plugging and determined that the district offices had completed priority worksheets for all 121 wells. The Commission's central office in Austin reviews and approves the wells the district offices recommend for plugging. The Commission had documentation supporting the prioritization, recommendation, and approval for 117 (97 percent) of the 121 wells recommended for plugging that auditors tested.

The Commission establishes annual operational goals for the number of wells each district office should plug.

Factors the Commission considers when developing goals for plugging wells include the number of wells plugged in prior periods, the results of cost analysis, and the available well-plugging budget. The Commission reported that it had plugged, had contracts to plug, or had bid out the plugging of 1,162 wells (95 percent of its well-plugging goal) for fiscal year 2012. The cost associated with plugging the 764 wells the Commission plugged in fiscal year 2012 was $12,309,477.

The Commission has designed and implemented effective processes and related controls to help ensure that regulated entities establish and maintain financial assurances in amounts consistent with state law and administrative rules.

The Commission has automated controls to help ensure that it calculates the appropriate amount of financial assurance each operator must provide. All 35 operators that auditors tested provided the correct amount of financial assurances. The Commission also has a process to help ensure that (1) its processing of financial assurances is accurate and (2) data entry for the organizational reports that operators submit is accurate. The Commission properly entered all of the key data from hard-copy documentation operators submitted into its mainframe system for the 60 operators that auditors tested.

The Commission has adequate processes and controls to help ensure that it sends demand notices to operators that do not submit required annual organizational reports.

As discussed above, in 63 (98 percent) of the 64 cases that auditors tested, the Commission appropriately sent demands to collect on operators' financial assurances. In one instance, however, the Commission did not send a demand before that operator's financial assurance (a letter of credit) had expired, resulting in the Commission not being able to collect on that operator's $25,000 letter of credit. The Commission has an informal process for ensuring that it sends demand notices; however, it has not documented that process to help ensure that it standardizes its process so that it can collect on financial assurances before they expire.

Summary of Management's Response

The Commission agreed with the recommendations in this report.

Summary of Information Technology Review

Auditors conducted a review of general controls and a review of application controls for the Commission's mainframe system and OFCU application. As discussed above, the Commission has adequate information technology controls in certain areas, but it should strengthen information technology controls in other areas.

Summary of Objectives, Scope, and Methodology

The audit objectives were to determine whether the Commission:

- Has established and adheres to a risk assessment process to prioritize the plugging of wells with state funds.

- Has designed and implemented effective processes and related controls to help ensure that (1) regulated entities establish and maintain the financial assurance required by Texas Natural Resources Code, Chapter 91, in amounts consistent with state law, administrative rules, and Commission policy and (2) the Commission collects funds from those sources in accordance with Commission policies and procedures, the administrative rules, and the terms of agreements related to that financial assurance.

The audit scope included reviewing records of oil and gas wells for eligibility for plugging with state funds and the associated financial assurances for fiscal year 2012 and fiscal year 2013 through February 2013.

The audit methodology included collecting information and documentation from the Commission; reviewing policies and procedures, statutes, and rules related to state-funded well-plugging and financial assurances; and analyzing and evaluating data and the results of tests. Specifically, auditors reviewed oil and gas well inspection records, documentation recommending wells for state-funded plugging, operators' organizational reports, and financial assurance documentation. Auditors assessed the reliability of the operator and well data used in the audit by (1) reviewing general controls and application controls for the mainframe system and OFCU application, (2) comparing data to other sources of information, (3) analyzing key data elements for completeness and reasonableness, and (4) interviewing Commission employees knowledgeable about the data. Auditors determined that the data was sufficiently reliable for the purposes of this audit.

Contents

Detailed Results

Chapter 1
The Commission Follows Its Process for Prioritizing and Recommending Oil and Gas Wells for Plugging 1

Chapter 2
The Commission Ensures That Operators Provide Required Financial Assurances, But It Should Strengthen Certain Controls Related to Those Financial Assurances 5

Chapter 3
The Commission Has Adequate Information Technology Systems Controls, But It Should Strengthen Controls in Certain Areas..9

Appendices

Appendix 1
Objectives, Scope, and Methodology 14

Appendix 2
Districts in the Railroad Commission's Oil and Gas Division.. 18

Appendix 3
Related State Auditor's Office Work 19

Detailed Results

Chapter 1

The Commission Follows Its Process for Prioritizing and Recommending Oil and Gas Wells for Plugging

The Railroad Commission (Commission) follows a process for prioritizing and recommending oil and gas wells for plugging that incorporates risk-based factors and complies with requirements in Texas Natural Resources Code, Section 91.1132 (see text box for additional information on those requirements). The Commission implemented its process to prioritize and recommend wells for plugging with state funds at each of its Oil and Gas Division's district offices (see Appendix 2 for a map of the district offices).

Texas Natural Resources Code Requirements

Texas Natural Resources Code, Section 91.1132, requires the Commission to develop a system to:

- Identify wells that pose a high risk of contaminating surface water or groundwater.
- Periodically test high-risk wells by conducting a fluid level test or, if necessary, a pressure test.
- Give priority to plugging high-risk wells with compromised casings.

The Commission establishes operational annual goals for the number of wells each district office should plug. The Commission considers several factors when developing those goals. To meet its well-plugging goal, each district office recommends wells for plugging based on a risk-based prioritization and decision making process. The Commission's central office in Austin then approves the district offices' recommendations based on various factors.

Priority Ratings

The Commission's district offices assign one of the following priority ratings to each well they recommend for plugging:

- 1 – This is the highest rating and is assigned to wells that are leaking.
- 2H – This rating is assigned to relatively higher risk wells, including wells in areas where usable quality water is not protected, wells in areas where hydrogen sulfide affects a public area, and wells with fluid at the surface that is not of a usable quality.
- 2 – This rating is assigned based on weighted scores to wells with a fluid level that is at or above the deepest base of usable quality water.
- 3 – This rating is assigned based on weighted scores.
- 4 – This is the lowest rating and is assigned based on weighted scores.

Source: The Commission.

Prioritizing, Recommending, and Approving Wells for Plugging with State Funds

The process for prioritizing wells for plugging incorporates risk-based factors. The Commission's policies and procedures provide the district offices with eligibility criteria for state-funded plugging and direction on how to prioritize and recommend wells for plugging (see text box for information on priority ratings). The district offices are responsible for submitting well-plugging recommendations to the Commission.

District offices use a worksheet the Commission developed to determine the priority rating to assign to a well they recommend for plugging. Factors on that worksheet include:

- Whether the well is capable of protecting usable quality groundwater.
- The mechanical integrity of the well.
- The fluid level in relation to usable quality water.
- The well's location with respect to sensitive areas.

- Whether the well has any effect on the environment, safety, or economy of its surrounding area.

Auditors tested the records for 121 wells recommended for plugging and determined that the district offices had completed priority worksheets for all 121 wells. The Commission's central office in Austin reviews and approves the wells the district offices recommend for plugging based on information in the priority worksheets.

The Commission had documentation supporting the prioritization, recommendation, and approval for 117 (97 percent) of the 121 wells recommended for plugging that auditors tested. For the remaining four wells, the Commission did not have complete documentation to support how it determined that the wells were eligible, in accordance with its policies, for plugging with state funds at the time of the recommendation for plugging. Specifically:

- One of the wells that a district office rated as priority 2 had production activity within 12 months of the well-plugging recommendation date. Therefore, that well was not in violation of the Commission's statewide rule regarding inactive wells (a condition that makes wells eligible for plugging with state funds). Although the well was not eligible for plugging with state funds at the time of the recommendation, it was eligible for plugging with state funds when it was plugged.

- One of the wells that a district office rated as priority 4 had production activity within 12 months of the recommendation date. Therefore, that well was not in violation of the Commission's statewide rule regarding inactive wells. That well was taken over by another operator after the Commission recommended it for plugging and was not plugged with state funds.

- The Commission could not provide all of the supporting documentation for two of the wells that a district office rated as priority 2H. As a result, there was not sufficient evidence regarding why those wells were eligible for plugging with state funds and why they were recommended for plugging. The Commission also did not have any documentation of its approval of those two wells for plugging. At the time of this audit, those wells had not been plugged.

The Commission's record retention policy states that well-plugging records must be maintained permanently. Not maintaining that documentation results in the Commission not having support for its decision to recommend wells for plugging with state funds.

Annual Well-plugging Goals

The Commission provides annual operational goals for the number of wells its Oil and Gas Division's district offices should plug. Factors the Commission considers when developing goals for plugging wells include the number of wells plugged in prior periods, the results of cost analysis, and the available well-plugging budget. The Commission reported that it had plugged, had contracts to plug, or had bid out the plugging of 1,162 wells (95 percent of its well-plugging goal) for fiscal year 2012. The cost associated with plugging the 764 wells the Commission plugged in fiscal year 2012 was $12,309,477. Table 1 summarizes the Commission's well-plugging goals and the number of wells the Commission reported it plugged in fiscal year 2012.

Table 1

Well-plugging Goals and Number of Wells Plugged
Fiscal Year 2012

District	Goal for Number of Wells to Plug	Wells Plugged or Under Bid or Contract to Plug			Percent of Goal Achieved
		Number of Wells Plugged	Number of Wells Under Bid or Contract to Plug	Total Number of Wells Plugged or Under Bid or Contract to Plug	
Districts 1 and 2 [a]	295	156	130	286	97%
District 3	102	71	91	162	159%
District 4	100	56	26	82	82%
Districts 5 and 6 [a]	140	95	23	118	84%
District 7B	175	207	59	266	152%
District 7C	45	31	53	84	187%
Districts 8 and 8A [a]	69	15	9	24	35%
District 9	291	128	7	135	46%
District 10	5	5	0	5	100%
Totals	**1,222**	**764**	**398**	**1,162**	**95%**

[a] A single district office monitors and reports combined well-plugging activity for these districts.

Source: Unaudited information the Commission provided.

In fiscal year 2013, the Commission had a goal to plug 815 wells. As of February 28, 2013, the Commission reported that it had plugged 245 wells during fiscal year 2013.

Recommendation

The Commission should maintain sufficient documentation showing (1) how it determines individual wells are eligible for plugging and (2) that the Commission approves each of those wells for plugging.

Management's Response

We agree with this recommendation. We agree that all state-managed plugging files should be permanently maintained at the Commission's headquarters in Austin. The Commission, under the records retention policy, films all state-managed plugging files as time permits for permanent storage.

Regarding the missing file mentioned in the report, a convenience copy of the file was maintained in the district office. As allowed by the record retention policy, the official record file has been re-built using the convenience copy, and is now maintained at the Austin headquarters.

Estimated implementation date: Implemented and ongoing.

Person responsible: Deputy Director of Field Operations, Oil and Gas Division

Chapter 2

The Commission Ensures That Operators Provide Required Financial Assurances, But It Should Strengthen Certain Controls Related to Those Financial Assurances

The Commission has designed and implemented effective processes and related controls to help ensure that:

> **Financial Assurances**
>
> Oil and gas well operators must provide financial assurances in one of the following forms:
>
> - An individual performance bond in the amount of $2 for each foot of total well depth for each well.
> - A blanket performance bond covering all wells operated. The amount of the bond ranges from $25,000 to $250,000, depending on the number of wells operated.
> - A letter of credit or cash deposit in the same amount required for an individual performance bond or blanket performance bond.
>
> Operators of wells in a bay are required to provide additional financial assurances of at least $60,000. Operators of offshore wells are required to provide additional financial assurances of at least $100,000.
>
> Sources: Title 16, Texas Administrative Code, Section 3.78, and Texas Natural Resources Code, Section 91.103.

- Oil and gas well operators provide the financial assurances that Texas Natural Resources Code, Chapter 91, requires in amounts consistent with state law and administrative rules (see text box for more information on financial assurances).
- The Commission collects on those financial assurances in accordance with administrative rules and the terms of agreements related to those financial assurances.

As of February 27, 2013, auditors' analysis of the Commission's operator data showed that the Commission held $378,443,900 in financial assurances from operators. Those financial assurances included:

- Letters of credit totaling $196,977,001.
- Bonds totaling $152,721,570.
- Cash totaling $28,745,329.

The Commission should improve certain controls to standardize its demand process to help ensure that it collects on financial assurances before they expire. In one instance, the Commission did not send a demand before that operator's financial assurance had expired.

Landowners with domestic gas wells are responsible for plugging the gas wells on their land, and they are not required to provide financial assurances. If the Commission plugs a domestic gas well, it uses state funds to pay for it.

Financial Assurances

The Commission's controls help to ensure that the Commission assesses and receives the correct financial assurances from operators. All 35 operators that auditors tested provided the correct amount of financial assurances. The Commission has automated controls to help ensure that it calculates the appropriate amount of financial assurance each operator must provide.

The Commission properly stores and accounts for financial assurances it receives in the form of bonds and letters of credit. The Commission has controls and processes to ensure that it safeguards those financial assurances. Specifically:

- The Commission stores financial assurance records in locked cabinets.
- The Commission requires staff to complete pull cards to document (1) the location of financial assurance records and (2) the names of the staff members responsible for financial assurance records they remove from the locked cabinets.
- The Commission physically secures the doors to the financial assurance work area and requires employees to use security badges to access that area.

Organizational Reports

Oil and gas operators must submit annual organizational reports to the Commission, and they cannot operate in the state without the Commission's approval of those reports. The organizational reports contain information such as an operator's location, organizational structure, and officers.

The Commission identifies when an operator does not submit its annual organizational report and designates the operator as delinquent. The Commission uses this as an indicator that an operator could have abandoned a well and the operator's responsibilities for maintaining that well. Ultimately, this can prompt the Commission to collect on the operator's financial assurance and plug the well.

Sources: Title 16, Texas Administrative Code, Section 3.1, and information the Commission provided.

The Commission also has a process to help ensure that (1) its processing of financial assurances is accurate and (2) data entry for the organizational reports that operators submit is accurate (see text box for additional details on organizational reports). The Commission properly entered all of the key data from hard-copy documentation operators submitted into its mainframe system for the 60 operators that auditors tested. The key data tested included the operator's organizational status, financial assurance amount, and address.

Demand Process

The Commission has adequate processes and controls to help ensure that it sends demand notices to operators that do not submit required annual organizational reports. Specifically, the Commission sends a demand notice that informs the operator and the operator's financial assurance issuer that the Commission is collecting on the operator's financial assurance due to noncompliance with Commission requirements. As of February 27, 2013, auditors' analysis of the Commission's operator data showed that 2,966 operators were delinquent in submitting their required annual organizational reports.

In 63 (98 percent) of the 64 cases that auditors tested, the Commission appropriately sent demands to collect on operators' financial assurances. In one instance, however, the Commission did not send a demand before that operator's financial assurance (a letter of credit) had expired; that resulted in the Commission not being able to collect on that operator's $25,000 letter of credit. The Commission must send a demand on a letter of credit within 90 days of the date an operator's organizational report is delinquent.

The Commission has an informal process to help ensure that it sends demand notices on time; however, it has not documented that process to help ensure that it standardizes its process so that it can collect on financial assurances before they expire. That increases the risk that the State could incur well-plugging expenses that could have been paid for by operators' financial assurances.

Domestic Gas Wells

Landowners with domestic gas wells are not required to provide financial assurances. A domestic gas well is a gas well that an operator transfers to a landowner at the end of the gas well's productive life, and the landowner uses the remaining gas for personal or domestic use only. When the gas wells are transferred to the landowners, the operators are released from responsibility for plugging the gas wells and from the financial assurances they previously provided to the Commission associated with those gas wells. The landowners are responsible for plugging those gas wells, and they are not required to provide financial assurances. If the Commission plugs a domestic gas well, the Commission uses state funds to pay for it.

Table 2 provides information on the estimated cost associated with plugging domestic gas wells.

Table 2

Estimated Cost to Plug Landowners' Domestic Gas Wells (as of February 27, 2013)	
Category	**Number or Dollar Amount**
Number of domestic gas wells	222
Total aggregate depth in feet of all domestic gas wells	636,487
Estimated cost per foot to plug domestic gas wells (according to the Commission's financial assurance terms and conditions)	$2.50
Total estimated cost to plug landowners' domestic gas wells	$1,591,218

Source: Auditor analysis based on information the Commission provided.

The actual cost to plug domestic gas wells could exceed the estimated cost.

Recommendation

The Commission should develop and implement documented policies and procedures to standardize its demand process to help ensure that it collects on operators' financial assurances, when appropriate, before they expire.

Management's Response

We agree with this recommendation. As noted in the report, the P-5 unit has an "informal process" regarding demand procedures under which it has been operating. We memorialized this process in a written policy and procedure document effective early June 2013.

The specific instance of non-collection referred to in the report occurred following a P-5 delinquency in July 2006. Since then, we addressed this issue by using a monthly "Collections Listing" mechanism. To ensure that all necessary demands have been issued, the P-5 manager reviews, on a monthly basis, the listing of operators for whom collection is appropriate. This quality control step will prevent similar events from happening in the future.

Estimated implementation date: Implemented.

Person responsible: Assistant Director of Administrative Compliance, Oil and Gas Division

Chapter 3

The Commission Has Adequate Information Technology Systems Controls, But It Should Strengthen Controls in Certain Areas

The Commission has adequate controls over its mainframe and its Oilfield Cleanup (OFCU) application in the following areas:

- Information technology security policies.
- User access policies.
- Use of generic user id accounts.
- Change management policies.
- Password controls for applications.
- Physical controls over the data center that houses the Commission's mainframe.

> **Oil and Gas Division Systems Audited**
>
> **Mainframe** – The Oil and Gas Division maintains data on operators, organizational reports, wells, production, financial assurances, and enforcement actions on a mainframe that is housed in the State's Austin Data Center.
>
> **Oilfield Cleanup (OFCU) Application** – The Oil and Gas Division uses this Web-based system to maintain data on wells recommended for plugging. That data includes priority calculations, high-risk well fluid test results, and the costs of plugging wells. The Oil and Gas Division also uses the OFCU application to produce reports on daily plugging activities; wells recommended for plugging but not yet plugged; and wells that have been plugged, including estimated and actual costs. The OFCU application is housed in the Commission's data center.

Auditors determined that the data in the Commission's mainframe and OFCU application was sufficiently reliable for the purposes of this audit (see text box for information on the Commission's mainframe and OFCU application).

However, the Commission should strengthen certain controls for its mainframe and OFCU application in the following areas:

- Review of user access.
- Segregation of programmer duties.
- Password controls for servers.
- Physical controls over the Commission's data center.

Review of User Access

Privileged accounts for the Commission's mainframe are appropriate. However, the Commission has not removed 5 user accounts for the OFCU application, 1 user account for the OFCU database, and 46 user accounts for the OFCU servers that are associated with former employees and former data center staff.

The Commission does not periodically review user accounts for its mainframe and OFCU application as required by its policy and the Texas Administrative Code. The Commission's information security policy requires the Commission to (1) update user accounts of individuals who separate from the Commission and (2) periodically review existing user accounts for validity. In addition, Title 1, Texas Administrative Code, Section 202.25, states that a user's access authorization must be appropriately modified or removed when the user's employment or job responsibilities within an agency change. Not reviewing user access increases the risk of unauthorized access to systems and the loss or destruction of data.

Segregation of Programmer Duties

The Commission has appropriately segregated duties between programming staff and the production environment for its mainframe, but not for the OFCU application. Two programmers have the ability to develop or change code for the OFCU application and migrate that code to the production environment.

The Commission asserts that staffing shortages prevent segregation of duties, but that its programmers do not have coding responsibilities for the code changes they migrate to the production environment. Auditors did not identify any instances in which the two programmers were assigned to change code for the OFCU application. However, as discussed above, those individuals still have the ability to develop or change code and migrate that code to the production environment, and those activities could potentially go undetected.

Title 1, Texas Administrative Code, Section 202.20, states that (1) changes shall be made only in an authorized manner, (2) assets shall be protected from unauthorized modifications, and (3) state agencies shall ensure adequate controls and separation of duties for tasks that are susceptible to fraudulent or other unauthorized activity. When duties are not segregated, there is a risk that unauthorized changes could be made to production systems and data, which could compromise the integrity of systems and data.

Password Controls for Servers

The Commission's password controls on two of its servers do not meet industry best practices. Although the Commission's information technology security policy for passwords for its network meets industry best practices, the Commission's policy does not specify those same standards for passwords for all of its systems and servers. Auditors provided additional details on the password control weaknesses to the Commission.

Title 1, Texas Administrative Code, Section 202.25, requires passwords to be based on industry best practices for password usage and documented state agency risk management decisions. Weaknesses in passwords increase the risk of unauthorized user access, which can compromise the integrity of a system and its data.

Physical Controls Over the Commission's Data Center

Physical and environmental controls over the Austin Data Center (which houses the Commission's mainframe) are adequate. The Commission has physical controls over its data center (which houses the OFCU application); however, it should improve certain controls. The Commission does not regularly monitor the physical maintenance and safety inspection schedule for its data center.

Title 1, Texas Administrative Code, Section 202.23, requires agencies to protect information resources from environmental hazards and requires that designated employees be trained to monitor environmental control procedures and equipment. Not ensuring that environmental protection systems function as intended places staff, equipment, systems, and data at risk.

The Commission also does not consistently document when visitors physically access its data center. Weak physical access controls can result in unauthorized access, which can compromise the facility, equipment, systems, and data. Title 1, Texas Administrative Code, Section 202.23, requires agencies to document and manage physical access to mission-critical information resources facilities to ensure the protection of those resources from unlawful or unauthorized access, use, modification, or destruction.

Recommendations

The Commission should:

- Perform and document periodic reviews of user accounts to help ensure that users' access to the mainframe and applications are appropriate.
- Segregate duties so that programmers cannot both develop or change code for the OFCU application and migrate that code to the production environment.
- Strengthen password controls on servers with password weaknesses to ensure that those controls meet industry best practices.
- Regularly monitor the physical maintenance and safety inspection schedule of its data center and monitor the implementation of corrective actions to address deficiencies identified during inspections.
- Consistently document the names of visitors who physically access its data center and the dates and times when they enter and exit.

Management's Response

The Commission should:

- *Perform and document periodic reviews of user accounts to help ensure that users' access to the mainframe and applications are appropriate.*

Response: *We agree with this recommendation. The Commission will implement an annual review procedure of user accounts to help ensure that users' access to the mainframe and applications are appropriate.*

The Information Security Officer will coordinate efforts with the Security Coordinator of the Oil and Gas Services Division and document the completion of the reviews with positive confirmations from the responsible program areas to ensure that reviews are completed annually.

Estimated implementation date: *Implemented and ongoing annually*

Person responsible: *Information Security Officer and Oil and Gas Division Security Coordinator*

- *Segregate duties so that programmers cannot both develop or change code for the OFCU application and migrate that code to the production environment.*

  Response: *We agree with this recommendation. The Commission will move the software release procedure from the Application Development and Maintenance Section to the Customer Service and Operations Section of the Information Technology Services Division to ensure that programmers cannot both develop or change code for the OFCU application and migrate that code to the production environment.*

  Estimated implementation date*: September 1, 2013*

  Person responsible: *Information Security Officer*

- *Strengthen password controls on servers with password weaknesses to ensure that those controls meet industry best practices.*

  Response: *We agree with this recommendation. The Commission will continue to comply with standards set forth within TAC 202.25, Commission Security Guidelines and the Austin Data Center Password standards. The Commission will file ISEC exemption requests or comply with the DIR procedures to accommodate password strength limitations where and when necessary upon migration to the Austin Data Center.*

  Estimated implementation date: *Ongoing*

  Person responsible: *Information Security Officer*

- *Regularly monitor the physical maintenance and safety inspection schedule of its data center and monitor the implementation of corrective action to address deficiencies identified during inspections.*

  Response: *We agree with this recommendation. The Commission will implement procedures, which allow for monitoring of the physical* *maintenance and safety inspection schedule of its data center and monitoring of the implementation of corrective action to address deficiencies identified during inspections.*

Estimated implementation date: *September 1, 2013*

Person responsible: *Information Security Officer*

- *Consistently document the names of visitors who physically access its data center and the dates and times when they enter and exit.*

  Response: *We agree with this recommendation. The Commission will implement a logging procedure to document the names of visitors who physically access its data center and the dates and times when they enter and exit.*

  Estimated implementation date: *September 1, 2013*

  Person(s) *responsible: Information Security Officer*

Appendices

Appendix 1

Objectives, Scope, and Methodology

Objectives

The audit objectives were to determine whether the Railroad Commission (Commission):

- Has established and adheres to a risk assessment process to prioritize the plugging of wells with state funds.
- Has designed and implemented effective processes and related controls to help ensure that (1) regulated entities establish and maintain the financial assurance required by Texas Natural Resources Code, Chapter 91, in amounts consistent with state law, administrative rules, and Commission policy and (2) the Commission collects funds from those sources in accordance with Commission policies and procedures, administrative rules, and the terms of agreements related to that financial assurance.

Scope

The audit scope included reviewing records for oil and gas wells for eligibility for plugging with state funds and the associated financial assurances for fiscal year 2012 and fiscal year 2013 through February 2013.

Methodology

The audit methodology included collecting information and documentation from the Commission; reviewing policies and procedures, statutes, and rules related to state-funded well-plugging and financial assurances; and analyzing and evaluating data and the results of tests. Specifically, auditors reviewed oil and gas well inspection records, documentation recommending wells for state-funded plugging, operators' organizational reports, and financial assurance documentation.

Auditors assessed the reliability of the operator and well data used in the audit by (1) reviewing general controls and application controls for the Commission's mainframe system and Oilfield Cleanup (OFCU) application, (2) comparing data to other sources of information, (3) analyzing key data elements for completeness and reasonableness, and (4) interviewing Commission employees knowledgeable about the data. Auditors determined that the data was sufficiently reliable for the purposes of this audit.

Auditors selected non-statistical samples primarily through random selection designed to be representative of the population. In those cases, results may be extrapolated to the population but the accuracy of the extrapolation cannot be measured. In some cases, auditors used professional judgment to select additional items for testing. Those sample items generally are not representative of the population and, therefore, it would not be appropriate to extrapolate those results to the population.

To test records for wells, auditors selected non-statistical, random samples of wells recommended for state-funded plugging based on priority data from the OFCU application. Auditors stratified the samples based on the total number of wells per priority in the population.

To test whether (1) operators provided the correct amount of financial assurances, (2) the Commission properly secured and accounted for financial assurances, and (3) the Commission sent demand notices to operators, auditors selected a non-statistical, random sample of 30 operators from the mainframe system for each of the tests performed. Auditors also selected targeted samples of operators for each test based on additional factors.

To test whether (1) the Commission accurately entered key data into its mainframe system and (2) the Commission demanded financial assurances before they expired, auditors determined that risk was high and that a sample size of more than 30 was required. As a result, auditors selected a non-statistical, random sample of 60 operators from the mainframe system for each of the tests performed. Auditors also selected targeted samples of operators to test whether the Commission demanded financial assurances before they expired based on additional factors.

<u>Information collected and reviewed</u> included the following:

- Commission policies and procedures.
- The Commission's *State Managed Plugging Manual.*
- Title 16, Texas Administrative Code, Chapter 3.
- Title 1, Texas Administrative Code, Chapter 202.
- Texas Natural Resources Code, Chapters 52, 81, 89, and 91.
- General Appropriations Act (82nd Legislature).
- Commission operator and well data.
- Commission well-plugging records and reports.
- Commission fiscal year 2012 and 2013 operational goals for plugging wells.
- Commission financial assurance and organizational report records.

- Commission well inspection records.

Procedures and tests conducted included the following:

- Interviewed Commission management and staff, including staff at the Oil and Gas Division district offices.
- Analyzed data pertaining to annual well-plugging goals and oil and gas wells plugged.
- Reviewed and tested compliance with Commission policies and procedures, Texas Administrative Code, and the Texas Natural Resources Code requirements for (1) plugging wells with state funds and (2) assessing and collecting financial assurances from operators.
- Reviewed general and application controls over the Commission's mainframe system and OFCU application.

Criteria used included the following:

- Commission policies and procedures.
- The Commission's *State Managed Plugging Manual.*
- Title 16, Texas Administrative Code, Chapter 3.
- Title 1, Texas Administrative Code, Chapter 202.
- Texas Natural Resources Code, Chapters 52, 81, 89, and 91.
- Financial assurance agreement terms and conditions.

Project Information

Audit fieldwork was conducted from January 2013 through May 2013. 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:

- Jennifer Lehman, MBA, CIA, CFE, CGAP (Project Manager)
- Lilia C. Srubar, CPA (Assistant Project Manager)
- Jason Carter

- Cyndie Holmes, CISA
- Norman G. Holz II
- Justin Saunders
- Dennis Ray Bushnell, CPA (Quality Control Reviewer)
- James Timberlake, CIA (Audit Manager)

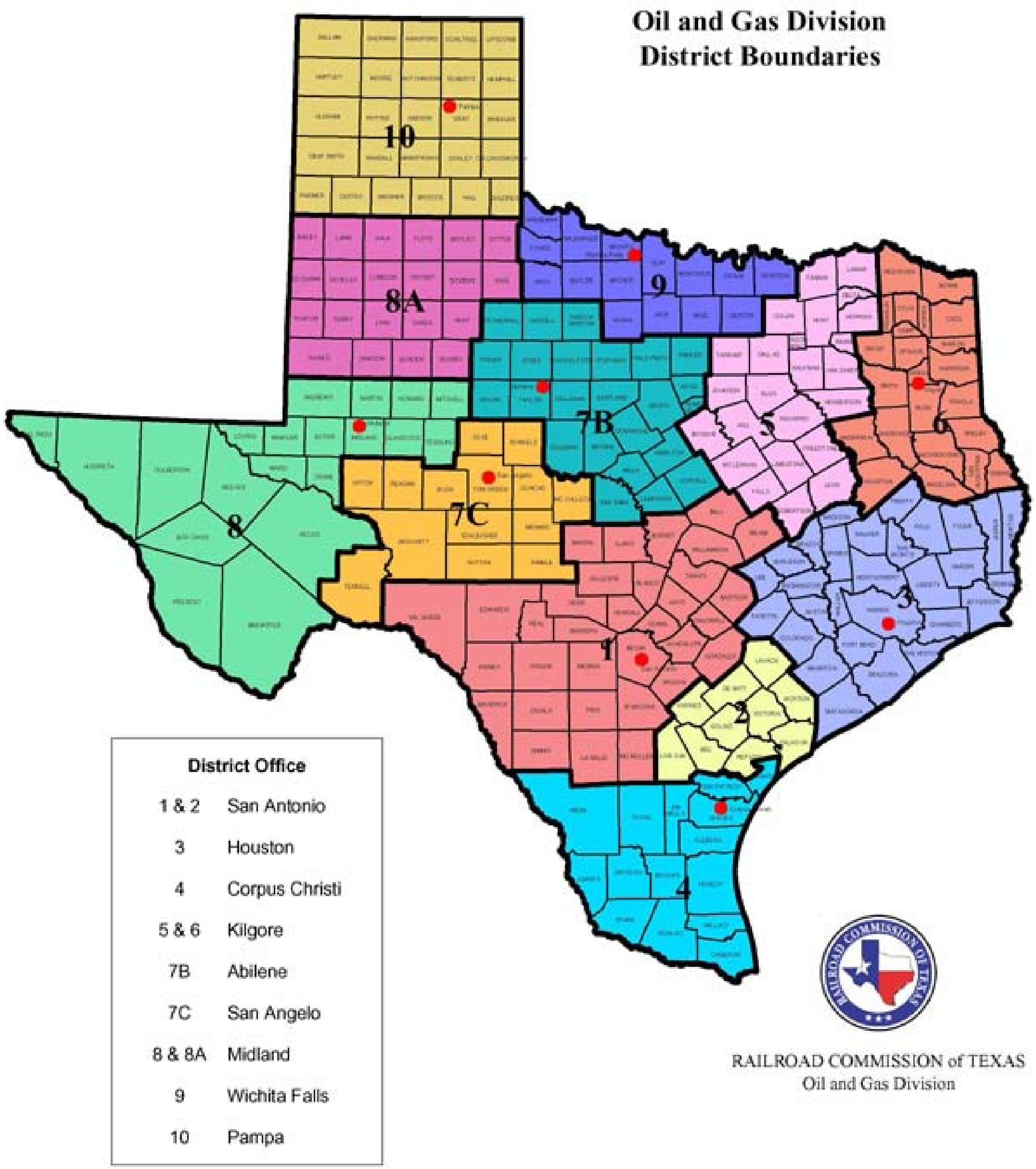
Appendix 2

Districts in the Railroad Commission's Oil and Gas Division

Figure 1 shows the districts in the Railroad Commission's Oil and Gas Division.

Figure 1

Districts in the Railroad Commission's Oil and Gas Division



Source: Railroad Commission.

Appendix 3

Related State Auditor's Office Work

Related State Auditor's Office Work		
Number	**Product Name**	**Release Date**
12-005	An Audit Report on Pipeline Safety at the Railroad Commission	November 2011
07-046	An Audit Report on Inspection and Enforcement Activities in the Field Operations Section of the Railroad Commission	August 2007

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 Thomas “Tommy” Williams, Senate Finance Committee
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

Railroad Commission

Members of the Railroad Commission
- The Honorable Barry T. Smitherman, Chairman
- The Honorable Christi Craddick
- The Honorable David Porter

Mr. Milton Rister, Executive Director