

FINANCE COMMISSION OF TEXAS
AUDIT COMMITTEE MEETING

Friday, June 10, 2016
8:00 a.m.

Finance Commission Building

Public comment on any agenda item or issue under the jurisdiction of the Finance Commission agencies is allowed unless the comment is in reference to a rule proposal for which the public comment period has ended. However, upon majority vote of the Commission, public comment may be allowed related to final rule adoption.

- A. Review and Approval of Minutes of the April 15, 2016, Audit Committee Meeting
- B. Audit Committee Review of Agencies' Activities
- C. Discussion of and Possible Vote to Recommend that the Finance Commission Take Action on the Office of Consumer Credit Commissioner's Fiscal Year 2016 Annual Internal Audit Report as Prepared and Presented by Garza/Gonzalez and Associates
- D. Discussion of and Possible Vote to Recommend that the Finance Commission Take Action on the Department of Banking's Fiscal Year 2016 Annual Internal Audit Report as Prepared and Presented by Garza/Gonzalez and Associates
- E. Discussion of and Possible Vote to Recommend that the Finance Commission Take Action on the Internal Auditor Contract for Garza/Gonzalez & Associates for Fiscal Year 2017
- F. Report on Activities Relating to the Texas Financial Education Endowment Fund

NOTE: The Audit Committee may go into executive session (close its meeting to the public) on any agenda item if appropriate and authorized by the Open Meetings Act, Texas Government Code, Chapter 551.

Meeting Accessibility: Under the Americans with Disabilities Act, the Finance Commission will accommodate special needs. Those requesting auxiliary aids or services should notify the Texas Department of Banking, 2601 North Lamar Boulevard, Austin, Texas 78705, (512) 936-6222, as far in advance of the meeting as possible.

This page left blank intentionally.

**MINUTES OF THE
AUDIT COMMITTEE MEETING
Friday, April 15, 2016
8:00 a.m.**

The Audit Committee of the Finance Commission of Texas convened at 8:00 a.m. on April 15, 2016, with the following members present:

Audit Committee Members in Attendance:

Molly Curl, Chairman

Hector Cerna

Lori McCool

Audit Committee Chairman Curl announced that there was a quorum of the Audit Committee of the Finance Commission of Texas with three members present *(0:01 on audio file)*.

AGENDA ITEM	ACTION	LOCATION ON AUDIO FILE
A. Review and Approval of Minutes of the February 19, 2016, Audit Committee Meeting	Lori McCool made a motion to approve the minutes of the February 19, 2016 Audit Committee Meeting. Hector Cerna seconded and the motion passed.	0:43 start of discussion 0:49 vote
B. Audit Committee Review of Agencies' Activities	No Action Required.	1:26 start of discussion
C. Discussion of and Possible Vote to Recommend that the Finance Commission Take Action on the Agencies' February 29, 2016 Investment Officer Reports: 1. Office of Consumer Credit Commissioner 2. Texas Department of Banking 3. Department of Savings and Mortgage Lending	Lori McCool made a motion to recommend that the Finance Commission take action on the agencies' February 29, 2016 Investment Officer Reports. Hector Cerna seconded and the motion passed.	4:07 start of discussion 14:15 vote
D. Discussion of and Possible Vote to Recommend that the Finance Commission Take Action on the Agencies' 2016 Second Quarter Financial Statements: 1. Office of Consumer Credit Commissioner 2. Texas Department of Banking 3. Department of Savings and Mortgage Lending	Lori McCool made a motion to recommend that the Finance Commission take action on the agencies' 2016 Second Quarter Financial Statements. Hector Cerna seconded and the motion passed.	14:35 start of discussion 27:48 vote

E. Report on Activities Relating to the Texas Financial Education Endowment Fund	No Action Required	28:06 start of discussion
--	--------------------	---------------------------

There being no further business of the Audit Committee of the Finance Commission of Texas, Molly Curl adjourned the meeting at 8:38 a.m. (38:44) *on audio file*)

Molly Curl, Audit Committee Chair
Finance Commission of Texas

Charles G. Cooper, Executive Director
Finance Commission of Texas

Anne Benites, Executive Assistant
Finance Commission of Texas

**Department of Savings and Mortgage Lending
Outstanding Audit Issues Report as of May 31, 2016**

None.

This page left blank intentionally.

Office of Consumer Credit Commissioner

There are currently no outstanding audit items.



STEVEN C. McCRAW
DIRECTOR
DAVID G. BAKER
ROBERT J. BODISCH, SR.
DEPUTY DIRECTORS

TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N. LAMAR BLVD. - BOX 4143 - AUSTIN, TEXAS 78765-4143
CRIME RECORDS SERVICE
512 / 424-7364



COMMISSION
CYNTHIA LEON, CHAIR
MANNY FLORES
FAITH JOHNSON
STEVEN P. MACH
RANDY WATSON

March 14, 2016

Ms. Leslie Pettijohn
Consumer Credit Commission
2601 N. Lamar Blvd.
Austin, TX 78705

Subject: Texas Dept. of Public Safety On-Site Audit

Dear Ms. Pettijohn:

Enclosed is the report on your recent non-criminal justice audit, which was performed on March 10, 2016 by Karen Germo and Susanne Dial-Herrera, Field Representatives from the Texas Department of Public Safety. The audit consisted of an interview with Mirand Zepeda, as designated by your agency. The interview specifically covered the non-criminal justice audit process as it pertains to state and federal laws.

After the interview, the auditor reviewed your organization's access, use, dissemination, storage, security and destruction of criminal history record information.

In order for our audit program to comply with state and federal laws, we must request that you address the **Required Actions** indicated in the report. **Please advise us in writing by April 23, 2016 of the actions you have taken to address the identified area(s). Failure to respond could result in sanctions for the agency.**

Please send response to:

Susie Dial-Herrera, Audit Supervisor
P O Box 4143
Austin, Texas 78765-4143
512/424-7927

Sincerely,

Mike Lesko, Deputy Assistant Director
Law Enforcement Support Division
Crime Records Service

ML/kpg

2016 MAR 28 PM 1:24
RECEIVED
CRIME RECORDS SERVICE
DPS Audit

DPS Audit Form AD-6

TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N LAMAR BLVD • BOX 4087 • AUSTIN, TEXAS 78773-0001
CRIME RECORDS SERVICE
512/424-7364



STEVEN C. McCRAW
DIRECTOR
DAVID G. BAKER
ROBERT J. BODISCH, SR.
DEPUTY DIRECTORS



COMMISSION
A CYNTHIA LEON, CHAIR
MANNY FLORES
FAITH JOHNSON
STEVEN P. MACH
RANDY WATSON

March 14, 2016

NON CRIMINAL JUSTICE AUDIT REPORT

Consumer Credit Commission
OrgID 174 / STATE-ND 0101E
ORI# TX920460Z

SUMMARY

The Texas Department of Public Safety (DPS) and Federal Bureau of Investigation (FBI) have established audit programs for the purposes of evaluating a criminal and non-criminal justice agency's compliance with state and federal statutes, regulations, policies, and procedures for the access, use, dissemination, storage, security, and destruction of criminal history record information.

TRAINING

During training, the following topics and others not listed here were discussed as baseline security awareness for all authorized personnel with access to criminal history record information: statutes and rules that describe the responsible access and dissemination of criminal history record information; protection of confidential information; threats, vulnerabilities, and risks associated with the handling of criminal history record information; visitor control and physical access to areas containing criminal history record information; electronic storage; destruction; and penalties for non-compliance.

As a reminder, *all* personnel with access to the DPS Secure Site must pass a DPS criminal history check. If you have any questions, please contact us at 512-424-7364.

AUDIT RESULTS

The DPS Access and Dissemination Bureau's Training and Audit Unit, recently conducted an on-site audit in reference to the security of the criminal history record information your agency receives from the DPS, and if applicable, the FBI. This audit report is based on Texas and Federal law regulating the access and dissemination of criminal history record information. [Reference: Texas Government Code 411 and the CJIS Security Policy].

AREAS AUDITED

ACCESS TO CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.083(b) (2) requires the DPS to grant access to criminal and non-criminal justice agencies authorized by state or federal statute, or executive order to receive criminal history record information.

2016 MAR 28 11:24

CRIMINAL HISTORY RECORD INFORMATION RECEIVED

A criminal and non-criminal justice entity must provide the DPS with the name, sex, race, date of birth, and working title of each employee/official who will access and utilize information received from DPS databases. The DPS will conduct a name-based criminal history record check on each name submitted, and reserves the right to require a fingerprint-based criminal history record check on any employee/official. Only persons approved by the DPS will be granted access to DPS databases or information on behalf of the entity. Any person who is not granted access due to the results of the name-based criminal history record check may dispute the findings through the submission of their fingerprints.

Important: The DPS reserves the right to limit the number of authorized employees/officials with access to DPS databases and information. In addition, DPS will strictly enforce the most restrictive set of rights, privileges, and guidelines governing access to DPS databases and information.

Finding: Out of Compliance

- **Former employee was not disabled as a data user.**

Required Action(s):

- **The agency, upon termination of individual employment, shall immediately terminate access to CJI.**

USE OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.084(a) Criminal history record information obtained from the department under this subchapter, including any identification information that could reveal the identity of a person about whom criminal history record information is requested and information that directly indicates or implies involvement of a person in the criminal justice system: (1) is for the exclusive use of the authorized recipient of the information; and (2) may be disclosed or used by the recipient only if, and to the extent that, disclosure or use is authorized or directed by: (A) this subchapter; (B) another statute; (C) a rule adopted under a statute; or (D) an order of a court of competent jurisdiction.

(a-1) The term "criminal history record" information under Subsection (a) does not refer to any specific document produced to comply with this subchapter but to the information contained, wholly or partly, in a document's original form or any subsequent form or use.

(b) Notwithstanding Subsection (a) or any other provision in this subchapter, criminal history record information obtained from the Federal Bureau of Investigation may be released or disclosed only to a governmental entity or as authorized by federal law and regulations, federal executive orders, and federal policy.

(c) An agency or individual may not confirm the existence or nonexistence of criminal history record information to any person that is not eligible to receive the information.

(d) If your agency is utilizing the Fingerprint-based Applicant Clearinghouse of Texas (FACT), records must be unsubscribed to when you are no longer entitled to access the information, per Government Code 411.0845.

2016/11/28
11:26
CJL:COMB/EDD
RECEIVED
IN COMPLIANCE

Finding: Out of Compliance

- **There was no supporting documentation for two of the thirty nine name-based CCH searches performed. There were also four fingerprint subscriptions of the fifteen verified that had no documentation for purpose.**

Required Action(s):

- **The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes.**

DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.083(a) Criminal history record information maintained by the department is confidential information for the use of the department and, except as provided by this subchapter, may not be disseminated by the department. (b) The department shall grant access to criminal history record information to: (1) criminal justice agencies; (2) non-criminal justice agencies authorized by federal statute or executive order or by state statute to receive criminal history record information.

(d) The department is not required to release or disclose criminal history record information to any person that is not in compliance with rules adopted by the department under this subchapter or rules adopted by the Federal Bureau of Investigation that relate to the dissemination or use of criminal history record information.

Important: Access to DPS and FBI criminal history record information by authorized employees/officials is subject to cancellation if dissemination of information is made outside the receiving department, related agency, or authorized entity. In addition, access to DPS and FBI criminal history record information may not be disseminated to a person not authorized to receive the information. Criminal penalties (Government Code 411.085) are also in place for the improper dissemination of criminal history record information.

Finding: In-Compliance

Required Action(s): None

STORAGE AND SECURITY OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Agencies are required to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security and integrity.

Per the DPS Databases and CJIS Security Policy: the computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any stored data; the location of all criminal history record information received from the DPS and FBI must have adequate physical security to protect against any

unauthorized viewing or access to displayed, stored or printed criminal history record information at all times; passwords must be secure to prevent unauthorized access; the auto save password feature should be disabled to prevent unauthorized logon; ensure that computer terminals have session lock features of less than thirty minutes; user access must be terminated when access is no longer authorized; file cabinets must have locks.

Finding: Out of Compliance

- **Individuals that are no longer licensed or expired have not been unsubscribed to in the Clearinghouse per GC §411.0845. At the time of the audit, the agency's policy was not available in regards to not unsubscribing to licensees until 180 days after expiration of license.**
- **CCH and fingerprint card information scanned into their Document Management system has not been removed.**
- **Database storing CHRI could not be verified if it is encrypted.**
- **One monitor allows unauthorized viewing as it is by the door and can be viewed by all that pass by.**
- **Password was auto saved.**
- **The DPS Secure Site online training had not been taken by several data users at the time of the audit.**
- **The CJIS Security Awareness Training had individuals entered but none had taken the training at the time of the audit.**
- **IT individuals that have access to the Document Management database containing CJI have not been vetted.**

Required Action(s):

- **Unsubscribe to records upon end of license or employment as you are no longer entitled to access the CHRI per TX GC§411.0845. If there is a regulation in place to this effect, we would need a copy, and it must be approved by DPS in order to coexist with the current statute.**
- **Recommend purging all old CHRI from system and over writing.**
- **Electronic storage should be encrypted and a FIPS certification provided.**
- **The agency shall control physical access to information system devices that display CJI and shall position information system devices in such a way as to prevent unauthorized individuals from accessing and viewing CJI.**

- Secure Site online training is mandatory for all DPS Secure Site approved data users.
- Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.
- These requirements apply to all personnel who have access to unencrypted CJI including those individuals with only physical or logical access to devices that store, process or transmit unencrypted CJI. For your employees:
 To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment.
 Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.

DESTRUCTION OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Destruction of criminal history record information must be performed by authorized personnel. Agencies with access to criminal history record information must follow their 411 statute and the CJIS Security Policy regarding the destruction of criminal history record information. If the 411 statute does not provide a destruction timeframe, then the agency should follow the recommended timeframe presented during training or contact the training and audit unit to discuss a reasonable timeframe.

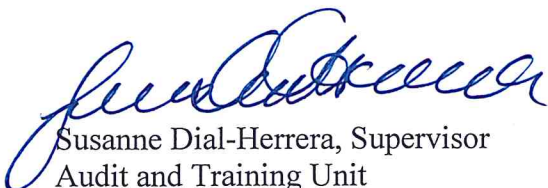
Finding: In-Compliance

Required Action(s): None

OTHER RECOMMENDATIONS OR MINOR INFRACTIONS:

- Secure Site users were unaware of the DPS Security policy.
- There was no policy in place at the time of the audit that would guide the treatment of CHRI.

Sincerely,



Susanne Dial-Herrera, Supervisor
 Audit and Training Unit
 Access and Dissemination Bureau
 Crime Records Service



April 22, 2016

Mike Lesko
Texas Department of Public Safety
5805 N. Lamar Blvd. - Box 4143
Austin, Texas 78765-4143

RE: OCCC's Response to Non-Criminal Justice Audit Report
OrgID 174/STATE-ND 0101E; ORI#TX920460Z

Dear Mr. Lesko:

We have received your report dated March 14, 2016 regarding the audit conducted on March 10, 2016 identified above. After reviewing the report's findings, the Office of Consumer Credit Commissioner (OCCC) has addressed the issues identified, and taken the required actions, as further described below.

Access to criminal history record information

Finding and Required Action: The audit found that a former employee was not disabled as a data user. Based on this finding, DPS required the OCCC to terminate an employee's access to CJI immediately upon termination of employment.

Response: The former employee identified in the report had left the agency's employment four business days before the audit was conducted. Following the audit, the OCCC disabled this employee's login access to the DPS computerized criminal history database. The OCCC has also revised its procedures to disable the access of an employee to CJI immediately upon termination.

Use of criminal history record information

Finding and Required Action: The audit found that there was no supporting documentation for two of the thirty-nine name-based CCH searches performed, and there were four fingerprint subscriptions of the fifteen verified that had no documentation for purpose. The audit required the agency to retain audit records for at least one year, and no longer needed for any purpose.

Response: The OCCC believes there is a typographical error in this finding. Specifically, the audit verified fifty (50) rather than fifteen (15) fingerprint subscriptions. Of these 50, the OCCC was not able to verify the purpose of four subscriptions during the audit. After the audit, the OCCC was able to verify that one subscription was initiated in connection with an active license.

The agency continues to believe that these three issues related to applicants for a license during the test period. The agency suspects that these three anomalies resulted from a loss of certain data fields during a transfer of data from the previous licensing database into the current (ALECS) licensing system. The agency will continue its efforts to identify the historical facts related to this problem, and to identify any additional anomalies in order to ensure future compliance.

The agency is currently reviewing and revising its records retention policy pursuant to Texas law. However, the OCCC currently retains, and will continue to retain, application, license, and registration information for at least one year and until no longer needed for any purpose. In addition, the OCCC continues to enhance systems, databases, and processes to make relevant information easily accessible.

Storage and security of criminal history record information

Finding and Required Action: The audit found that individuals that are no longer licensed had not been unsubscribed to the DPS clearinghouse. The audit required the agency to unsubscribe to records upon the end of a license or employment.

Response: In order to unsubscribe persons, DPS requires the agency to identify each person by a state issued identification number (SID). This number is generated by DPS, and the OCCC does not capture or retain this number as part of its licensing activities. As a result, it is very difficult as a practical matter for the OCCC to accurately identify and efficiently unsubscribe individuals after the expiration of their license.

Before the audit, the OCCC identified 2,529 persons who should be unsubscribed based on exact name matches. On two occasions (March 7, 2016 and March 11, 2016), the agency attempted to unsubscribe these persons. However, the agency has been unable to obtain confirmation from DPS that these attempts were successful. Therefore, the OCCC requests DPS assistance to clarify and resolve this situation.

The OCCC has identified an additional 6,358 persons who may need to be unsubscribed, but was unable to obtain an exact name match. The agency is concerned that some of these individuals are actively licensed. If so, the act of unsubscribing would prevent the agency from receiving future criminal justice information about these persons and taking appropriate action based on such information. While the agency continues to seek possible solutions, we request DPS assistance to clarify and resolve this situation.

Finding and Required Action: The agency was not able to produce its policy justification for continuing subscriptions for 180 days after expiration of a license. The audit required the agency to produce its policy justification.

Response: Section 349.303 of the Finance Code permits a person to pay a late filing fee, and renew an expired license not later than the 180th day after its expiration. A significant number of expired licenses are renewed in this manner each year. Accordingly, the agency retains authority to monitor CJI concerning such expired licenses until the 181st day after expiration.

Finding and Required Action: The audit found the agency could not verify if CHRI stored in its database was encrypted. The audit report recommended that the agency to purge and overwrite all old CHRI from its system, and encrypt all data.

Response: The OCCC has purged all old CHRI from the document manager system and we are no longer electronically storing any CHRI information. This action was confirmed by email sent by the OCCC's Mirand Zepeda to Karen Germo and Susanne Dial-Herrera on March 18, 2016.

Finding and Required Action: The audit found one computer monitor was positioned to allow unauthorized viewing, and that a password on one computer was automatically saved. The report required the agency to control access to information systems that display CJI and prevent unauthorized access.

Response: A privacy screen was purchased for the computer monitor to prevent unauthorized viewing, and the automatically saved password has been deleted. Users have received refresher training on security measures.

Finding and Required Action: The audit found that several users had not taken the DPS Secure Site online training, and that no user had taken the CJIS Security Awareness Training. The report required the agency to ensure all users take the required training within the prescribed deadlines.

Response: All OCCC users of the DPS Secure Site have completed the required training. All OCCC staff with access to CJI have completed the CJIS training.

Finding and Required Action: The report found that IT staff with access to the Document Management database containing CJI had not been subject to a background check. The report requires all employees with access to CJI to be subject to a "state of residency and national fingerprint-based record check" within 30 days of employment.

Response: The agency believes this finding was made in error. All staff with access to CJI have been identified as users, and DPS has conducted a name-based background check on all users. Page two of the audit report states that DPS runs a name-based check on all OCCC users, and reserves the right to run fingerprint-based check if necessary. This statement is consistent with the clarification DPS Auditor Karen Germo gave to the OCCC on April 4, 2016.

In addition, we have reviewed the FBI's Criminal Justice Information (CJIS) Security Policy; Version 5.4 dated October 6, 2015. Appendix J to this document is a supplemental guide for noncriminal justice agencies such as the OCCC. At the bottom of page J-7, this document states "Agencies located within states that have not passed legislation authorizing or requiring civil fingerprint-based background checks are exempted from this requirement until such time as appropriate legislation has been written into law." (Similar language was included in the prior edition [Version 5.3, dated August 4, 2014] at pages J1-J2). Texas law does not currently authorize or require such checks. Therefore, the OCCC is exempt from the fingerprint-based records check requirement.

Conclusion

The OCCC continues to work to maintain the security and integrity of CHRI, and welcomes the opportunity to focus on these processes and procedures. Consistency in communication between our respective agencies can help us work together as we move forward.

Respectfully,

A handwritten signature in black ink, appearing to read "Leslie Pettijohn", with a stylized flourish at the end.

Leslie Pettijohn
Commissioner

This page left blank intentionally.

Texas Department of Banking
Outstanding Audit Findings Report as of June 1, 2016

The agency has no outstanding audit issues.



STEVEN C. McCRAW
DIRECTOR
DAVID G. BAKER
ROBERT J. BODISCH, SR.
DEPUTY DIRECTORS

TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N. LAMAR BLVD. - BOX 4143 - AUSTIN, TEXAS 78765-4143
CRIME RECORDS SERVICE
512 / 424-7364



COMMISSION
A CYNTHIA LEON, CHAIR
MANNY FLORES
FAITH JOHNSON
STEVEN P. MACH
RANDY WATSON

March 15, 2016

RECEIVED
MAY 02 2016
DEPARTMENT OF BANKING
AUSTIN, TEXAS

Ms. Carrie Lemke
Texas Banking Commission
2601 N. Lamar Blvd
Austin, TX 78705

Subject: Texas Dept. of Public Safety On-Site Audit

Dear Ms. Lemke:

Enclosed is the report on your recent non-criminal justice audit, which was performed on April 12, 2016 by Karen Geramo and Esmeralda Romero, Field Representatives from the Texas Department of Public Safety. The audit consisted of an interview with you, as designated by your agency. The interview specifically covered the non-criminal justice audit process as it pertains to state and federal laws.

After the interview, the auditor reviewed your organization's access, use, dissemination, storage, security and destruction of criminal history record information.

In order for our audit program to comply with state and federal laws, we must request that you address the **Required Actions** indicated in the report. **Please advise us in writing by May 25, 2016 of the actions you have taken to address the identified area(s). Failure to respond could result in sanctions for the agency.**

Please send response to:

Susie Dial-Herrera, Audit Supervisor
P O Box 4143
Austin, Texas 78765-4143
512/424-7927

Sincerely,

Mike Lesko, Deputy Assistant Director
Law Enforcement Support Division
Crime Records Service

ML/kpg

DPS Audit
Form
AD-6

20

TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N LAMAR BLVD • BOX 4087 • AUSTIN, TEXAS 78773-0001
CRIME RECORDS SERVICE
512/424-7364



STEVEN C. McCRAW
DIRECTOR
DAVID G. BAKER
ROBERT J. BODISCH, SR.
DEPUTY DIRECTORS



COMMISSION
A CYNTHIA LEON, CHAIR
MANNY FLORES
FAITH JOHNSON
STEVEN P. MACH
RANDY WATSON

April 15, 2016

NON-CRIMINAL JUSTICE AUDIT REPORT

Texas Banking Commission
OrgID 824 / State-ND 0101E
ORI# TX920450Z

SUMMARY

The Texas Department of Public Safety (DPS) and Federal Bureau of Investigation (FBI) have established audit programs for the purposes of evaluating a criminal and non-criminal justice agency's compliance with state and federal statutes, regulations, policies, and procedures for the access, use, dissemination, storage, security, and destruction of criminal history record information.

TRAINING

During training, the following topics and others not listed here were discussed as baseline security awareness for all authorized personnel with access to criminal history record information: statutes and rules that describe the responsible access and dissemination of criminal history record information; protection of confidential information; threats, vulnerabilities, and risks associated with the handling of criminal history record information; visitor control and physical access to areas containing criminal history record information; electronic storage; destruction; and penalties for non-compliance.

As a reminder, *all* personnel with access to the DPS Secure Site must pass a DPS criminal history check. If you have any questions, please contact us at 512-424-7364.

AUDIT RESULTS

The DPS Access and Dissemination Bureau's Training and Audit Unit, recently conducted an on-site audit in reference to the security of the criminal history record information your agency receives from the DPS, and if applicable, the FBI. This audit report is based on Texas and Federal law regulating the access and dissemination of criminal history record information. [Reference: Texas Government Code 411 and the CJIS Security Policy].

AREAS AUDITED

ACCESS TO CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.083(b) (2) requires the DPS to grant access to criminal and non-criminal justice agencies authorized by state or federal statute, or executive order to receive criminal history record information.

A criminal and non-criminal justice entity must provide the DPS with the name, sex, race, date of birth, and working title of each employee/official who will access and utilize information received from DPS databases. The DPS will conduct a name-based criminal history record check on each name submitted, and reserves the right to require a fingerprint-based criminal history record check on any employee/official. Only persons approved by the DPS will be granted access to DPS databases or information on behalf of the entity. Any person who is not granted access due to the results of the name-based criminal history record check may dispute the findings through the submission of their fingerprints.

Important: The DPS reserves the right to limit the number of authorized employees/officials with access to DPS databases and information. In addition, DPS will strictly enforce the most restrictive set of rights, privileges, and guidelines governing access to DPS databases and information.

Finding: In-Compliance

Required Action(s): None

USE OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.084(a) Criminal history record information obtained from the department under this subchapter, including any identification information that could reveal the identity of a person about whom criminal history record information is requested and information that directly indicates or implies involvement of a person in the criminal justice system: (1) is for the exclusive use of the authorized recipient of the information; and (2) may be disclosed or used by the recipient only if, and to the extent that, disclosure or use is authorized or directed by: (A) this subchapter; (B) another statute; (C) a rule adopted under a statute; or (D) an order of a court of competent jurisdiction.

(a-1) The term "criminal history record" information under Subsection (a) does not refer to any specific document produced to comply with this subchapter but to the information contained, wholly or partly, in a document's original form or any subsequent form or use.

(b) Notwithstanding Subsection (a) or any other provision in this subchapter, criminal history record information obtained from the Federal Bureau of Investigation may be released or disclosed only to a governmental entity or as authorized by federal law and regulations, federal executive orders, and federal policy.

(c) An agency or individual may not confirm the existence or nonexistence of criminal history record information to any person that is not eligible to receive the information.

(d) If your agency is utilizing the Fingerprint-based Applicant Clearinghouse of Texas (FACT), records must be unsubscribed to when you are no longer entitled to access the information, per Government Code 411.0845.

Finding: Out of Compliance

- **CHRI that is received prior to an application being submitted, is an unauthorized purpose.**

- Several CCH records had no supporting documentation.

Required Action(s):

- **CHRI searches shall be performed only for authorized purposes. (TX GC §411.092) In order to be an applicant for employment or licensing purposes, a completed application must be received by the agency before any CHRI is initiated or received. The FAST Pass / Service Code should be provided to individuals after the application is received and removed from unfettered online access.**
- **The agency shall retain audit records for at least one (1) year. Once the minimum retention time period has passed, the agency shall continue to retain audit records until it is determined they are no longer needed for administrative, legal, audit, or other operational purposes. (CJIS Security Policy)**

DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.083(a) Criminal history record information maintained by the department is confidential information for the use of the department and, except as provided by this subchapter, may not be disseminated by the department. (b) The department shall grant access to criminal history record information to: (1) criminal justice agencies; (2) non-criminal justice agencies authorized by federal statute or executive order or by state statute to receive criminal history record information.

(d) The department is not required to release or disclose criminal history record information to any person that is not in compliance with rules adopted by the department under this subchapter or rules adopted by the Federal Bureau of Investigation that relate to the dissemination or use of criminal history record information.

Important: Access to DPS and FBI criminal history record information by authorized employees/officials is subject to cancellation if dissemination of information is made outside the receiving department, related agency, or authorized entity. In addition, access to DPS and FBI criminal history record information may not be disseminated to a person not authorized to receive the information. Criminal penalties (Government Code 411.085) are also in place for the improper dissemination of criminal history record information.

Finding: In-Compliance

Required Action(s): None

STORAGE AND SECURITY OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Agencies are required to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security and integrity.

Per the DPS Databases and CJIS Security Policy: the computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the

computer equipment or to any stored data; the location of all criminal history record information received from the DPS and FBI must have adequate physical security to protect against any unauthorized viewing or access to displayed, stored or printed criminal history record information at all times; passwords must be secure to prevent unauthorized access; the auto save password feature should be disabled to prevent unauthorized logon; ensure that computer terminals have session lock features of less than thirty minutes; user access must be terminated when access is no longer authorized; file cabinets must have locks.

Finding: Out of Compliance

- **The agency has not unsubscribed to CHRI of individuals that are no longer associated with the Banking Commission under GC§411.092.**
- **The agency is scanning CHRI into their data management system of which the server is housed in the IT's area on the third floor. The IT is able access the information on that system yet they have not been vetted per the CJIS Security Policy.**
- **The required Secure Site training had not been completed by all approved data users.**
- **The CJIS Security Awareness training had not been taken by all users with access to CHRI.**
- **At this time, per their IT Joe Broz, any CHRI that may be deleted from the server is not overwritten and can be recreated.**
- **Secure Site passwords were auto saved on the computers.**

Required Action(s):

- **Unsubscribe to records upon end of contract, licensing or employment as you are no longer entitled to access the CHRI. (TX GC§411.0845)**
- **To verify identification, a state of residency and national fingerprint-based record checks shall be conducted within 30 days of assignment for all personnel who have direct contact to CJI and those who have direct responsibility to configure and maintain computer systems and networks with direct access to CJI.**
- **Secure Site online training is mandatory for all DPS Secure Site approved data users.**
- **Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI.**
- **All deleted CCH information shall be overwritten or degaussed by IT.**
- **Disable the auto save feature for passwords to prevent unauthorized logon.**

DESTRUCTION OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Destruction of criminal history record information must be performed by authorized personnel. Agencies with access to criminal history record information must follow their 411 statute and the CJIS Security Policy regarding the destruction of criminal history record information. If the 411 statute does not provide a destruction timeframe, then the agency should follow the recommended timeframe presented during training or contact the training and audit unit to discuss a reasonable timeframe.

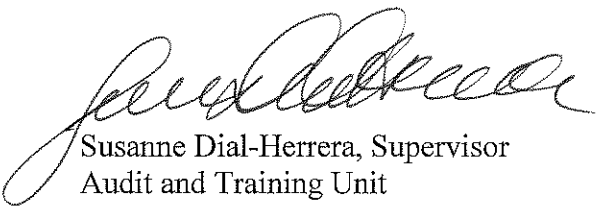
Finding: In-Compliance

Required Action(s): None

OTHER RECOMMENDATIONS OR MINOR INFRACTIONS:

- **Review the DPS Security Policy located on the Secure Site periodically for updates.**

Sincerely,



Susanne Dial-Herrera, Supervisor
Audit and Training Unit
Access and Dissemination Bureau
Crime Records Service



Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 / 877-276-5554
www.dob.texas.gov

May 18, 2016

Ms. Susie Dial-Herrera
Audit Supervisor
Texas Department of Public Safety
P.O. Box 4143
Austin, TX 78765-4143

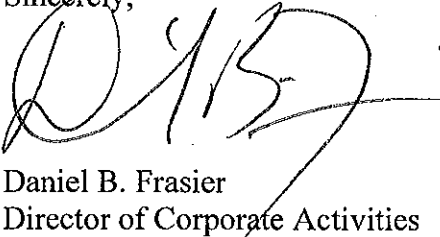
RE: Texas Department of Public Safety ("DPS") On-Site Audit

Dear Ms. Dial-Herrera:

Thank you for providing the result of the recent onsite audit and for providing an opportunity to respond. Please find attached a listing of the findings from the above mentioned audit report along with corrective action. The Department of Banking is committed to the security of the criminal history information and takes the audit findings seriously. The guidance that Ms. Karen Germo provided during the audit is much appreciated.

You may reach me at (512) 475-1322 or dfrasier@dob.texas.gov if you have any questions.

Sincerely,



Daniel B. Frasier
Director of Corporate Activities

DBF/cl

USE OF CRIMINAL HISTORY RECORD INFORMATION

Findings:

- CHRI that is received prior to an application being submitted, is an unauthorized purpose.
- Several CCH records had no supporting documentation.

Explanation: For clarification, the Department did not request fingerprints to be taken prior to receiving an application. However, it was common for an applicant to have their fingerprints submitted for processing prior to the applicant submitting their application to the Department of Banking ("Department").

Corrective Action: Information about how to submit fingerprints to the Department was taken off of our website and out of application materials effective May 11, 2016. In its place, we will notify potential applicants that fingerprint instructions will only be provided upon receipt of an application or the Authority to Release Information form. Additionally, we will inform applicants that they must not submit fingerprints to IdentGo prior to receiving fingerprint instructions from us. The Department will continue to retain documentation supporting the reason that Criminal History Record Information (CHRI) was obtained for at least one year.

STORAGE AND SECURITY OF CRIMINAL HISTORY RECORD INFORMATION

Findings:

- The agency has not unsubscribed to CHRI of individuals that are no longer associated with the Banking Commission under GC§411.092.

Corrective Action: Effective May 11, 2016, the Department has unsubscribed from CHRI of all individuals except those that are currently undergoing an open background check. Our processes and procedures have been revised to unsubscribe to CHRI once a decision on the application has been made.

- The agency is scanning CHRI into their data management system of which the server is housed in the IT's area on the third floor. The IT is able [to] access the information on that system yet they have not been vetted per CJIS Security Policy.

Corrective Action: Effective May 10, 2016, all CHRI data has been removed from electronic systems. Going forward, we will only keep physical CHRI in locked cabinets, and will not retain CHRI in an electronic format. As a result, IT personnel will no longer have access to CHRI.

- **The required Secure Site training had not been completed by all approved data users.**

Corrective Action: The one individual that was identified as not having completed training completed their training on March 8, 2016. Going forward, training will be monitored at least annually to ensure that all required training for Secure Site users have been completed.

- **The CJIS Security Awareness training had not been taken by all users with access to CHRI.**

Corrective Action: The one individual that had not completed required training at the time of the audit completed required training on April 25, 2016. Going forward, training will be monitored at least annually to ensure that all users with access to CHRI have completed their training.

- **At this time, per their IT Joe Broz, and CHRI that may be deleted from the server is not overwritten and can be recreated.**

Corrective Action: Effective May 10, 2016, all CHRI data has been removed from electronic systems. Furthermore, as of May 18, 2016, the Department finished running Microsoft's SDelete (Secure Delete) on the Imaging server's "D" drive which held the former CHRI data. SDelete implements the Department of Defense clearing and sanitizing standard DOD 5220.22-M, to ensure all deleted files are gone forever. Going forward, we will only keep physical CHRI in locked cabinets, and will not retain CHRI in an electronic format.

- **Secure Site passwords were auto saved on computers.**

Corrective Action: Effective April 12, 2016, the saved passwords were removed, and employees were reminded that Secure Site passwords are not to be saved on their computers. Periodic checks by our IT security staff throughout the year will be conducted to ensure passwords are not being retained in the web browser.



STEVEN C. McCRAW
DIRECTOR
DAVID G. BAKER
ROBERT J. BODISCH, SR.
DEPUTY DIRECTORS

TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N. LAMAR BLVD. - BOX 4143 - AUSTIN, TEXAS 78765-4143
CRIME RECORDS SERVICE
512 / 424-7364



COMMISSION
A CYNTHIA LEON, CHAIR
MANNY FLORES
FAITH JOHNSON
STEVEN P. MACH
RANDY WATSON

April 15, 2016

RECEIVED
MAY 02 2016
DEPARTMENT OF BANKING
AUSTIN, TEXAS

Ms. Corina Moreno
Texas Dept. of Banking - Technology
2601 N. Lamar Blvd.
Austin, TX 78705

Subject: Texas Dept. of Public Safety On-Site Audit

Dear Ms. Moreno:

Enclosed is the report on your recent non-criminal justice audit, which was performed on April 12, 2016 by Karen Germa and Esmerelda Romero, Field Representatives from the Texas Department of Public Safety. The audit consisted of an interview with you, as designated by your agency, along with Lorisa Wright. The interview specifically covered the non-criminal justice audit process as it pertains to state and federal laws.

After the interview, the auditor reviewed your organization's access, use, dissemination, storage, security and destruction of criminal history record information.

In order for our audit program to comply with state and federal laws, we must request that you address the **Required Actions** indicated in the report. **Please advise us in writing by May 25, 2016 of the actions you have taken to address the identified area(s). Failure to respond could result in sanctions for the agency.**

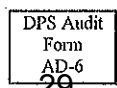
Please send response to:

Susie Dial-Herrera, Audit Supervisor
P O Box 4143
Austin, Texas 78765-4143
512/424-7927

Sincerely,

Mike Lesko, Deputy Assistant Director
Law Enforcement Support Division
Crime Records Service

ML/kpg



TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N LAMAR BLVD • BOX 4087 • AUSTIN, TEXAS 78773-0001
CRIME RECORDS SERVICE
512/424-7364



STEVEN C. McCRAW
DIRECTOR
DAVID G. BAKER
ROBERT J. BODISCH, SR.
DEPUTY DIRECTORS



COMMISSION
A CYNTHIA LEON, CHAIR
MANNY FLORES
FAITH JOHNSON
STEVEN P. MACH
RANDY WATSON

April 15, 2016

NON-CRIMINAL JUSTICE AUDIT REPORT

Banking Commission - Technology

OrgID 14816 / Tech-ND

ORI# TX923536Z

SUMMARY

The Texas Department of Public Safety (DPS) and Federal Bureau of Investigation (FBI) have established audit programs for the purposes of evaluating a criminal and non-criminal justice agency's compliance with state and federal statutes, regulations, policies, and procedures for the access, use, dissemination, storage, security, and destruction of criminal history record information.

TRAINING

During training, the following topics and others not listed here were discussed as baseline security awareness for all authorized personnel with access to criminal history record information: statutes and rules that describe the responsible access and dissemination of criminal history record information; protection of confidential information; threats, vulnerabilities, and risks associated with the handling of criminal history record information; visitor control and physical access to areas containing criminal history record information; electronic storage; destruction; and penalties for non-compliance.

As a reminder, *all* personnel with access to the DPS Secure Site must pass a DPS criminal history check. If you have any questions, please contact us at 512-424-7364.

AUDIT RESULTS

The DPS Access and Dissemination Bureau's Training and Audit Unit, recently conducted an on-site audit in reference to the security of the criminal history record information your agency receives from the DPS, and if applicable, the FBI. This audit report is based on Texas and Federal law regulating the access and dissemination of criminal history record information. [Reference: Texas Government Code 411 and the CJIS Security Policy].

AREAS AUDITED

ACCESS TO CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.083(b) (2) requires the DPS to grant access to criminal and non-criminal justice agencies authorized by state or federal statute, or executive order to receive criminal history record information.

A criminal and non-criminal justice entity must provide the DPS with the name, sex, race, date of birth, and working title of each employee/official who will access and utilize information received

from DPS databases. The DPS will conduct a name-based criminal history record check on each name submitted, and reserves the right to require a fingerprint-based criminal history record check on any employee/official. Only persons approved by the DPS will be granted access to DPS databases or information on behalf of the entity. Any person who is not granted access due to the results of the name-based criminal history record check may dispute the findings through the submission of their fingerprints.

Important: The DPS reserves the right to limit the number of authorized employees/officials with access to DPS databases and information. In addition, DPS will strictly enforce the most restrictive set of rights, privileges, and guidelines governing access to DPS databases and information.

Finding: In-Compliance

Required Action(s): None

USE OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.084(a) Criminal history record information obtained from the department under this subchapter, including any identification information that could reveal the identity of a person about whom criminal history record information is requested and information that directly indicates or implies involvement of a person in the criminal justice system: (1) is for the exclusive use of the authorized recipient of the information; and (2) may be disclosed or used by the recipient only if, and to the extent that, disclosure or use is authorized or directed by: (A) this subchapter; (B) another statute; (C) a rule adopted under a statute; or (D) an order of a court of competent jurisdiction.

(a-1) The term "criminal history record" information under Subsection (a) does not refer to any specific document produced to comply with this subchapter but to the information contained, wholly or partly, in a document's original form or any subsequent form or use.

(b) Notwithstanding Subsection (a) or any other provision in this subchapter, criminal history record information obtained from the Federal Bureau of Investigation may be released or disclosed only to a governmental entity or as authorized by federal law and regulations, federal executive orders, and federal policy.

(c) An agency or individual may not confirm the existence or nonexistence of criminal history record information to any person that is not eligible to receive the information.

(d) If your agency is utilizing the Fingerprint-based Applicant Clearinghouse of Texas (FACT), records must be unsubscribed to when you are no longer entitled to access the information, per Government Code 411.0845.

Finding: Out of Compliance

- **The agency is utilizing their State IT account to fingerprint and run name based searches on all of the agency's applicants, employees and contractors, not just for IT employee purposes.**

Required Action(s):

- **CHRI searches shall be performed only for authorized purposes. The Government Code for this account is §411.1405 for IT personnel only. Refrain from utilizing this account for any other type of personnel.**
Legislation was modified effective September 1, 2013 on your regular Banking Commission account which is under GC §411.092 that allowed you to perform criminal history searches of your employees and contractors on that account with the ORI#TX920450Z.
Your IT employees may be run under either account.

DISSEMINATION OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Texas Government Code 411.083(a) Criminal history record information maintained by the department is confidential information for the use of the department and, except as provided by this subchapter, may not be disseminated by the department. (b) The department shall grant access to criminal history record information to: (1) criminal justice agencies; (2) non-criminal justice agencies authorized by federal statute or executive order or by state statute to receive criminal history record information.

(d) The department is not required to release or disclose criminal history record information to any person that is not in compliance with rules adopted by the department under this subchapter or rules adopted by the Federal Bureau of Investigation that relate to the dissemination or use of criminal history record information.

Important: Access to DPS and FBI criminal history record information by authorized employees/officials is subject to cancellation if dissemination of information is made outside the receiving department, related agency, or authorized entity. In addition, access to DPS and FBI criminal history record information may not be disseminated to a person not authorized to receive the information. Criminal penalties (Government Code 411.085) are also in place for the improper dissemination of criminal history record information.

Finding: In-Compliance

Required Action(s): None

STORAGE AND SECURITY OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Agencies are required to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security and integrity.

Per the DPS Databases and CJIS Security Policy: the computer site and/or terminal area must have adequate physical security to protect against any unauthorized personnel gaining access to the computer equipment or to any stored data; the location of all criminal history record information received from the DPS and FBI must have adequate physical security to protect against any unauthorized viewing or access to displayed, stored or printed criminal history record information at all times; passwords must be secure to prevent unauthorized access; the auto save password feature

should be disabled to prevent unauthorized logon; ensure that computer terminals have session lock features of less than thirty minutes; user access must be terminated when access is no longer authorized; file cabinets must have locks.

Finding: Out of Compliance

- **The DPS Secure Site training had not been completed.**
- **CJIS Security Awareness Training had not been taken by all individuals having access to CHRI.**

Required Action(s):

- **Secure Site online training is mandatory for all DPS Secure Site approved data users.**
- **Basic security awareness training shall be required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJL. (CJIS Security Policy)**

DESTRUCTION OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Destruction of criminal history record information must be performed by authorized personnel. Agencies with access to criminal history record information must follow their 411 statute and the CJIS Security Policy regarding the destruction of criminal history record information. If the 411 statute does not provide a destruction timeframe, then the agency should follow the recommended timeframe presented during training or contact the training and audit unit to discuss a reasonable timeframe.

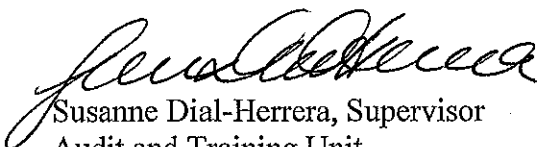
Finding: In Compliance

Required Action(s): None

OTHER RECOMMENDATIONS OR MINOR INFRACTIONS:

- **Review the DPS Access & Dissemination Security Policy located on the Secure Site periodically for updates.**
- **Both Government Codes were provided to the agency at the time of the audit. GC§411.1405 that covers this account and GC§411.092 that relates to their other account and employees.**

Sincerely,


Susanne Dial-Herrera, Supervisor
Audit and Training Unit
Access and Dissemination Bureau
Crime Records Service



Charles G. Cooper
Commissioner

TEXAS DEPARTMENT OF BANKING

2601 North Lamar Blvd., Austin, Texas 78705
512-475-1300 / 877-276-5554
www.dob.texas.gov

May 10, 2016

Susie Dial-Herrera, Audit Supervisor
Texas Department of Public Safety
P.O. Box 4146
Austin, Texas 78765-4143

RE: Response to Texas Department of Public Safety (DPS) On-Site Audit

Ms. Dial-Herrera:

In response to the Required Actions for findings during the on-site audit of the Texas Department of Banking on April 12, 2016, the following actions have been taken by the Department:

Use of Criminal History Record Information

The Department has ceased use of the IT account under Government Code §411.1405, except for IT staff.

Further, the Department submitted a request for a new ORI to the DPS Criminal History Support Supervisor on May 6, 2016, to run applicant, employee and contractor fingerprints under Government Code §411.092 (see attached). We have received an email indicating the application is under review.

Storage and Security of Criminal History Record Information


Users Corina Moreno and Lori Wright have completed all required training as noted on the attached print screens from the DPS system.

User Brenda Medina has been removed from access to the DPS secure site as she is not a regular user, which resulted in her failing to meet the training requirements. The remaining users will continue to comply with the required training requirements.

Lastly, the DPS Access and Dissemination Security Policy will be periodically reviewed for updates.

Please feel free to call me directly at (512) 475-1280 or Lori Wright, Human Resources Manager at (512) 475-1345 with any questions or if you need further information.

Sincerely,


Stephanie Newberg
Deputy Commissioner

OFFICE OF CONSUMER CREDIT COMMISSIONER
Austin, Texas

ANNUAL INTERNAL AUDIT REPORT

Fiscal Year 2016



OFFICE OF CONSUMER CREDIT COMMISSIONER
Austin, Texas

Annual Internal Audit Report
Fiscal Year 2016

TABLE OF CONTENTS

	<u>Page</u>
Internal Auditor's Report	1
Introduction	2
Internal Audit Objectives.	3
Executive Summary	
Motor Vehicle Sales Finance Examinations	
Background.	4-5
Audit Objective, Scope, and Methodology.	6-7
I. Compliance with Texas Government Code 2102: Required Posting of Internal Audit Information	7
II. Internal Audit Plan for Fiscal Year 2016	7-9
III. Consulting and Nonaudit Services Completed.....	9
IV. External Quality Assurance Review.....	9
V. Observations/Findings and Recommendations.	10-14
VI. External Audit Services Procured in Fiscal Year 2016.....	15
VII. Reporting Suspected Fraud and Abuse.....	15
VIII. Proposed Internal Audit Plan for Fiscal Year 2017	15
IX. Organizational Chart	16

Garza/Gonzalez & Associates

CERTIFIED PUBLIC ACCOUNTANTS

Finance Commission Members and
Finance/Audit Committee Members
Office of Consumer Credit Commissioner
Austin, Texas

We performed tests of management's assertion about the effectiveness and efficiency of the internal control structure over the Motor Vehicle Sales Finance (MVSF) Examinations area of the Office of Consumer Credit Commissioner (OCCC); and, its compliance with the Texas Finance Code, Texas Administrative Code, and OCCC's established policies and procedures, as applicable to the MVSF Examinations area, for the 7 months ended March 31, 2016.

The results of our tests disclosed that such controls were adequate and no material instances of noncompliance were noted; however, we noted certain matters that are included in this report, that are opportunities for strengthening internal controls and ensuring compliance with State requirements and OCCC's established policies and procedures. We also performed a follow-up of the findings that were presented in the prior year annual internal audit report and this report reflects the implementation status of those matters; and, includes all information required for the State of Texas Internal Audit Annual Report requirements.

We have discussed the comments and recommendations from the MVSF Examinations audit; and, the implementation status from the follow-up performed, with various OCCC personnel, and we will be pleased to discuss them in further detail; to perform an additional study of these matters; or, to assist you in implementing the recommendations.



May 13, 2016

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

INTRODUCTION

The Office of Consumer Credit Commissioner (OCCC) operates pursuant to Texas Finance Code, §14.001, and under the oversight of the Texas Finance Commission, who appoints the consumer credit commissioner. OCCC has authority to regulate consumer credit transactions and interest rates in Texas, offers protection to consumers, coordinates educational efforts aimed at consumers and industry alike, and advises lenders on compliance issues.

OCCC's primary task is to license and examine finance companies, home equity and junior lien mortgage lenders, residential mortgage loan originators, payday lenders, signature loan companies, motor vehicle sales finance companies, property tax lien lenders, and pawnshops. Pawnshop employees must also be licensed.

OCCC was granted Self-Directed, Semi Independent (SDSI) status in the 81st Legislative Session. As an SDSI agency, OCCC is not required to have their budget approved by the Legislature; however, the Finance Commission is responsible for setting OCCC's spending authority or limits. OCCC's entire operating funds are generated from fees assessed to the businesses it supervises and are used to fund both direct and indirect costs. General revenue funds are not used to support OCCC's operations.

2016 Internal Audit Plan

Following are the internal audits and other functions performed, as identified in OCCC's approved 2016 Internal Audit Plan:

- Motor Vehicle Sales Finance Examinations
- Follow-up of Prior Year Internal Audits
- Other Tasks

This report contains the results of our audit of the Motor Vehicle Sales Finance Examinations area, reflects the follow-up performed in the current year, and meets the State of Texas Internal Audit Annual Report requirements.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

INTERNAL AUDIT OBJECTIVES

In accordance with the **International Standards for the Professional Practice of Internal Auditing**, the audit scope encompassed the examination and evaluation of the adequacy and effectiveness of OCCC's system of internal control and the quality of performance in carrying out assigned responsibilities. The audit scope included the following objectives:

- **Reliability and Integrity of Financial and Operational Information** – Review the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report such information.
- **Compliance with Policies, Procedures, Laws, Regulations and Contracts** – Review the systems established to ensure compliance with those policies, procedures, laws, regulations, and contracts which could have a significant impact on operations and reports, and determine whether the organization is in compliance.
- **Safeguarding of Assets** – Review the means of safeguarding assets and, as appropriate, verify the existence of such assets.
- **Effectiveness and Efficiency of Operations and Programs** – Appraise the effectiveness and efficiency with which resources are employed.
- **Achievement of the Organization's Strategic Objectives** – Review operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

EXECUTIVE SUMMARY

Motor Vehicle Sales Finance Examinations

Background

Organizational Structure

The Director of Consumer Protection, who reports to the Commissioner, is responsible for administering the Examination and Enforcement Division (Division), which is responsible for conducting Motor Vehicle Sales Finance (MVSF) examinations. The Division is comprised of 3 regional supervisory examiners, 3 assistant supervisors (1 position currently vacant), 5 review examiners, 1 out-of-state coordinator, 2 financial analysts, 3 administrative support positions and 39 examiners.

MVSF Licensees

MVSF licensees, licensed with OCCC, are both sellers and holders of retail installment contracts. Businesses that are required to be licensed with OCCC are retail motor vehicle sellers who provide financing, which includes sellers who originate and collect on installment sales and those who originate and sell retail installment contracts; and, finance companies who buy retail installment contracts (indirect lenders), and those who review applications from sellers and then buy the retail installment contract.

Examination Process

On-site examinations are performed to ensure MVSF licensees (licensees) are compliant with Chapter 348 of the Texas Finance Code (TFC), Chapter 84 of the Texas Administrative Code (TAC), and other federal requirements. As of March 31, 2016, there were 8,895 MVSF entities licensed with OCCC.

Examination Scheduling

Examination schedules are prepared by each of the 3 regional supervisory examiners on a monthly basis for their respective region using an add-on tool in the Application Licensing Examination Compliance System (ALECS) database. Licensees are selected for examination using various factors which include: (1) license date, (2) date of last examination, (3) examination ratings, (4) complaints, and (5) other risks and considerations.

MVSF Examinations

The Division has developed tailored examination work papers for MVSF examinations that are used by the examiners to denote compliance with and/or exceptions to TFC and TAC requirements. As part of the examination process, the examiner reviews a sample of contracts, applications, agreements, and other various documents, as applicable, to ensure compliance with various sections of the TFC and TAC. The examiners also ensure the licensee is properly displaying all the required consumer disclosures in a clearly visible area where sales are finalized; and, properly licensed with OCCC.

At the conclusion of the examination, the examiner assigns the exam a rating, using a scale of "1" to "5" based on the licensee's level of compliance, as follows:

Rating	Basis
1	No exceptions; no comment report.
2	Few exceptions; no significant examination issues.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

- 3 Several exceptions; few significant issues requiring remedy; possible minimal refunding required.
- 4 Several significant issues requiring urgent remedy; moderate refunding required; prior examination issues not addressed by licensee; moderate procedural or systemic error; follow-up examination is required.
- 5 Significant issues requiring immediate remedy; substantial refunding required; repeated examination issues on previous exams not addressed by licensee; serious procedural or systemic errors; follow-up examination is required; licensee will be monitored until unacceptable level of compliance is cleared or administrative action is taken.

Examinations rated a “4” or “5” require verbal approval from the director or review examiner. The examiner is required to document the name of the approver and the approval date on the exam work papers, to denote approval of the exam rating.

The examiner then proceeds to prepare a report of examination (ROE), which is provided to the licensee while the examiner is still on-site, and includes the findings identified, if any, during the examination. Findings that require a response are included in the “Special Instructions” section of the ROE and the licensee is required to respond to these matters within 60 to 90 days from the ROE date. These reports also require the signature of the licensee or licensee representative, which signifies that they have read the report and agree to respond to the findings within the required number of days.

Licensees submit their responses to OCCC’s Austin office, for review by the review examiners. A reminder/notification letter is sent to licensees who fail to provide a response within the required time period to inform them that their response is overdue. Failure to correct the matter can result in a follow-up examination or administrative action.

As of March 30, 2016, the Division completed 1,238 MVSF examinations, with the following ratings:

	Ratings					Total
	1	2	3	4	5	
MVSF Exams	155	198	606	275	4	1,238

Examination Review

ROEs with ratings of “4” and “5” require the review of the director, review examiner, or supervisory examiner (review staff). The Division’s goal is to review examination reports within 120 days of the ROE processing date, which is the Friday following the ROE date. An exam summary log is maintained and used to track receipt of all ROEs, and for the assignment of ROEs for review. Each individual of the review staff maintains a log of the ROEs that they have reviewed, and a summary of all the logs is prepared on a quarterly basis and submitted to the director for his review.

Fees

TAC §84.706 authorizes OCCC to assess a fee at a rate of \$100 per hour to conduct a follow-up examination. Although the Division has performed follow-up examinations, OCCC has not determined a need to assess such fees.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

Audit Objective, Scope, and Methodology

Objective

The objective of our audit was to gain an understanding of the processes and controls in place over the Motor Vehicle Sales Finance (MVSF) Examinations area to determine whether it is being managed in accordance with applicable rules and regulations and OCCC's established policies and procedures.

Scope

The scope of our audit covered the time period from September 1, 2015 through March 31, 2016, and included a review of the processes and the effectiveness of controls in place for performing MVSF examinations.

Methodology

The audit methodology included a review of policies and procedures, laws and regulations, and other internal and external documentation; an interview with OCCC employees, to include the Director of Consumer Protection; and, a review of sample examination work papers and reports.

We obtained and/or reviewed the following information:

- a. OCCC policies and procedures related to MVSF examinations.
- b. Examination and Enforcement Division organizational chart.
- c. A listing of examinations performed during the period from September 1, 2015 through March 30, 2016.
- d. A listing of active MVSF licensees as of March 31, 2016.
- e. Samples of various MVSF examination work papers and reports.
- f. Sample MVSF notification letters.
- g. ALECS overview report for examinations conducted during fiscal year 2016.
- h. Reports on the summary of exams reviewed for fiscal year 2016.
- i. Initial examiners training agenda.

We performed various procedures, to include the following:

1. Reviewed and obtained an understanding of the rules, laws and regulations of the Texas Finance Code (TFC), and Texas Administrative Code (TAC), as applicable to the MVSF Examinations area.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

2. Obtained and reviewed established policies and procedures, collected documentation, and conducted interviews to obtain an understanding of the processes and current practices in for conducting MVSF examinations.
3. Obtained a report of MVSF examinations performed from September 1, 2015 through March 30, 2016 and randomly selected 25 examinations to test for the following attributes:
 - a. Completion of the examination work papers;
 - b. Proper sample size of transactions selected for testing;
 - c. Reasonableness of assigned examination rating;
 - d. Approval from director or review examiner for examinations rated “4” or “5”;
 - e. Exceptions cited in the ROE correspond to the exceptions include in the examination work papers;
 - f. Signature of licensee’s owner or manager in the examination report, if applicable;
 - g. Examinations reviewed in accordance with the Division’s goals; and,
 - h. Response and notification letter sent to the licensees, if applicable.
4. Reviewed examination work papers tailored for MVSF examinations to ensure inclusion of significant TFC and TAC compliance requirements.

I. Compliance with Texas Government Code 2102: Required Posting of Internal Audit Information

To comply with the provisions of Texas Government Code 2102.015 and the State Auditor’s Office, within 30 days of approval by the Finance Commission, OCCC will post the following information on its website:

- An approved fiscal year 2017 audit plan, as provided by Texas Government Code, Section 2102.008.
- A fiscal year 2016 internal audit annual report, as required by Texas Government Code, Section 2102.009.

The internal audit annual report includes any weaknesses, deficiencies, wrongdoings, or other concerns raised by internal audits and other functions performed by the internal auditor as well as the summary of the action taken by OCCC to address such concerns.

II. Internal Audit Plan for Fiscal Year 2016

The Internal Audit Plan (Plan) included one audit to be performed during the 2016 fiscal year. The Plan also included a follow-up of the prior year audit recommendations, other tasks as may be assigned by the Finance Commission, and preparation of the Annual Internal Audit Report for fiscal year 2016.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

Risk Assessment

Utilizing information obtained through the inquiries and background information reviewed, 17 audit areas were identified as the potential audit topics. A risk analysis utilizing our 8 risk factors was completed for each individual audit topic and then compiled to develop an overall risk assessment.

Following are the results of the risk assessment performed for the 17 potential audit topics identified:

HIGH RISK	MODERATE RISK	LOW RISK
Motor Vehicle Sales Finance Examinations Registration Texas Financial Education Endowment Fund	Records Management Property Tax Lender Examinations Billing and Collection of Fees Fiscal Division Complaint Intake and Investigations Regulated Lenders Examinations	Professional Licensing (Pawnshop Employees & MLO) Pawn Examinations Fixed Assets Management Information Systems Risk Management Business Licensing Credit Access Business Examinations Human Resources

In the prior 3 years, internal audits were performed in the following areas:

Fiscal Year 2015:

- Texas Financial Education Endowment Fund

Fiscal Year 2014:

- Professional Licensing

Fiscal Year 2013:

- Credit Access Business Examinations

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

The areas recommended for internal audits and other tasks to be performed for fiscal year 2016 were as follows:

Report No.	Audits/Report Titles	Report Date
1.	Motor Vehicle Sales Finance Examinations	5/13/2016
1.	Annual Internal Audit Report – Follow-Up of Prior Year Internal Audits	5/13/2016
-	Other Tasks Assigned by the Finance Commission	None

III. Consulting and Nonaudit Services Completed

The internal auditor did not perform any consulting services, as defined in the Institute of Internal Audit Auditors' *International Standards for the Professional Practice of Internal Auditing* or any non-audit services, as defined in the *Government Auditing Standards, December 2011 Revision*, Sections 3.33-3.58.

IV. External Quality Assurance Review

The internal audit department's most recent *System Review Report*, dated October 7, 2015, indicates that its system of quality control has been suitably designed and conforms to applicable professional standards in all material respects.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

V. Observations/Findings and Recommendations

Report No.	Report Date	Name of Report	Observations/ Findings and Recommendations	Current Status (Implemented, Partially Implemented, Implementation Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	May 13, 2016	MVSF Examinations	<p>1. Notification Letter</p> <p>Section XII – Examination Process of the Examiner Manual states that a copy of the notice of the upcoming examination (notification letter), sent to the licensee, will be sent to the Austin office by uploading it into the imaging system, along with the examination work papers.</p> <p>Our review of the 25 examinations selected for testing disclosed 6 instances where the notification letter was not included in the examination work papers.</p> <p>Recommendation We recommend that OCCC comply with Section XII – Examination Process of the Examiner Manual and ensure a copy of the notification letter is included in the examination work papers that are submitted to the Austin office to provide evidence that the notification letter was sent to the licensee, as required.</p> <p>Management's Response The OCCC complies with the statutory requirement to give notice to a MVSF licensee prior to conducting an examination. The OCCC examination procedure purposefully creates confirmation of the notice in the examination process. The administrative and statistical portion of the examination workpapers has a section in which the examiner documents the date and method of notification. In the 6 examples cited above, the notations were contained in the records signifying that the licensee was provided notification. The examination procedure additionally directs the examiner to include a copy of the notification or an acknowledgement of the notification in the examination workpaper file. In these 6 examples, the examiners did not provide the additional copy. All examiners have been retrained on the procedure and have provided an acknowledgment of the policy.</p> <p>The examination process will be significantly improved with the new IT application development for an examination tool presently underway. The examination tool not only brings efficiencies and robust functionality, it also serves to strengthen internal controls and compliance with policies and procedures. Notification of a MVSF examination will be provided through the system to licensees with a system account and the audit history will maintain evidence of the notification.</p>		To ensure compliance with OCCC's policies and procedures.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

Report No.	Report Date	Name of Report	Observations/ Findings and Recommendations	Current Status (Implemented, Partially Implemented, Implementation Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	May 13, 2016	MVSF Examinations	<p>2. Examination Work Papers</p> <p>Our testing of 25 MVSF examinations for various attributes disclosed the following:</p> <ul style="list-style-type: none"> 2 instances where examination work papers were not entirely completed, as follows— <ul style="list-style-type: none"> 1 instance where 3 procedures on the examination check sheet were not annotated to denote whether there was or was not a violation, or whether it was not applicable; and, 1 instance where the <i>Motor Vehicle Examination Review</i> work paper lacked transaction volume information, which documents the total number of accounts the business has as of the examination date, and is the population used for selecting the minimum required transactions for testing. 1 instance where discrepancies reported in the ROE did not agree to the discrepancies reflected in the <i>Monetary Correction Worksheet</i>. <p>Recommendation We recommend OCCCC implement quality control procedures to ensure proper completion of examination work papers.</p> <p>Management's Response The examination process will be significantly improved with the new examination tool. The application will include edit checks to ensure completion and quality control. Any examination may not be finalized by an examiner until all applicable data fields and responses are completed. All three of the instances mentioned above would not have occurred if the examinations had been conducted after the implementation of the examination tool. In the interim, all examiners will receive refresher training, focusing on thorough and accurate report completion.</p>		To ensure completion of examination work papers.

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

Report No.	Report Date	Name of Report	Observations/ Findings and Recommendations	Current Status (Implemented, Partially Implemented, Implementation Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	May 13, 2016	MVSF Examinations	<p>3. ROE Review</p> <p>The Examination Review Completion Procedure indicates that it is OCCC's goal to review examination reports, with a compliance rating of 4 or 5, within 120 days of the ROE processing date.</p> <p>Our testing of 25 MVSF examinations disclosed 2 instances where reports assigned a rating of 4 were reviewed 4 and 24 days after the 120 days from the ROE processing date.</p> <p>Recommendation We recommend that OCCC strengthen controls to comply with the established goal.</p> <p>Management's Response Currently the review process is coordinated by a senior staff examiner and several additional senior staff members review examination reports as an additional duty. At this time the examination review coordinator is the only staff member with the primary duty of reviewing examination reports. A review of workload vs staffing will be conducted to ensure adequate resources are assigned. Additionally, staff will review the procedure to strengthen deadline compliance.</p> <p>The examination review process will also be significantly improved with the new examination tool. The workflow will include a review assignment queue that will allow better prioritization and work load distribution which should support timely review processing.</p> <p>4. Reminder Letters</p> <p>Findings included in the special instructions section of the ROE require the licensee to respond and/or provide verification of action taken, within 60 to 90 days from the ROE date. It is OCCC's practice for the examiner to send the licensee a reminder/notification letter if a response or verification of action taken is not received by the response due date, to inform them they are noncompliant and to make a 2nd request for the information. Failure to correct the matter can result in a follow-up examination or administrative action.</p>		<p>To comply with the established ROE review goal.</p> <p>To ensure compliance with OCCC's procedures and practices.</p>

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

Report No.	Report Date	Name of Report	Observations/ Findings and Recommendations	Current Status (Implemented, Partially Implemented, Implementation Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	May 13, 2016	MVSF Examinations	<p>Our testing of 25 MVSF examinations disclosed 2 instances where the licensee did not respond by the response due date and the reminder/notification letters, which management indicated were sent on January 21, 2016 and April 29, 2016, were sent 1 month after the response due date and were not provided for our review. However, we did note that in 1 instance the licensee signed an Agreed Order dated February 1, 2016 and agreed to pay an administrative penalty fee; and, in the other instance, the licensee paid restitution to its customers, and OCCC is currently preparing the Agreed Order.</p> <p>Recommendation We recommend that OCCC strengthen controls to ensure reminder/notification letters sent to the licensees are maintained with the examination work papers to provide evidence that licensees are informed of their delinquency and support the basis for performing a follow-up examination or issuing an administrative action.</p> <p>Management's Response The examination process will be significantly improved with the new examination tool. The application will include a workflow process that will monitor response due dates and generate automatic communication and alerts to support the examination process and licensee responses. In the two instances mentioned above, if the examinations had been conducted after the implementation of the examination tool, the system would reflect notations that the examinations had been referred to legal for additional work. In the interim, examination staff with responsibility for examination responses will review current policy to improve examination processing and communication.</p>		

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

Report No.	Report Date	Name of Report	Observations/ Findings and Recommendations	Current Status (Implemented, Partially Implemented, Action Delayed, No Action Taken, Do Not Plan to Take Corrective Action, or Other)	Fiscal Impact/Other Impact
1	May 13, 2016	2016 Follow-Up	<p>Follow-Up of Prior Year Audits</p> <p>Following is the status of the recommendations made during fiscal year 2015 that had not been implemented.</p> <p><u>TFEE Fund</u></p> <p>1. Policies and Procedures</p> <p>We recommended that OCCC, with guidance from the GAC, revise the TFEE Fund's policies and procedures to reflect current practices in place and to include guidance for issues and requirements not currently addressed.</p> <p>2. Grant Award Amounts</p> <p>We recommended that the rationale used in determining the allocation of grants awarded to various applicants be documented to provide evidence that it was done in a systematic and rational manner.</p> <p>Following is the status of the recommendations made during fiscal year 2014 that had not been implemented.</p> <p><u>Professional Licensing</u></p> <p>1. Review and Approval of Applications</p> <p>We recommended that OCCC consider implementing a quality control review process whereby the population of the RML0 and Pawnshop Employee applications received are sampled and reviewed on a periodic basis to provide added assurance.</p>	<p>Implemented</p> <p>Implemented</p> <p>Implemented</p>	

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

VI. External Audit Services Procured in Fiscal Year 2016

OCCC procured the internal audit services documented in the Internal Audit Plan for fiscal year 2016.

VII. Reporting Suspected Fraud and Abuse

OCCC has provided information on their home page on how to report suspected fraud, waste, and abuse to the State Auditor's Office (SAO) by posting a link to the SAO's fraud hotline. OCCC has also developed a Fraud Policy that provides information on how to report suspected fraud.

VIII. Proposed Internal Audit Plan for Fiscal Year 2017

The risk assessment performed during the 2016 fiscal year was used to identify the following *proposed* area that is recommended for internal audit and other tasks to be performed for fiscal year 2017. The Internal Audit Plan for Fiscal Year 2017 will be developed and presented to the Finance Commission at a meeting to be determined at a later date.

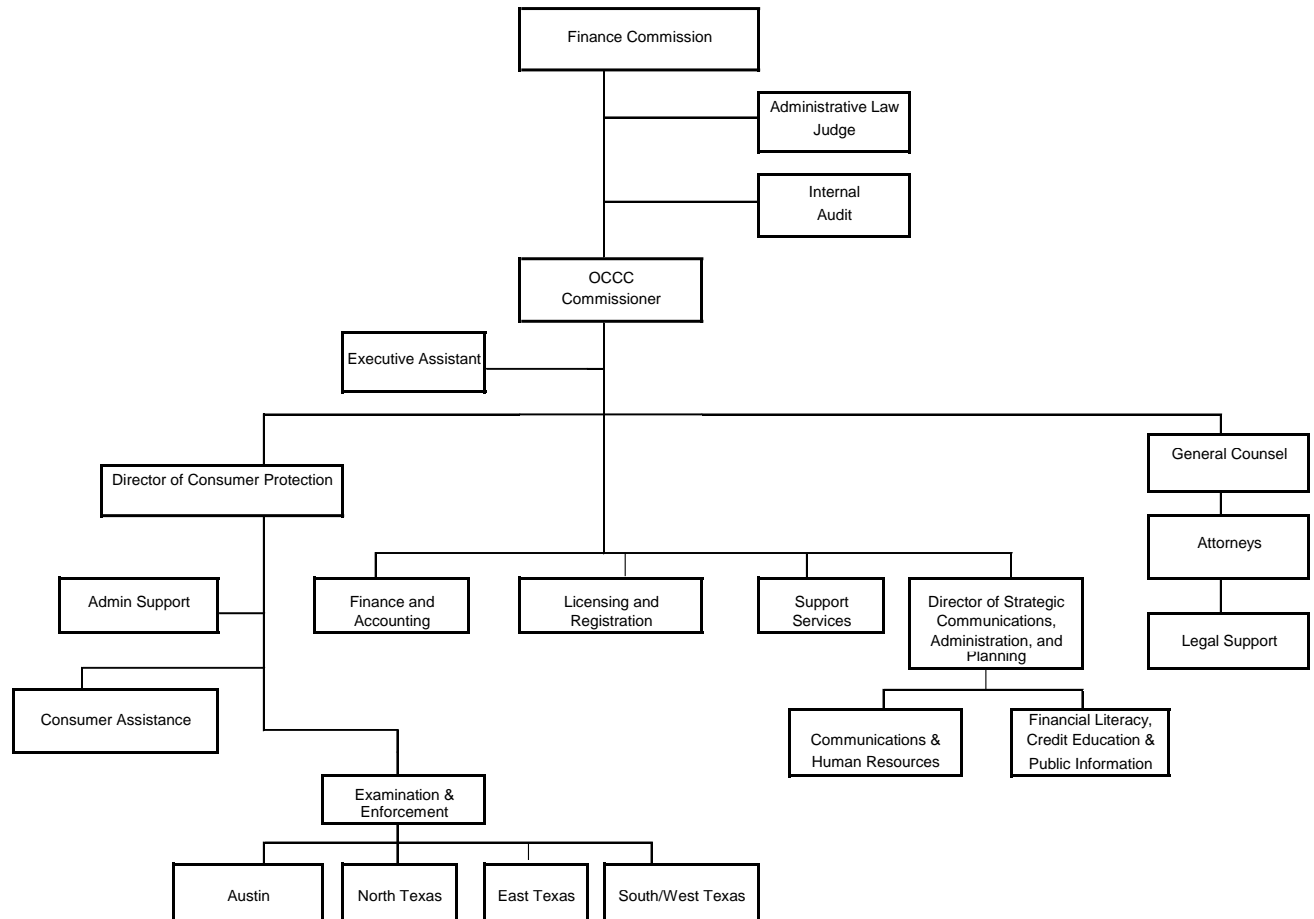
- Registration
- Follow-up of Prior Year Internal Audits
- Other Tasks Assigned by the Finance Commission

OFFICE OF CONSUMER CREDIT COMMISSIONER

Annual Internal Audit Report

Fiscal Year 2016

IX. Organizational Chart



TEXAS DEPARTMENT OF BANKING
Austin, Texas

ANNUAL INTERNAL AUDIT REPORT

Fiscal Year 2016



TEXAS DEPARTMENT OF BANKING
Austin, Texas

Annual Internal Audit Report
Fiscal Year 2016

TABLE OF CONTENTS

	<u>Page</u>
Internal Auditor's Report	1
Introduction	2
Internal Audit Objectives	3
Executive Summary	
Information Technology (IT) Examinations	
Background	4-6
Audit Objective, Scope, and Methodology	6-7
Imaging and Records Management	
Background	8-9
Audit Objective, Scope, and Methodology	9-10
I. Compliance with Texas Government Code 2102: Required Posting of Internal Audit Information.....	10
II. Internal Audit Plan for Fiscal Year 2016	11-12
III. Consulting and Nonaudit Services Completed.....	12
IV. External Quality Assurance Review.....	12
V. Observations/Findings and Recommendations	13-17
VI. External Audit Services Procured in Fiscal Year 2016.....	18
VII. Reporting Suspected Fraud and Abuse.....	18
VIII. Proposed Internal Audit Plan for Fiscal Year 2017	18
IX. Organizational Chart	18

Garza/Gonzalez & Associates

CERTIFIED PUBLIC ACCOUNTANTS

Finance Commission Members and
Finance/Audit Committee Members
Texas Department of Banking
Austin, Texas

We performed tests of management's assertion about the effectiveness and efficiency of the internal control structure over the Information Technology (IT) Examinations, and Imaging & Records Management areas of the Texas Department of Banking (DOB); and, its compliance with State requirements, the Texas Finance Code, and DOB's established policies and procedures, as applicable to these areas, for the 5 months ended January 31, 2016 (IT Examinations) and the 7 months ended March 31, 2016 (Imaging & Records Management).

The results of our tests disclosed that such controls were adequate and no material instances of noncompliance were noted; however, we noted certain matters that are included in this report, that are opportunities for strengthening internal controls and ensuring compliance with State requirements and DOB's established policies and procedures. This report also includes all information to meet the State of Texas Internal Audit Annual Report requirements.

We have discussed the comments and recommendations from the above audits, with various DOB personnel, and we will be pleased to discuss them in further detail, or to perform an additional study of these matters.



March 30, 2016 – IT Examinations

April 26, 2016 – Imaging & Records Management

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

INTRODUCTION

The Texas Department of Banking (DOB) operates under the oversight of the Texas Finance Commission, and is an agency of the State of Texas that performs functions designed to maintain a financial regulatory system for Texas that promotes a consistent banking environment, provides the public with convenient, safe, competitive banking and other legislative financial services.

DOB operates pursuant to the authority of various provisions of the Texas Finance Code; the Texas Health and Safety Code; and the Texas Administrative Code. DOB regulates state banks; foreign bank branches, agencies, and representative offices; trust companies; prepaid funeral benefit contract sellers; perpetual care cemeteries; money service businesses; private child support enforcement agencies; and check verification entities.

The major functions of DOB are to:

- Charter, regulate, and examine all state banks, foreign bank branches, agencies, and representative offices;
- Charter, regulate, and examine trust departments of commercial banks and trust companies;
- License, regulate, and examine sellers of prepaid funeral contracts;
- License, regulate, and examine perpetual care cemeteries;
- License, regulate, and examine money services businesses;
- Register and investigate complaints of private child support enforcement agencies; and
- Register check verification entities.

DOB was granted Self-Directed, Semi Independent (SDSI) status in the 81st Legislative Session. As an SDSI agency, DOB is not required to have their budget approved by the Legislature; however, the Finance Commission is responsible for setting their spending authority or limits. DOB's entire operating funds are generated from fees assessed to the businesses it supervises and are used to fund both direct and indirect costs. General revenue funds are not used to support DOB's operations.

2016 Internal Audit Plan

Following are the internal audits and other functions performed, as identified in DOB's approved 2016 Internal Audit Plan:

- IT Examinations
- Imaging & Records Management
- Follow-up of Prior Year Internal Audits *
- Other Tasks

* There were no findings from prior year internal audits that required a follow-up during fiscal year 2016.

This report contains the results of our audit of the IT Examinations and the Imaging & Records Management areas; and, meets the State of Texas Internal Audit Annual Report requirements.

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

INTERNAL AUDIT OBJECTIVES

In accordance with the **International Standards for the Professional Practice of Internal Auditing**, the audit scope encompassed the examination and evaluation of the adequacy and effectiveness of DOB's system of internal control and the quality of performance in carrying out assigned responsibilities. The audit scope included the following objectives:

- **Reliability and Integrity of Financial and Operational Information** – Review the reliability and integrity of financial and operating information and the means used to identify, measure, classify, and report such information.
- **Compliance with Policies, Procedures, Laws, Regulations, and Contracts** – Review the systems established to ensure compliance with those policies, procedures, laws, regulations, and contracts which could have a significant impact on operations and reports, and determine whether the organization is in compliance.
- **Safeguarding of Assets** – Review the means of safeguarding assets and, as appropriate, verify the existence of such assets.
- **Effectiveness and Efficiency of Operations and Programs** – Appraise the effectiveness and efficiency with which resources are employed.
- **Achievement of the Organization's Strategic Objectives** – Review operations or programs to ascertain whether results are consistent with established objectives and goals and whether the operations or programs are being carried out as planned.

EXECUTIVE SUMMARY

Information Technology (IT) Examinations

Background

The Information Technology (IT) Examinations area is administered by the Bank & Trust Supervision Division of the Texas Department of Banking (DOB) and is responsible for performing IT examinations for state chartered banks, trust companies, and certain technology service providers (TSPs). DOB's IT Examinations area is comprised of a Director of IT Security Examinations (DITSE), a Chief IT Security Examiner (CITSE), and 8 IT specialists located throughout the state. As of February 26, 2016, the IT Examinations area was responsible for the examination of 250 banks, 19 trust companies, and 3 TSPs.

Examination Priorities

IT examinations are generally performed in conjunction with Safety & Soundness (S&S) examinations, which are also administered by the Bank & Trust Supervision Division. Financial institutions regulated by DOB are required to receive a Full Scope IT examination (IT examination) at the frequency of every 6, 12, or 18 months, depending on the asset size, bank composite rating, and IT examination rating. An exception to this frequency schedule is when a continuous examination is performed, which is a series of targeted examinations performed throughout a 12 month period, for large banks with an asset size of \$20 billion or greater. Another exception is that TSPs are required to have an IT examination not less than every 36 months. The responsibility for performing IT examinations is shared amongst DOB, the Federal Deposit Insurance Corporation (FDIC), and the Federal Reserve Bank (FRB). Thus, the IT examination and subsequent issuance of the Report of Examination (ROE) may be performed jointly by these agencies, or independently by either of the agencies. Agencies generally alternate the performance of the IT examination, to the extent scheduling permits.

Compliance with the established examination priorities, or the percentage of examinations performed on time, is the IT Examinations area's primary performance measure. An IT examination is considered "on time" if the onsite examination starts on or before the grace date, which is the due date plus a 30-day grace period. Of the 88 IT examinations performed with a grace date from September 1, 2015 to January 31, 2016, 86, or 98%, were performed on time. In 2 instances the IT examinations were considered late since they started 1 day after the grace date at a bank, and 2 days after the grace date at a trust company.

IT Examination Process

Planning: An IT examination begins with the planning phase, which is performed by the Examiner-in-Charge (EIC), who completes the planning and control procedures outlined in DOB's work program. The procedures include obtaining various IT-related information from the regulated entity's management; reviewing the Technology Profile Script (TPS) or the IT Profile (ITP) form to assess the entity's complexity risk level; and, determining the examination scope based on the evaluation of information obtained. Using the risk-based listing of core work programs as the baseline, the EIC may expand or narrow the scope by adding or waiving one or more work programs, as he/she considers appropriate; however, the CITSE must approve the scope of each IT examination prior to its commencement. Effective January 2016, DOB requires all banks it regulates to measure their inherent cyber risks and cybersecurity maturity (preparedness), which is submitted to DOB upon request. Banks may perform this function by completing the Cybersecurity Assessment Tool (CAT), which was developed by the Federal Financial Institutions Examination Council (FFIEC); or, by any other method that provides the same type of results.

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

Examination: The IT Examinations area has, for a number of years, utilized work programs titled IT Risk Management Program (IT-RMP) to perform and document IT examinations. IT-RMP work programs were based on a framework developed by the FDIC and customized by DOB. In January 2016, the IT Examinations area implemented the use of new work programs titled Information Technology Risk Examination (InTREx), which were developed by the FDIC, the FRB, and state agencies, as a joint agency project. InTREx work program are currently undergoing a peer review process that involves feedback from the regulatory agencies, and expected to be finalized in June 2016. Upon completion of each work program (both versions), in the Summary of Findings (SOF), the IT Examiner summarizes findings as “Report Worthy” or “Not Report Worthy”. All “Report Worthy” findings are included in the Report of Examination (ROE), while “Not Report Worthy” findings are informally communicated to the financial institution.

Report of Examination (ROE): At the conclusion of each examination, findings, if applicable, and examination ratings are communicated to the financial institution in the ROE. IT examination results can be reported either in a stand-alone ROE or embedded within the S&S ROE. Financial institutions are required to provide a response to those findings identified as Matters Requiring Attention (MRA) in the ROE, within 45 days of the report date.

At the conclusion of an IT examination, DOB and federal agencies assign each financial institution an examination rating using the Uniform Rating System for Information Technology (URSIT). A component rating is assigned to each of the 4 components considered critical to an IT examination, which are (1) Audit; (2) Management; (3) Development and Acquisition; and, (4) Support and Delivery (AMDS). A composite rating is then derived from the overall IT examination results. The composite and component ratings are based on a scale of 1 to 5, with a rating of 1 representing the highest (best) rating and 5 being the lowest. DOB considers a bank with a composite rating of 3, 4, or 5 to be a “problem institution” that requires close monitoring. Until December 2015, only the composite rating of an IT examination was reported in the ROE. Starting January 2016, both, the component and composite ratings are included in the ROE.

Work Paper Review: The EIC and/or the Supervisory-Examiner-in-Charge (SEIC) are responsible for ensuring that all examination procedures and work papers have been properly completed and are available electronically. Each IT examination also receives a limited level of review by a “first reviewer”, who is one of the commissioned IT examiners; and, then the CITSE. DOB has procedures in place to ensure the work of the CITSE is also reviewed by other parties. In addition, on a sample basis, the CITSE and the Examiners Council (EC) conduct comprehensive reviews of IT examinations during the year for quality control purposes. The EC is an internal, independent team of examiners comprised of an S&S examiner from each regional office, a trust examiner, and an IT examiner, each serving a 2 year term. The results of the comprehensive reviews are used to identify areas for improvement in performing and documenting IT examinations.

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

Report Processing Schedule: DOB has established an examination processing schedule to ensure ROEs are processed in a timely manner. The examination processing schedule followed is dependent on whether the examination qualifies for the Delegation of Signature Authority that allows the Regional Office (RO) instead of the Headquarters (HQ) office to process, sign, and submit ROEs, which is generally applicable to safer and smaller financial institutions. Thus, the report processing timeline follows either Schedule A (examination does not qualify for Delegation of Signature Authority) or Schedule B (examination qualifies for Delegation of Signature Authority).

The processing time requirements for stand-alone IT examination ROEs are shown below (in calendar days):

Task	Schedule A (HQ)	Schedule B (RO)
EIC Preparation	5	5
RO Review	+ 17	+ 18
Total RO Processing Time	22	23
Headquarters Review	18	--
Total Processing Time	40	23

When the IT examination results are embedded in the S&S ROE, the EIC preparation time is increased by 2 days in both, Schedule A and B, increasing the total processing time by 2 days.

Audit Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether DOB has developed and implemented policies and procedures and internal controls for effective and timely performance of IT examinations as required by the state and federal guidelines.

Scope

The scope of this audit was Full Scope IT examinations (IT examinations) performed independently by DOB during the time period from September 1, 2015 through January 31, 2016.

Methodology

The audit methodology included a review of policy and procedures, and other internal and external documentation; an interview of the CITSE; a review of a sample of work papers and the respective ROE; a review of compliance reporting; and, the evaluation of data reliability of DOB's database.

We obtained and/or reviewed the following information:

- DOB policies and procedures (i.e. Administrative Memorandum, Supervisory Memorandum, Examiner Bulletin).
- Guidance compiled by DOB from FDIC, FRB, FFIEC and other entities that is listed as "Reference Material" and accessible at DOB's website.
- Data from DOB's Examination Database Information System on the Network (EDISON)

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

- d. DOB's internal reporting on compliance with examination priorities, dated January 5, 2016.
- e. Sample selection of IT examination work papers and respective ROE.
- f. Personal training profile report for IT examiners as of March 3, 2016.

We performed various procedures, to include the following:

- a. Obtained an understanding of the controls in place over the IT Examinations area through review of DOB's established policies and procedures; applicable laws and regulations; and, an interview with the CITSE.
- b. Of the 43 IT examinations performed by DOB during the period from September 1, 2015 through January 31, 2016, we randomly selected 5 and reviewed the corresponding work papers to assess the internal controls in place over the IT examination process.
- c. Reviewed the ROEs of these 5 IT examinations to determine whether they (a) are reflective of the examination results documented in the work papers; (b) report accurate information; and, (c) are prepared in accordance with established policies and procedures.
- d. Reviewed DOB's Personal Training Profile Report as of March 1, 2016 to determine whether commissioned IT examiners meet DOB's training requirements.
- e. Obtained DOB's "Past Due Report" for the period from September 1, 2015 through January 31, 2016 to determine whether—
 - a) IT examinations are performed in a timely manner;
 - b) the data agrees to DOB's examination priorities compliance reporting; and,
 - c) the report was complete by comparison to a listing of regulated banks and trust companies.

Strengths

- DOB has developed and implemented controls to ensure IT examinations are performed in a timely manner. During the period reviewed, 98% of the IT examinations performed by DOB were on time.
- Work performed was well documented in work papers. Amongst the work papers we reviewed, all Report Worthy findings identified in the Summary of Findings (SOF) were included in the ROE, and all Findings included in the ROE were listed as Report Worthy in the SOF.

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

Imaging and Records Management

Background

DOB's Imaging and Records Management area (the Area) is governed by the Texas Government Code Chapter 441 Subchapter L, which defines records management as "the application of management techniques to the creation, use, maintenance, retention, preservation, and destruction of state records for the purposes of improving the efficiency of recordkeeping, ensuring access to public information under Chapter 552, and reducing costs." Corresponding Administrative rules are outlined in Title 13, Chapter 6 of the Texas Administrative Code – State Records.

The Area is managed by the Strategic Support division, and the Director of Strategic Support is DOB's designated Records Management Officer (RMO). The RMO, with the assistance from the Financial Analyst, is responsible for facilitating the review, update, and implementation of the Records Retention Schedule (RRS), and administering DOB's agency-wide records management program to ensure reliability and availability, and timely destruction of state records.

Records Retention Schedule (RRS)

The RRS is a document that identifies and describes a state agency's records and the length of time that each type of record must be retained. Texas state agencies are required to prepare a RRS, using Form SLR 105, and submit it to the Texas State Library and Archives Commission (TSLAC) on a predetermined schedule. Form SLR 105 is designed to ensure compliance with state statutory requirements applicable to the RRS and contains standard information data fields to be completed for each record; such as, the record series item number and title, retention period, and the archival value, if applicable. TSLAC and the State Auditor's Office, if applicable, approve the RRS. A state agency is authorized to dispose of agency records in accordance with an approved RRS, without further consultation with TSLAC.

At DOB, the RRS is prepared by first comparing the existing schedule to the common records listed in the Texas State Records Retention Schedule, to ensure completeness, and then by circulating it to the administrators and division directors for their review and proposed revisions, as applicable to their respective divisions. Upon completion of this internal review process, the RMO will perform a final review and approve the RRS, which is submitted to TSLAC for their approval. DOB's current RRS was approved by TSLAC effective July 7, 2014, and is valid through the last business day of July 2019.

Records Imaging

DOB's state records, in document form (Word, Excel, PDF, etc.), are stored in Document Manager, an enterprise document management system, which is accessed by employees through the following applications:

- TX DOB (primary application)
- Accounting
- Accounting Reporting
- Human Resources
- Exam Work Papers
- Finance Commission
- Executive
- TAPS (tracker for commissioned examiners and candidates)

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

Electronic records are backed up nightly, and duplicate copies of the backup are also stored at DOB's alternate site, in accordance with its disaster recovery plan.

A record in Document Manager consists of two parts: the index and the imaged record. The index is utilized to search and locate records and includes information; such as, the document date, document type, and retention period. Imaging and indexing of records is performed within each division, where employees add records to Document Manager using applications applicable to their respective division. As such, each division is responsible for establishing imaging and indexing procedures and performing a quality control (QC) check. DOB requires a QC check for 100% of imaged records to verify the accuracy of the index and quality of the imaged record. The results of the QC check from each division are reported to the Financial Analyst on a monthly basis to ensure unusual variances are identified and addressed in a timely manner.

Records Deletion

DOB has determined that the administrative burden of complying with the open records requirements pursuant to Government Code Chapter 552, is greatly reduced by promptly destroying records in accordance with their respective retention period. In August 2008, DOB implemented the semiannual records deletion procedures, where each division director is responsible for identifying records for destruction; and, authorizing the Financial Analyst to delete such records from Document Manager. The most recent agency-wide records deletion was conducted in October 2015.

Audit Objective, Scope, and Methodology

Objective

The objective of this audit was to determine whether DOB has developed and implemented policies, procedures, and internal controls to ensure compliance with the State requirements and the Finance Code, as applicable to the Imaging & Records Management area (the Area).

Scope

The scope of our audit covered the time period from September 1, 2015 through March 31, 2016, and included review of the processes and the effectiveness of controls in place in (a) preparing and complying with the RRS; (b) records deletion; and, (c) records imaging.

Methodology

The audit methodology included a review of policy and procedures, the RRS, and other internal and external documentation; an interview of DOB employees, to include the RMO and Financial Analyst; a review of a sample of records stored in Document Manager; and, an observation of the imaging and QC processes.

We obtained and/or reviewed the following information:

- a. DOB policies and procedures related to records management, including the RRS approved on July 7, 2014.
- b. Form SLR 104, a formal designation of DOB's Records Management Officer dated December 5, 2007.

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

- c. A listing of records deleted from Document Manager and the corresponding authorizations during the period from September 1, 2015 through March 31, 2016.
- d. A listing of records imaged/scanned to Document Manager during the period from September 1, 2015 through March 31, 2016.
- e. Document Manager's user access control table.
- f. Sample QC reports for the months of January, February, and March, 2016.
- g. Various internal and external correspondences.

We performed various procedures, to include the following:

- a. Reviewed and obtained an understanding of the applicable rules, laws and regulations of the Texas Administrative Code, the Texas Finance Code, and the Texas Government Code.
- b. Reviewed the current RRS to ensure compliance with the Texas Government Code Section 441.185 and the Texas Administrative Code, Title 13, Sections 6.3 and 6.5.
- c. Randomly selected 25 records from a listing of records deleted from Document Manager during the period from September 1, 2015 through March 31, 2016 to determine whether they were destroyed in accordance with the RRS and DOB's internal procedures.
- d. Randomly selected 20 records, and haphazardly selected 10 records, from a listing of records imaged/scanned to Document Manager during the period from September 1, 2015 through March 31, 2016 to observe the image quality and verify accuracy of the index.
- e. Obtained and reviewed the Document Manager's user access control table to assess the reasonableness of the access levels granted to each employee in relation to their job responsibilities.
- f. Observed the imaging and the QC processes performed by the Bank & Trust Supervision division employees to ensure controls are working effectively.

I. Compliance with Texas Government Code 2102: Required Posting of Internal Audit Information

To comply with the provisions of Texas Government Code, 2102.015 and the State Auditor's Office, within 30 days after approval by the Finance Commission, DOB will post the following information on its website:

- An approved fiscal year 2017 audit plan, as provided by Texas Government Code, Section 2012.008.
- A fiscal year 2016 internal audit annual report, as required by Texas Government Code, Section 2012.009.

The internal audit annual report includes any weaknesses, deficiencies, wrongdoings, or other concerns raised by internal audits and other functions performed by the internal auditor as well as the summary of the action taken by DOB to address such concerns.

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

II. Internal Audit Plan for Fiscal Year 2016

The Internal Audit Plan (Plan) included 2 audits to be performed during the 2016 fiscal year. The Plan also included a follow-up of the prior year audit recommendations, other tasks as may be assigned by the Finance Commission, and preparation of the Annual Internal Audit Report for fiscal year 2016.

Risk Assessment

Utilizing information obtained through the inquiries and background information reviewed, 17 audit areas were identified as potential audit topics. A risk analysis utilizing our 8 risk factors was completed for each individual audit topic and then compiled to develop an overall risk assessment.

Following are the results of the risk assessment performed for the 17 potential audit topics identified:

HIGH RISK	MODERATE RISK	LOW RISK
Bank Examinations	Trust Examinations	Corporate Activities
IT Examinations	Imaging & Records Management	Prepaid Funeral Contracts
Prepaid Funeral Guaranty	Fixed Asset Management	Financial Reporting
Trust/Insurance Funds	Payroll & Human Resources	Travel
	Purchasing	Management Information Systems
	Revenue Accounting Process	Risk Management
		Money Service Businesses
		Perpetual Care Cemeteries

In the prior 3 years, internal audits were performed in the following areas:

Fiscal Year 2015:

- Revenue Accounting Process
- Perpetual Care Cemeteries

Fiscal Year 2014:

- Money Services Businesses
- Management Information Systems

Fiscal Year 2013:

- Corporate Activities
- Prepaid Funeral Contracts

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

The areas recommended for internal audits and other tasks to be performed for fiscal year 2016 were as follows:

Report No.	Audits/Report Titles	Report Date
1.	IT Examinations	3/30/2016
2.	Imaging & Records Management	4/26/2016
2.	Annual Internal Audit Report	4/26/2016
-	Other Tasks Assigned by the Finance Commission	None

III. Consulting and Nonaudit Services Completed

The internal auditor did not perform any consulting services, as defined in the Institute of Internal Audit Auditors' *International Standards for the Professional Practice of Internal Auditing* or any non-audit services, as defined in the *Government Auditing Standards, December 2011 Revision*, Sections 3.33-3.58

IV. External Quality Assurance Review

The internal audit department's most recent *System Review Report*, dated October 7, 2015, indicates that its system of quality control has been suitably designed and conforms to applicable professional standards in all material respects.

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

V. Observations/Findings and Recommendations

Report No.	Report Date	Name of Report	Findings/Recommendations	Status (Implemented, Partially Implemented, Action Delayed, No Action Taken, Do Not Plan to Take Corrective Action or Other)	Fiscal Impact/Other Impact
1	March 30, 2016	IT Examinations	<p>1. Guidance for Scope Waiver</p> <p>Examiner Bulletin XB-2015-03 IT requires the Examiner-in-Charge (EIC) to complete the Scope Form and include a detailed reason for the waiver of an examination procedure. Upon completion, and prior to commencement of the examination, the Scope Form must be approved by the Chief IT Security Examiner (CITSE).</p> <p>Of the 5 IT examination work papers reviewed, 4 sets of (superseded) work papers included a Scope Form that was completed by the EIC and approved by the CITSE, and included a waiver to waive the procedure "#IT-15: Remote Deposit Capture". In 3 instances, the reason documented for the waiver was "N/A" since the institutions did not offer the service; however, in one instance, the reason documented was "no issues in the last exam report."</p> <p>Our discussions with the CITSE indicated that DOB does not have written guidance regarding required documentation for waiver of a procedure; but, in general, determination and approval to waive a procedure is based solely on the judgment of the EIC and CITSE, respectively; and, is primarily used when the procedure is not applicable to the institution.</p> <p>In this specific instance, the CITSE provided a reasonable explanation for approving the scope waiver; however, such justification was not documented in the Scope Form.</p> <p>Recommendation We recommend that DOB provide specific guidance in its policies and procedures to ensure reasons for waiving of examination procedures are appropriate and adequately documented in the Scope Form.</p> <p>Management's Response We agree with this recommendation and updated the IT Examination Scope Form to include valid reasons for waiving examination procedures. The current IT examination procedures, including the scope form, are being replaced with implementation of the Information Technology Risk Examination (InTReX) program. Written guidance for waiving examination procedures has been added to the InTReX scope in use during the pilot program, and the changes will be carried forward to the final version. The InTReX program is expected to be adopted by the DOB by the end of fiscal year 2016.</p>		Improve consistency in the documentation required for waiver of a procedure.

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

Report No.	Report Date	Name of Report	Findings/Recommendations	Status (Implemented, Partially Implemented, Action Delayed, No Action Taken, Do Not Plan to Take Corrective Action or Other)	Fiscal Impact/Other Impact
1	March 30, 2016	IT Examinations	<p>2. Accuracy of TPS/ITP</p> <p>Examiner Bulletin XB-2015-03 IT requires the Technology Profile Script (TPS) worksheet or IT Profile (ITP) worksheet to be completed and/or updated for every examination. The TPS (prior to January 2016) and the ITP (effective January 2016) worksheets are used to assess the complexity of a financial institution's IT operations. In these worksheets, the EIC enters Yes/No in the various fields based on responses received from the respective financial institution. Based on these Yes/No values, a total TPS/ITP score is calculated, which is used to assign a financial institution one of three Complexity Risk Levels. DOB generally assigns an IT Examiner to financial institutions with a moderate to high complexity risk level; while, a non-IT Examiner may be assigned to those with a low complexity risk level. DOB also provides the TPS/ITP score to the FDIC.</p> <p>Our review of 5 IT examination work papers resulted in the following:</p> <ol style="list-style-type: none"> One set of work papers included an incomplete TPS worksheet. Due to a certain input field left blank, the Total Institution Profile Score was calculated as 45, which was 5 points less than what it should have been if the TPS worksheet was properly completed. As a result, the financial institution was assigned as "Type I & II", the lowest risk level represented by scores of 0-49, versus "Type III", represented by scores of 50-79. One Scope Form reflected the TPS Type for the financial institution as "I"; however, the TPS Type according to the TPS worksheet was "III". <p>In both of the above examinations, procedures were performed by an IT Examiner; therefore, misclassification did not cause the inappropriate assignment of an examiner.</p> <p>Recommendation We recommend that DOB establish a procedure to ensure the accuracy of the TPS/ITP worksheet and that financial institutions are appropriately classified in the Scope Form.</p> <p>Management's Response One of the issues occurred because a Y/N box was inadvertently left blank on the TPS by the assistant examiner completing the script. The other error resulted from the assistant examiner completing the scope form not understanding that the TPS Type was not the same as the Exam Type. These were isolated incidents, and the Information Technology Profile (ITP), which replaced the</p>		Improve accuracy of work papers

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

Report No.	Report Date	Name of Report	Findings/Recommendations	Status (Implemented, Partially Implemented, Action Delayed, No Action Taken, Do Not Plan to Take Corrective Action or Other)	Fiscal Impact/Other Impact
1	March 30, 2016	IT Examinations	Technology Profile Script (TPS), will be reviewed by the CITSE prior to approving future scope forms to ensure accuracy and completeness. Additionally, the InTReX program will eliminate the risk of incorrect classifications on future scope forms. The InTReX scope form no longer includes the TPS Type, as "typing" the banks is not part of the InTReX program.		

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

Report No.	Report Date	Name of Report	Observations/Findings and Recommendations	Status (Implemented, Partially Implemented, Action Delayed, No Action Taken, Do Not Plan to Take Corrective Action or Other)	Fiscal Impact/Other Impact
2	April 26, 2016	Imaging & Records Management	<p>1. Records with Archival Values</p> <p>DOB's current Records Retention Schedule (RRS) includes several types of records identified with an archival code "A", meaning the record must be transferred to the Texas State Library and Archives Commission (TSLAC) for retention. Although DOB has a process in place to ensure compliance with this requirement, and such records are generally transferred, there were 3 types of records identified that have not been transferred to TSLAC, as required.</p> <p>Recommendation We recommend that DOB transfer the 3 types of records to TSLAC for retention, to comply with this requirement.</p> <p>Management's Response Management agrees with the recommendation. The three items were sent to TSLAC as reflected in the RRS on May 31, 2016.</p> <p>2. Accurate Retention Period Indexing</p> <p>Each record in Document Manager consists of two parts, the index and the imaged record. Accuracy of the index is critical for searching records in Document Manager; and, the indexed retention period is relied upon by Divisions to ensure records are destroyed in accordance with the retention period during the semiannual records deletion process.</p> <p>Our testing of 30 records imaged and indexed in Document Manager during the period from September 1, 2015 to March 31, 2016 identified one instance where the retention period of a consumer complaint was indexed as 10 years compared to the 2 years in the RRS.</p> <p>Recommendation We recommend DOB implement controls to improve accuracy of the indexed retention period in the Document Manager; such as, utilizing an Image Control Sheet, as used by certain Divisions.</p> <p>Management's Response The Department agrees with the recommendation and will have each division utilize an imaging control sheet to improve indexing. Special Audits implemented the imaging sheet on May 19, 2016.</p>		<p>Ensure compliance with the Records Retention Schedule</p> <p>Improve accuracy of the indexed retention period in Document Manager</p>

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

Report No.	Report Date	Name of Report	Findings/Recommendations	Status (Implemented, Partially Implemented, Action Delayed, No Action Taken, Do Not Plan to Take Corrective Action or Other)	Fiscal Impact/Other Impact
2	April 26, 2016	Imaging & Records Management	<p>3. Semiannual Records Deletion</p> <p>DOB's Administrative Memorandum (AM) 2042 – Deletion of Records, requires each Division Director to identify and authorize the destruction of obsolete records within their respective division, in accordance with the retention period reflected in the RRS. Division Directors are reminded of the semiannual records deletion process and asked to provide the Records Management Officer (RMO) with either a listing of records authorized for deletion to ensure records are deleted from Document Manager in a timely manner; or, an explanation of why there are no records to be deleted.</p> <p>During the most current semiannual records deletion period, only 3 Division Directors responded to the semiannual records deletion email notice dated September 23, 2015. We were also informed by DOB personnel that during April 2016, another Division conducted a thorough review of its documents and identified records for deletion.</p> <p>Recommendation We recommend that DOB enforce compliance with AM 2042 to ensure records are deleted in a timely manner or explanations are provided that support the decision not to delete records with an expired retention period.</p> <p>Management's Response We agree with the recommendation. The Department will enforce the requirements in Administrative Memorandum 2042 to require that a statement from each Director be obtained indicating compliance with the agency retention policy. As of May 31, 2016, management revised the policy to require that any exception to the policy must be approved by a Deputy Commissioner with supporting rationale. As of May 31, 2016, all divisions are in compliance with the deletion policy.</p> <p>4. Records Retention Schedule</p> <p>Our testing indicated that several records series listed in the current RRS either never existed or are no longer utilized by DOB. However, it has been DOB's practice not to delete existing records series from the RRS to avoid the administrative burden in the event of reinstatement of these records.</p> <p>Recommendation We recommend that DOB review each records series and consider removing those no longer relevant to the agency.</p> <p>Management's Response We agree with continuing to amend the RRS as needed based upon our review of the Department's documents. However, management does not agree with removing items regarding agency functions that could be legislatively required in the future.</p> <p>It should be noted that the Texas State Library and Archives discourages removing items that could reemerge in the future from the RRS.</p>		<p>Ensure compliance with DOB's internal policy</p> <p>Improve clarity of Records Retention Schedule</p>

TEXAS DEPARTMENT OF BANKING

Annual Internal Audit Report

Fiscal Year 2016

VI. External Audit Services Procured in Fiscal Year 2016

DOB procured the internal audit services documented in the Internal Audit Plan for fiscal year 2016.

VII. Reporting Suspected Fraud and Abuse

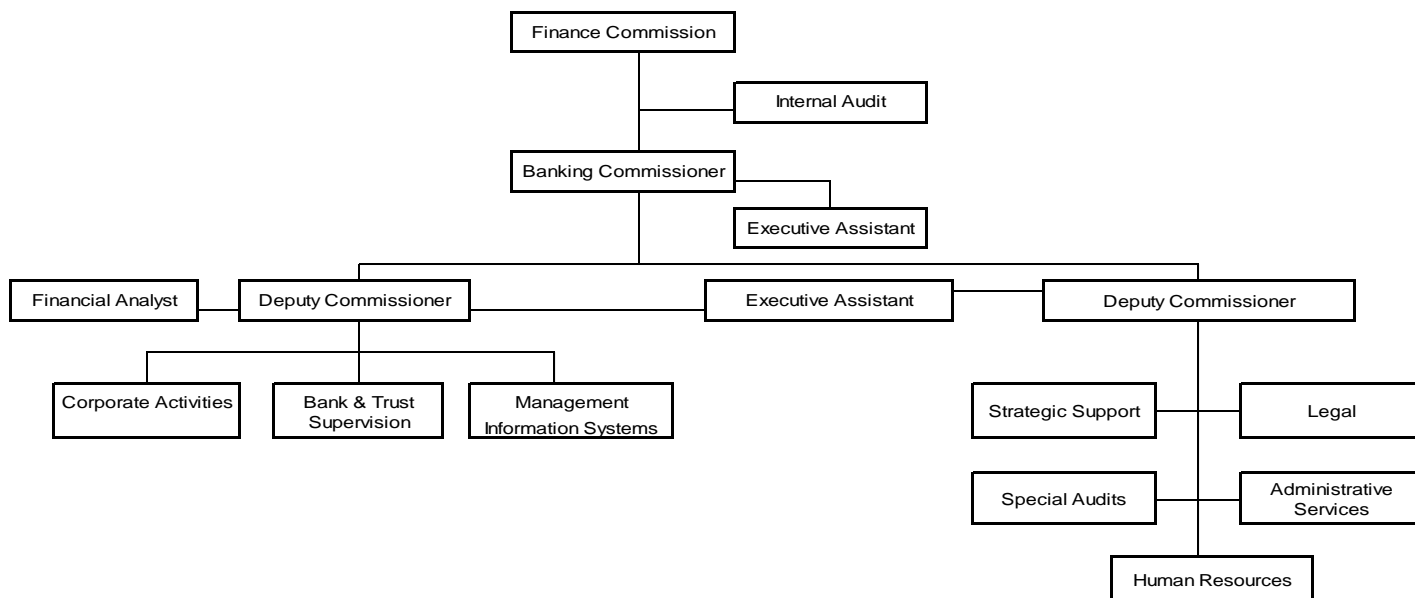
DOB has provided information on their home page on how to report suspected fraud, waste, and abuse to the State Auditor's Office (SAO) by posting a link to the SAO's fraud hotline. DOB has also developed a Fraud Policy that provides information on how to report suspected fraud.

VIII. Proposed Internal Audit Plan for Fiscal Year 2017

The risk assessment performed during the 2016 fiscal year was used to identify the following *proposed* areas that are recommended for internal audits and other tasks to be performed for fiscal year 2017. The Internal Audit Plan for Fiscal Year 2017 will be developed and presented to the Finance/Audit Committee at a meeting to be determined at a later date.

- Trust Examinations
- Prepaid Funeral Guaranty Trust/Insurance Funds
- Follow-up of Prior Year Internal Audits
- Other Tasks Assigned by the Finance Commission

IX. Organizational Chart



Finance Commission Agencies Audit Firms History

Fiscal Year	Audit Firm
FY 2000	Garza/Gonzales & Associates
FY 2001	Garza/Gonzales & Associates
FY 2002	Garza/Gonzales & Associates
FY 2003	Garza/Gonzales & Associates
FY 2004	Garza/Gonzales & Associates
FY 2005	Garza/Gonzales & Associates
FY 2006	Wiener Strickler LLP
FY 2007	Strickler & Prieto LLP
FY 2008	Garza/Gonzales & Associates
FY 2009	Garza/Gonzales & Associates
FY 2010	Garza/Gonzales & Associates
FY 2011	Garza/Gonzales & Associates
FY 2012	Garza/Gonzales & Associates
FY 2013	Garza/Gonzales & Associates
FY 2014	Garza/Gonzales & Associates
FY 2015	Garza/Gonzales & Associates
FY 2016	Garza/Gonzales & Associates

Garza/Gonzales & Associates has committed to rotate audit personnel each year for each agency.



April 18, 2016

Mr. Sami Chandli
Director of Administrative Services
Finance Commission of Texas
State Finance Commission Building
2601 N. Lamar Blvd.
Austin, TX 78705

Re: Audit Delegation Request 449-2016-001

Dear Mr. Chandli:

In accordance with Texas Government Code, Section 321.020, the State Auditor's Office delegates to the Finance Commission of Texas, the Department of Banking, the Department of Savings and Mortgage Lending, and the Office of Consumer Credit Commissioner (Agencies) the authority to employ a private auditor to provide internal audit services as described in your online request submitted April 7, 2016.

This delegation of authority is subject to the following:

1. The services provided should be performed in accordance with the Texas Internal Auditing Act (Texas Government Code, Chapter 2102).
2. This delegation of authority is for state fiscal year 2017.
3. The Agencies will notify the State Auditor's Office if an amendment to the contract significantly alters any contract terms, including, but not limited to, the scope of work to be performed and the term of the contract.
4. The Agencies will comply with applicable law in the procurement of audit services, the expenditure of funds under the contract, and all other aspects of forming and administering the contract with the private auditor.
5. The Agencies will ensure that the State Auditor's Office promptly receives a copy of any report resulting from a peer review of the private auditor that is received by the private auditor after entering into the contract with the Agencies.
6. Any contracts entered into under this delegation of authority should include the following language: The Contractor understands that acceptance of state funds under this contract acts as acceptance of the authority of the State Auditor's Office to conduct an audit or investigation in connection with those funds. The Contractor further agrees to cooperate fully with the State Auditor's Office in the conduct of the audit or investigation, including providing all records requested. The Contractor will ensure that this clause concerning the State Auditor's Office's authority to audit

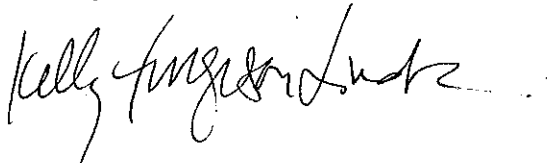
Mr. Sami Chandli
Director of Administrative Services
Finance Commission of Texas
April 18, 2016
Page 2

state funds and the requirement to cooperate fully with the State Auditor's Office is included in any subcontracts it awards. Additionally, the State Auditor's Office shall at any time have access to and the rights to examine, audit, excerpt, and transcribe any pertinent books, documents, audit documentation, and records of the Contractor relating to this contract.

7. If the terms of the agreement with the private auditor are set forth only in an engagement letter, the engagement letter will include the language quoted in #6 above.
8. A signed copy of the contract or contract amendment should be provided to the State Auditor's Office within two weeks of execution. You may send it electronically to auditdelegation@sao.texas.gov or send a hard copy to the attention of Audit Delegation. Additionally, a copy of final audit reports should be provided to the State Auditor's Office upon completion. Texas Government Code, Section 2102.0091, requires that internal audit reports be filed with the State Auditor's Office, the Sunset Advisory Commission, the budget division of the Governor's Office, and the Legislative Budget Board not later than the 30th day after the date the report is submitted to the state agency's governing board or the administrator of the state agency if the state agency does not have a governing board. Internal audit reports may be sent to the State Auditor's Office electronically to iacoordinator@sao.texas.gov or a hard copy may be sent to the attention of Internal Audit Coordinator. Please include the audit delegation request number 449-2016-001 with all submissions and related correspondence.

If you have any questions, please contact Michael Clayton, Audit Manager, or me at (512) 936-9500.

Sincerely,



Kelly Furgeson Linder, CGAP, CIA
Assistant State Auditor

cc Mr. Charles G. Cooper, Banking Commissioner
Ms. Leslie L. Pettijohn, CPA, Commissioner, Office of Consumer Credit Commissioner
Ms. Caroline Jones, Commissioner, Department of Savings and Mortgage Lending

This page left blank intentionally.



2601 North Lamar Boulevard
Austin, Texas 78705
Phone: 512.936.7639
Facsimile: 512.936.7610
www.tfee.texas.gov

Texas Financial Education Endowment Report

Jessica Salazar was selected for the Financial Literacy & Communications Specialist position in late April. She will be assisting the 2016-17 TFEЕ recipients.

During this transition, she has reached out to the eight grantees and provided contact information as their new liaison.

Currently, the Grant Coordinator is conducting status meetings with the grantees to ensure proper documentation is being collected for the required semi-annual grant reports due no later than July 31. The grant report will provide a narrative detailing the performance of the grant-funded program during the reporting period (January 1 – June 30). The grantees will also be eligible to submit a request for reimbursement of funds at this time.