



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 11, 2015

Sheriff K.R. "Kenny" Lemons Jr.
Clay County Sheriff's Office
215 W. Gilbert St.
Henrietta, Texas 76365

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

Dear Sheriff Lemons,

Enclosed is the report on your recent non-criminal justice audit, which was performed on March 9, 2015 by Janet Raeke, Field Representative from the Texas Department of Public Safety. The audit consisted of an interview with Tracie Jinkins, which specifically covered the non-criminal justice audit process as it pertains to state and federal laws.

After the interview, Access and Dissemination personnel performed an audit on the access, use, dissemination, storage, security, and destruction of criminal history record information.

No areas of non-compliance were found.

If you have any questions in regard to the results of this audit, please contact Susie Dial-Herrera, Access and Dissemination Bureau Supervisor, at 512-424-7927.

Sincerely,

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

ML/jmr

DPS Audit
Form
AD-6



TEXAS DEPARTMENT OF PUBLIC SAFETY

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



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

March 11, 2015

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

CRIMINAL JUSTICE AUDIT REPORT

Clay County Sheriff's Office
ORG ID 22075/ORI TX03900H1

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 through secure databases 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 non-criminal justice agencies authorized by state or federal statute, or executive order to receive criminal history record information.

DPS Audit
Form
AD-6

A 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 non-criminal justice 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: In-Compliance

Required Action(s): None

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: (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 Secure Databases and CJIS Security Policies: 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: In-Compliance

Required Action(s): None

DESTRUCTION OF CRIMINAL HISTORY RECORD INFORMATION

Policy: Destruction of criminal history record information must be performed by authorized users. Agencies with access to criminal history record information must follow their 411 statute 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.

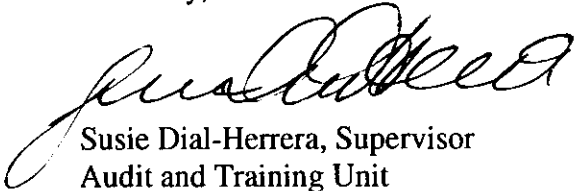
Finding: In-Compliance

Required Action(s): None

OTHER RECOMMENDATIONS

N/A

Sincerely,



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