TEXAS DEPARTMENT OF PUBLIC SAFETY

5805 N. LAMAR BLVD • BOX 4087 • AUSTIN, TEXAS 78773-0001
512/424-2000
www.txdps.state.tx.us

August 8, 2008

Chief Ralph Meyer
Texas State University Police Department
601 University Drive
San Marcos, Texas 78666-4616

Dear Chief Meyer:

Enclosed is the report on your recent TCIC/NCIC Audit, which was performed July 21, 2008. The audit consisted of an interview with the Terminal Agency Coordinator, Liza Ramos. The interview covered several specific areas of TCIC/NCIC operation as indicated in the attached report.

During your previous audit on August 10, 2005, the following areas of non-compliance were noted: Training, Security and Validation.

After the interview, the auditors performed a review of on-line records. A list of current TCIC/NCIC records was compared with your case files. The records checked were from the TCIC Vehicle File. Had your agency entered wanted person records, protective order records and missing person records they would have been checked as well. The records were checked for completeness, accuracy, and validity.

We did not identify any substantive policy violations at your agency. We appreciate your continuing effort to comply with TCIC/NCIC policy.

If you have any questions in regard to the results of this audit, please contact Janet Raeke, TCIC Audit Supervisor, at (512) 424-2809.

Sincerely,

David Gavin, Assistant Chief of Administration
Crime Records Service

DG/ir

TCIC/NCIC AUDIT REPORT

TEXAS STATE UNIVERSITY POLICE DEPARTMENT
TX1050300

JULY 2008

TRAINING

Terminal Operators

State law requires a minimum of one terminal operator be certified per shift as "telecommunicators" by attending 40 hours of TCLEOSE approved training. It should be noted that not all 40-hour "telecommunicator" courses include TCIC/NCIC training. TCIC/NCIC requires that each terminal operator receive TCIC/NCIC training approved by DPS. If the operator takes a "telecommunicator" course that includes TCIC/NCIC training approved by DPS, such as the DPS TLETS/NLETS and TCIC/NCIC Basic Procedures Course, this requirement is fulfilled. In addition to the DPS approved 40-hour telecommunications/procedures school, telecommunication operators can fulfill the TCIC/NCIC requirement by taking a separate DPS approved TCIC/NCIC course (TCLEOSE course number 3802) which is offered through TCLEOSE approved training academies and TCLEOSE "agreement trainers".

The minimum required training for full access operators is the 16-hour TCIC/NCIC Policy and Procedure.

Of the ten authorized terminal operators, nine have been to a telecommunications course which fulfills the TCIC/NCIC requirement. Operator training was said to be on-the-job training.

The recently hired operator must attend approved TCIC/NCIC training.

AS A REMINDER - DPS requires all agencies maintain one forty hour certified DPS trained operator per shift. This includes the DPS TLETS/NLETS Operators Course (24) hours. For more information go to the TLETS menu screen, type in SCHOOLS and depress the PF1 or F1 key.

Officers, CID, Management Personnel

TCIC/NCIC policy requires that these personnel receive TCIC/NCIC training. TCLEOSE offers DPS approved training modules that can be used by TCLEOSE certified academies and "agreement trainers" to fulfill the TCIC/NCIC training requirements.

The minimum required training for officers is the 4-hour TCIC/NCIC Policy and Procedure.

NCIC/TCIC training requirements have been met by the personnel in this section.

Records Personnel/Support Staff

TCIC/NCIC policy requires that these personnel receive TCIC/NCIC training. TCLEOSE offers DPS approved training modules that can be used by TCLEOSE certified academies and "agreement trainers" to fulfill the TCIC/NCIC training requirements.

NCIC/TCIC training requirements have been met by the personnel in this section.

AS A REMINDER – If you provide TCIC/NCIC/TLETS/NLETS information to non-terminal agencies' personnel, they also must be trained.

SECURITY

The TLETS Terminals are secure from unauthorized persons having direct access to the terminals on a 24-hour basis. A background check and fingerprint check are made of all new employees who have access to TCIC/NCIC information. Only authorized personnel may operate the terminals.

There is a written policy addressing terminal access.

DISSEMINATION

The policy of the department is that system-derived information is used only for criminal justice purposes by criminal justice employees. The policy is documented.

TCIC/NCIC QUALITY CONTROL

A standard procedure is in place for handling Quality Control. Departmental policy is that the Terminal Agency Coordinator will handle Quality Control messages. The policy of Quality Control is written.

VALIDATION

Validation requires the Originating Agency to confirm that the record is complete, accurate and still outstanding. Validation is accomplished by reviewing the TCIC/NCIC record and current supporting documents. In the Vehicle file, Boat file, Wanted Person file, and Missing Person file, validation also requires recent consultation with any appropriate source, such as the complainant, victim, prosecutor, or court (see NCIC 2000 Operating Manual, Introduction Section 3.4).

Your agency has a system of recontact in place for the Vehicle file, Boat file, Protective Order File, Missing Person file, and Wanted Person file records.

A written policy concerning Validation is in place. Due to the number of errors policy is not being followed effectively.

HIT CONFIRMATION

Hit Confirmation Policy requires that departments with active TCIC/NCIC records be able to respond to inquiries regarding the validity of those records within the time limit specified in the request, either **Priority 1 for Urgent** or **Priority 2 for Routine**. Confirmation of the record must be made by review of the case file or original warrant.

Confirmation is done by verifying with the case file, protective order file, missing person file or original warrant, which is the correct method.

A written policy concerning Hit Confirmation is in place.

USE OF COMPUTERIZED CRIMINAL HISTORY RECORD INFORMATION (CHRI)

Computerized Criminal History Record Information stored in TCIC/NCIC is not available to the public over TLETS. Certain restrictions apply to the purposes for which it can be requested and how it may be disseminated. CHRI may be requested through the TLETS terminal by Criminal Justice agencies for the administration of Criminal Justice or background investigation of a Criminal Justice applicant. Section 411.124 of the Texas Government Code allows for certain inquiries for conviction data on drivers of public transportation vehicles. Section 411.085 of the Texas

Government Code addresses the penalty for the unauthorized obtaining, use, or disclosure of Criminal History Record Information (see Texas User Pages III, A-B; CR NEWS Sept. 1993 and Spring 1998; NCIC 2000 Operating Manual III; CJIS SECURITY POLICY).

During the audit interview, the TAC, Liz Ramos, stated that Criminal History inquiries were not run through the TLETS terminal for unauthorized purposes, such as: private or governmental employment (except Criminal Justice employment), fire department employment, military recruiting, or a citizen's own record review.

At the time of the audit, your agency had no criminal history log to review.

The "REQ" field is properly identified when running Criminal History inquiries.

The "ATN" field is properly identified when running Criminal History inquiries.

The "OPR" field is properly identified when running Criminal History inquiries.

The Purpose Code "J" is properly used when inquiring on Criminal Justice Agency applicants.

There is a written policy for handling of CCH by department personnel.

AS A REMINDER -- All inquiries must be properly identified in the REQ, ATN, and OPR fields by unique identifiers. The best practice would be Title/Rank First Name Last Name.

CJIS Security Policy states:

An automated log shall be maintained for a minimum of one (1) year on all NCIC and III transactions. The III portion of the automated log shall clearly identify both the operator and the authorized receiving agency. III logs shall also clearly identify the requester and the secondary recipient. The identification on the log must take the form of a unique identifier that must remain unique to the individual requester and to the secondary recipient (see *CJIS Security Policy,* May 2006, Version 4.3, 8.0 Use and Dissemination of Criminal History Record Information (CHRI) and NCIC "Hot File" Information, 8.4 Logging).

The Privacy Act of 1974 requires the FBI to maintain an audit trail of the purpose of each disclosure of a criminal history record and the recipient of that record. Therefore, inquiries and record requests transmitted to III must include the purpose for which the information is to be used. The purposes for which certain agencies may use III and the appropriate codes for use are the following:

Criminal Justice (purpose code C) – Used for official duties in connection with the administration of criminal justice. (*NCIC 2000 Operating Manual,* III, Section 2.1, 4)

Criminal Justice Employment (purpose code J) – Used when the III transaction involves employment with a criminal justice agency or the screening of employees of other agencies over which the criminal justice agency maintains management control. (*NCIC 2000 OPERATING MANUAL,* III, Section 2.1, 4)

Weapons-related Checks (purpose code F) – Used by criminal justice agencies for the purposes of (a) issuing firearms-related permits and explosives permits pursuant to state law, regulation, or local ordinance; (b) returning firearms to their lawful owners; and (c) enforcing federal and state law prohibiting certain persons with criminal records from possessing firearms, in circumstances in which firearms have been pawned. (NCIC Technical and Operational Update, Section 2, 2.1., p. 2-2, September 9, 2002)

The Department requested that you provide documentation for a small percentage of Criminal History inquires for the month of March and April 2008. Of the nine CCH requests, your agency verified the purpose for nine inquiries.

AS A REMINDER – In addition to the use of purpose codes and logging information, all users shall provide a reason for all III inquiries whenever requested by NCIC System Managers, CSA's, local agency administrators, or their representatives. Pursuant to FBI policy which states that an agency must be able to provide a reason for running a CCH/III inquiry, TLETS-provided screens for criminal history inquiries will contain a new optional field, RFI (reason for inquiry). All personnel are encouraged to submit information in this field whenever possible. When used, the RFI field may contain up to 75 characters (alphabetic/numeric/special characters). Some examples of RFI: booking classification, traffic stop, drug investigation, jailer applicant, warrant entry (or validation). A case number may also be included with the reason, but is not required. Recent FBI/NCIC audits have caused the DPS to create this new field to allow the local agency, and the DPS, to capture additional information regarding criminal history transactions and store that information in the automated DPS transaction logs (see *CJIS Security Policy,* May 2006, Version 4.3, 8.0 Use and Dissemination of Criminal History Record Information (CHRI) and NCIC "Hot File" Information 8.3 Justification and Penalization, 8.3.1 Justification).

ORIGINATING AGENCY IDENTIFIER (ORI)

NCIC policy requires "agencies making inquiries for another agency must use the ORI of the other agency". These inquiries include any wanted person, missing person, stolen property, or criminal history checks made for another agency (see CJIS SECURITY POLICY).

At this time, your agency does not make inquiries for other agencies.

RECORDS KEEPING

At the time of the audit, your agency had no wanted persons, missing persons or protective orders entered into TCIC/NCIC.

Prior to the audit, the auditors reviewed fifteen vehicle records entered by your department into TCIC/NCIC. While at your agency, the auditors compared those records to the case files. In the records, the following errors were found:

VEHICLES

INVALID RECORDS

No Protective Order/Missing Person/Theft Report or Original Warrant	**0**
Duplicate Records	**0**
In computer after property recovered/ warrant served/missing person located	**0**
Entry criteria (property lost, not stolen; subject wanted for questioning only; CAPIAS PRO FINE; will not extradite (EW); will not transport anywhere in Texas (EE); etc.)	**0**
INACCURATE KEY FIELD (NAM, SEX, RAC, DOB, LIC, LIS, VIN) MIS-HITS.	**0**
NON-KEY FIELD	**2**
INCOMPLETE	**1**
UNTIMELY ENTRY	**0**

The accuracy of a record is double-checked by a second party.

To ensure maximum effectiveness, NCIC 2000 records must be entered immediately when the conditions for entry are met, not to exceed 3 days, upon receipt by the entering agency. The only exceptions to immediate entry are when otherwise prescribed by federal law or when documentation exists to support delayed entry.

ROLE OF THE NCIC TERMINAL AGENCY COORDINATOR

The NCIC Terminal Agency Coordinator (TAC) shall be responsible for ensuring compliance with state and NCIC policy and regulations, including validation requirements. The person selected as TAC should be knowledgeable in all aspects of TCIC/NCIC use and should have the authority to implement operation changes and oversee operations which affect the use of TCIC/NCIC.

END