	Houston Independent School District Police Department Directives	DIRECTIVE: 460-005
		EFFECTIVE DATE: August 29, 2018
	SUBJECT: TCIC/NCIC Records	REVISED DATE: February 13, 2022

PURPOSE

This directive aims to establish guidelines for the Houston Independent Police Department personnel when utilizing the TCIC/NCIC system. This directive applies to all Houston Independent School District Police Department personnel.

POLICY

It is the policy of the Houston ISD Police Department to ensure all local, state, and federal regulations are adhered to when utilizing the TCIC/NCIC system.

GENERAL

All communications operators will read and initial all Crime Records Newsletters and posted notices. We will keep a permanent file of these notices in the communications area for reference.

The terminal will be kept secure at all times, and access will be restricted to authorized personnel only.

All problems relating to TCIC/NCIC will be forwarded to the Terminal Agency Coordinator for resolution.

The department's participation in the TCIC/NCIC system is conditional upon our adherence to the policy as set out in the NCIC Operating Manual and applied through these guidelines. We are subject to audit by the DPS and FBI on a triennial basis for compliance with all TCIC/NCIC policies.

QUALITY CONTROL

DPS and FBI will send quality control messages when they find errors in the agency's records. Follow the procedures below for any messages received from DPS or the FBI:

MESSAGES FROM DPS

When any DPS messages are received, the communications operator on duty will resolve the problem at the time, if possible, forwarding the messages to the Senior Dispatcher and the TAC. If the operator cannot resolve the problem, the agency will send DPS a message advising that they are looking into the problem and notify the supervisor of the problem.

If our records are correct, the communications operator will notify DPS that our records show the entry to be valid and forward all messages to the supervisor.

MESSAGES FROM FBI/NCIC

Error messages from the FBI will have a $.E. at the top of the message. The record will already have been canceled by the FBI/NCIC. The communications operator on duty at the time will try to resolve the serious error and re-enter the record if possible, passing information to the supervisor. If the communications operator cannot resolve the problem, they will notify the communications supervisor of the $.E. message.

VALIDATION PROCEDURES

Every month DPS will send a printout of one month of our records that we must verify as accurate, valid, and complete. The Terminal Agency Coordinator will direct activities to validate the stated deadline. Validation is a high-priority records-keeping control, and all employees will assist the TAC as appropriate.

The definitions and procedures for validation are as follows:

a) Validation (vehicle, boat, fugitives, protective orders, and missing person entries) requires the entering agency to confirm the record is complete, accurate, and still outstanding or active.

b) Validation is accomplished by reviewing the original entry and current supporting documents and by recent consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files, or other appropriate sources or individuals.

c) If the entering agency is unsuccessful in its attempts to contact the victim, complainant, etc., the entering agency must decide whether or not to retain the original entry in the file based on the best information and knowledge available.

d) The established validation procedures must be formalized and copied on file for review during TCIC/NCIC audits.

NOTE: NCIC has advised that contacting prosecutors, courts, or other appropriate sources or individuals do not have to be concurrent with the validation mailing. If you have a system that provides contact within approximately 90 days after entry and annually after that, your department is within NCIC guidelines. There is no requirement that this “recent consultation” be by phone. You may use a system of written notification if that would be preferable.

HIT CONFIRMATION PROCEDURES

Responsibilities during Hit Confirmation, whether requesting it from another agency or providing it to another agency, must accomplish the following:

a) Ensure that the person or property inquired upon is identical to the person or property identified in the record.

b) Ensure that the warrant, missing person, or theft report is still outstanding.

c) Obtain a decision regarding the extradition of the wanted person.

d) Obtain information regarding the missing person's return to the appropriate authorities.

e) Obtain information regarding the return of stolen property to its rightful owner.

f) We will be especially careful to ensure that the person or property in custody is the same as the person or property in the theft report or warrant, regardless of whether we are requesting the confirmation ourselves or replying to another agency's request for confirmation on one of our records.

When we are asked for confirmation on our records:

a) The operator on duty will reply to all requests for Hit Confirmation within the time limit specified in the request.

b) If they cannot provide the positive or negative confirmation within that time, they will immediately send a message to the requesting agency giving them a specific amount of time to confirm or deny.

c) We will confirm all hits by reviewing the original case report or warrant accomplishing the above five items.

d) We will provide written Hit Confirmation to requestors whenever possible. If it is impossible for some reason, we will confirm the phone and follow up with a terminal message when possible.

e) Under no circumstances will a Hit Confirmation request to our agency be allowed to go unanswered.

When we ask another agency for confirmation of one of their records, It is the OPERATORS responsibility to:

a) Notify the officer of the hit and request confirmation, then send a message to the agency that entered and fully described the person or property in custody.

b) The inquiring agency is responsible for determining the priority of the request (URGENT or ROUTINE). An URGENT priority request should be used when a substantive response is needed within ten minutes. A ROUTINE priority request should be used when a substantive response is needed within one hour.

c) If within the time limit specified in the first request, the entering agency does not provide positive confirmation, negative confirmation, or the

specific amount of time they need to confirm or deny, the operator will send another message requesting confirmation to the entering agency. The operator will enter the number two (2) in the request number field. This will cause the message to be also sent to the appropriate state CTA(s).

d) If the agency does not confirm within the time specified in the second request, the operator will send a message to the entering agency. The operator will enter the number three (3) in the request number field. This will also cause the message to be sent to the appropriate state CTA(s) and the FBI/NCIC in Clarksburg, W. Virginia.

It is the OFFICERS responsibility to:

a) Understand that the hit alone is not probable cause to arrest. The hit confirmed with the originating agency is one factor to be added to other factors at the scene to arrive at an arrest decision.

b) Understand the Hit Confirmation process and that they are responsible for ensuring that the person/property in custody is the same as the person/property of the record, along with the other safeguards stated above.

c) NCIC guidelines describe Hit Confirmation over the terminal; however, there is no NCIC requirement for Hit confirmation written. We will accept telephone Hit Confirmation only when terminal confirmation is impossible for some reason. Then we will insist that the agency follow up with terminal confirmation when it becomes possible.

We will obtain Hit Confirmation from the entering agency before taking any of the following actions on hits:

a) Arresting the wanted person.

b) Detaining the missing person.

c) Seizing the stolen property.

RECORD LOCATE (HITS)

After receiving Hit Confirmation from an agency on one of their records for a person or property in custody, the communications operator will place a locate on that record if the entering agency has not cleared it.

Agencies may place locates on their records, which will enable them to place a detainer when necessary.

RECORD ENTRY (PROPERTY)

Records will be entered only when a valid theft report is on file or other TCIC/NCIC entry criteria are met.

The record will be entered as soon as possible after the theft report has been received, not to exceed three days, unless proper documentation is available supporting the delayed entry.

It is the INVESTIGATING OFFICERS responsibility to:

a) Ensure that an official theft report is made or other entry criteria are met.

b) Ensure all information in the theft report is accurate and all required information is included.

c) Provide the information to the communications operator as soon as possible.

It is the TELECOMMUNICATORS responsibility to:

a) Verify that the information meets TCIC/NCIC entry criteria.

b) Verify vehicle and boat registrations.

c) Bring to the attention of the Dispatch Manager/TAC any missing or incorrect data.

d) Enter the record with available data, if possible. Once the report is checked, the telecommunicators operator needs to annotate the date and time the report was received for entry and ensure the record is entered within three days.

e) Double-check the information on the screen before entry.

f) Record the entry in the proper file, including date, operator's initials, and hard copy of entry acknowledgment. Also, include a hard copy of registration returns as well.

g) Return report file to officer or reports section.

It is the communications supervisor's responsibility to:

a) Verify the validity of the record.

b) Double-check all data entered against the theft report.

c) Ensure that the record is entered as soon as possible after receiving the theft report.

d) Coordinate with the investigating officers on obtaining complete information when it is not included in the theft reports.

RECORD ENTRY (PERSONS)

Records will be entered only when a valid warrant, protective order, or missing person report is on file or other NCIC entry criteria are met.

The record will be entered as soon as possible after the warrant, protective order, or missing person report has been received, not exceeding three days (unless proper documentation supports the delayed entry). The exception to the 3-day entry is the entry of missing juveniles. Missing juveniles must be entered within 2 hours of receipt of the report. Federal criteria apply to any missing person under the age of

It is the INVESTIGATING OFFICERS responsibility to:

a) Ensure that an official warrant is issued or a missing person report is made.

b) Ensure all information in the warrant, protective order, or missing person report is accurate and all required information is included.

c) Obtain a forecast of extradition for wanted persons.

d) Provide the information to the communications operator as soon as possible.

It is the TELECOMMUNICATORS responsibility to:

a) Verify that the information in the warrant, protective order, or missing person report meets TCIC/NCIC entry criteria.

b) Verify vehicle registration through DMV and identification information through DL and CCH checks. Include in the entry alias information from DL and CCH returns, but only when there is a high degree of certainty that DL and CCH returns are subject to the warrant.

c) Bring to the attention of the Dispatch Manager/TAC any missing or incorrect data that makes TCIC/NCIC entry impossible. Enter the record with available data, if possible. Once the report is checked, telecommunicators need to annotate the date and time the report was received for entry and ensure the record is entered within three days.

d) Double-check the information on the screen before entry.

e) Forward the hard copy of the record to the officer for inclusion in the proper case file, including date, operator's initials, and hard copy of entry acknowledgment. Also include a hard copy of DMV, DL, and CCH checks.

f) As current policy indicates, enter the wanted person record into TCIC and NCIC.

g) Enter the protective order person into TCIC and NCIC based on information obtained from the court.

It is the communications supervisor's responsibility to:

a) Verify the validity of the record.

b) Double-check all data entered against the warrant or missing person report and DMV, DL, CCH checks. Ensure that DL and CCH information was added as appropriate. This double-checking includes verification that the wanted person was entered into TCIC only, or TCIC and NCIC, as appropriate according to the forecast of extradition.

c) Ensure that the record is entered as soon as possible after receiving the warrant or missing person report.

d) Coordinate with the officers on obtaining complete information when it is not included in the warrant or missing person report.

RECORD LOCATE (RECORD CLEAR)

After receiving Hit Confirmation from an agency on one of their records for a person or property in custody, the communications operator will place a locate on that record if the entering agency has not cleared it.

Agencies may place locates on their records, which will enable them to place a detainer when necessary.

HANDLING OF INFORMATION OBTAINED OVER THE TLETS TERMINAL

Who can request information?

a) Only commissioned officers and other authorized persons within the department will be allowed to request terminal inquiries of any kind.

b) Requests from outside the department will be honored when the identity of the Requestor can be verified as a commissioned officer or another authorized person (probation officer, parole officer, judge, etc.) who is requesting for a criminal justice purpose. Appropriate logging for CCH information, as indicated below, is mandatory.

c) All authorized personnel are responsible for limiting their requests to the official,

d) criminal justice purposes only.

STOLEN AND WANTED INFORMATION

Stolen and wanted information can be requested by officers as needed. No dissemination log is necessary, and the information can be broadcast over the radio without restriction, except as necessary to safeguard the officer.

We will always check for TCIC/NCIC warrants on incoming arrestees and prisoners as they are being released.

We will check for wanted using all alias names, dates of birth, and identifying numbers that come to our attention for each subject. When an NCIC inquiry yields a hit, the terminal operator will note on the printout precisely how, when and to whom the information was given; initial and date this notation and forward it to the inquiring officer or agency for retention in the case file.

We will obtain Hit Confirmation from the entering agency before taking any of the following actions on hits:

a) Arresting the wanted person.

b) Detaining the missing person.

c) Seizing the stolen property.

CRIMINAL HISTORY INFORMATION

Criminal history information is confidential, and certain restrictions apply to the purposes for which it can be requested and how it can be disseminated.

WHO CAN REQUEST CRIMINAL HISTORY INFORMATION?

Only commissioned officers and other authorized persons can request criminal history checks within the department. These requests can be made through appropriate personnel. Logging, as indicated below, is mandatory.

Requests from outside the department will be honored only when the Requestor can be verified as an authorized person as indicated in PART 10 of the NCIC Operating Manual, "Who May Access Criminal History Data." Logging, as indicated below, is mandatory.

Purposes for which CCH can be requested:

a) It must be criminal justice investigation or investigation of a criminal justice applicant (applicant at the police department, sheriff's office, or other criminal justice agency--not at a noncriminal justice city or county office).

b) It cannot be requested by anyone regardless of rank or status for any other purpose. The telecommunications operator will report any CCH inquiries that they know are for unauthorized purposes to their

supervisor.

c) It is also permissible to run a CCH on an individual to return a weapon. The appropriate purpose code for this inquiry is PUR/F.

d) CCHs must also be run before entering warrants, missing persons, and protective order records. Per NCIC Operating Manual (page 2 of introduction), all records must be kept accurate and up to date with all available information. In keeping with NCIC policy, CCHs must also be run when these records are validated each year.

e) No one shall request inquiries for unauthorized purposes or persons.

LOGGING OF CCH INQUIRIES: OPERATOR/REQUESTOR/ATTENTION FIELDS:

Requestors must be properly identified in the "REQ" and "ATN" fields. If numbers are used in the REQUESTOR and ATTENTION fields along with the Requestor's last name, numbers must be unique to your department and NOT be reissued to another employee when your agency no longer employs the current holder. You may use the title and full name of the requesting party in the "Requestor" or "Attention" field (example: REQ/Officer Betty Rhoades; REQ/Chief Roy Davis; ATN/Officer Don Stone; ATN/Neil Brooks DA). The preferable method is to use the title along with the first and last name of the Requestor.

If the Requestor is an authorized person from another agency or office, identify that person by name and the name of their agency or office in the "REQ" and "ATN" fields (example: REQ/Officer Tim Moon Anywhere PD; ATN/DA James Wood). If you are authorized to use the other agency's ORI, you must use their ORI instead of your own ORI.

The person operating the terminal must be properly identified in the "OPR" field. You cannot use first names only or initials or non-unique numbers. The preferable method is to use the first and last names of the person operating the TLETS terminal (example: OPR/Vera Patterson; OPR/Norman Green).

Train your operators to be consistent in identifying the REQUESTOR, ATTENTION, and OPERATOR fields.

LOGGING OF CCH INQUIRIES: REASON FOR INQUIRY

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. (NCIC Operating Manual, III, Introduction Section 2.1.4)

Pursuant to FBI policy which states that an agency must provide a reason for running a CCH/III inquiry, TLETS-provided screens for criminal history inquiries will contain an RFI field.

The RFI field may contain 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 criminal history transactions and store that information in the automated DPS transaction logs.

DISSEMINATION OF CCH INFORMATION

The Criminal history information obtained over the terminal will be given only to the person in the REQ, ATN, or written log. It can be passed to that person through an appropriate support person.

The officer receiving the information is responsible for keeping the printout secure and immediately returning it to the appropriate file or properly disposing of it.

If someone outside the department needs a CCH printout, another CCH inquiry will be made because of the frequent updates/revisions to the NCIC III and TCIC CCH records.

We will maintain an audit trail of the handling of the printout within the department by keeping it with the case file at all times or by disposing of it immediately after it's' no longer needed and when there is no case file.

Manual logging of QH and QR inquiries is optional but highly recommended.

Making the requestor sign a manual log for the printout is optional but recommended. It would help if you established procedures for storing and destroying received information. The destruction process must provide an audit trail either by logging or by the implementation of standard or auditable

Agency procedures to assure that destruction is accomplished by routine steps. A manual log with a "Disposition of Printout" column would be a good way to start an audit trail.

BROADCASTING OF CCH INFORMATION

Criminal history data may be transmitted over any electronic device when an officer determines there is an immediate need for this information to further an investigation or a situation affecting an officer's safety or the general public.

We will not indicate over the radio whether or not a subject has a criminal history in situations where the officer has not determined a need for the record information. We will check for criminal history on all alias names, dates of birth, and identifying

numbers that come to our attention for each subject. The responses we receive over the terminal are possible identifications only; we will have to submit fingerprints to DPS to obtain identification.

POLICY VIOLATIONS

Department personnel violating TLETS/NLETS, TCIC/NCIC policies are subject to administrative and criminal sanctions based upon the severity of the misuse. Violations will be handled on a case by case basis by the agency administrator and may lead to the following action(s):

a) Written or verbal counseling;

b) Written or verbal reprimand;

c) Suspension, termination, or prosecution under Government Code 411.085.

RECORD CANCELLATION AND CLEAR

It is the OFFICERS responsibility to:

a) Notify the communications division as soon as possible when information becomes available indicating that a theft report or warrant was invalid.

b) Notify the communications division as soon as possible when the property of a theft report is recovered, or a warrant is served, recalled, or in any other manner becomes inactive.

c) Mark the case files to indicate the status of the enclosed theft reports/warrants and file appropriate hard copy terminal returns to document the status of the TCIC/NCIC records involved.

d) A stamp on the outside of the file or a checklist inside to indicate the TCIC/NCIC record status is highly recommended.

It is the COMMUNICATION OPERATORS responsibility to:

a) Remove records from the file as soon as possible after being notified by an officer that the case has been cleared or that the record was invalid. Invalid records will be canceled with the “X” message key, and recovered property/person records will be cleared with the “C” message key.

b) Forward the hard copy of the terminal return showing the cancel or clear to the officer for placement in the case file.

c) Be sure that the record(s) are cleared from the system(s), including TCIC and NCIC, when the record was entered into both systems.

It is the COMMUNICATION SUPERVISORS responsibility to ensure that the record(s) are cleared from the system(s) in a timely manner with the proper message key.

DISPOSAL OF MEDIA

The agency shall sanitize, that is, overwrite at least three times or degauss digital media before disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps to sanitize or destroy electronic media. Agencies shall ensure authorized personnel witness or carry out sanitization or destruction. (CJIS Security Policy 5.5 - 5.8.3 Digital Media Sanitization and Disposal) Using formal procedures, physical media shall be securely disposed of when no longer required. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromised by unauthorized individuals. Physical media shall be destroyed by shredding or incineration. Agencies shall ensure authorized personnel witness or carry out the disposal or destruction. (CJIS Security Policy 5.5 – 5.5.8.4 Disposal of Physical Media)

Approved By _____

Pedro Lopez Jr., Chief of Police