THE CRIME RECORDS SERVICE NEWSLETTER

CR NEWS

Volume 14, Number 2-3

April — Sept

HIGHLIGHTS:

CR NEWS is published by the Texas Department of Public Safety. Comments, Suggestions and mailing list updates are welcome.

Contact:
CR News MSC 0230
Attn: Jim Phillips
PO Box 4143
Austin, TX 78765-4143
Jim.phillips@txdps.state.tx.us

TCIC/NCIC Entries of Vehicles Stolen in Mexico

THE PROBLEM

Upon returning to their homes in Texas after having had their personal vehicles stolen in Mexico, Texas citizens are finding that there is not a uniform statewide policy among law enforcement agencies regarding the entry of those vehicles into TCIC/NCIC. Some agencies are making TCIC/NCIC entries in these cases, but not necessarily under the same conditions. This document is to define a statewide policy.

BACKGROUND

Most law enforcement agencies are aware that FBI policy limits the authority to enter a stolen vehicle to the agency of primary jurisdiction over the location of the theft incident:

> *"6. All NCIC 2000 entries should be made only by the agency holding the theft report and having primary jurisdiction over the place of actual theft. An exception to this occurs when a criminal justice agency or regional dispatch center acts as holder of a record for another agency that has no telecommunication equipment…" (NCIC Operating Manual; Vehicle File)*

Some agencies may not be aware that there is also a policy that allows for the entry of vehicles stolen in other countries, as well:

(Continued on page 3)

CRS DIRECTORY

CRS MANAGEMENT

David Gavin	Assistant Chief, Administration	david.gavin@txdps.state.tx.us	512-424-2077
Mike Lesko	Deputy Administrator	mike.lesko@txdps.state.tx.us	512-424-2524
Alan Ferretti	Information Security Officer	alan.ferretti@txdps.state.tx.us	512-424-5686

ACCESS & DISSEMINATION BUREAU

Don Farris	Manager	donald.farris@txdps.state.tx.us	512-424-2078
Baerbel Cleveland	Supervisor, Support	baerbel.cleveland@txdps.state.tx.us	512-424-2023
Sharon Hill	Supervisor, Training & Audit	sharon.hill@txdps.state.tx.us	512-424-7920
Elaine Smith	Supervisor, CHIU	elaine.smith@txdps.state.tx.us	512-424-5474
Assistance Line	Record Checks		512-424-5079
Assistance Line	Secure Site		512-424-2474

CRIMINAL HISTORY RECORD INFORMATION PROCESSING BUREAU

Angie Klein	Manager	angie.klein@txdps.state.tx.us	512-424-2471
Greg Easley	Assistant Manager	greg.easley@txdps.state.tx.us	512-424-7163
Holly Morris	Section Supervisor, Data Integrity	holly.morris@txdps.state.tx.us	512-424-2154
Vacant	Assistant Supervisor, ER		512-424-7253
Pat Molloy	Section Supervisor, Fingerprints	patricia.molloy@txdps.state.tx.us	512-424-2153
Gretna Holiday	Dayshift Supervisor, Fingerprints	gretna.holiday@txdps.state.tx.us	512-424-2408
Kathy Parks	Dayshift Supervisor, Fingerprints	kathy.Parks@txdps.state.tx.us	512-424-5749
Claudia Crislip	Evening Shift Supv., Fingerprints	claudia.Crislip@txdps.state.tx.us	512-424-5709
Judy Miller	Midnight Shift Supv., Fingerprints	judith.miller@txdps.state.tx.us	512-424-5748
Vacant	LiveScan Coordinator		512-424-2409
Cassandra Richey	Supervisor, CJIS Field Reps	cassandra.richey@txdps.state.tx.us	512-424-2479
Cheryl Sanchez	AFIS Project Assistant	cheryl.sanchez@txdps.state.tx.us	512-424-2089
Charlene Cain	CCH Internet Coordinator	charlene.cain@txdps.state.tx.us	512-424-2090
Ursula Cook	EDR Coordinator	ursula.cook@txdps.state.tx.us	512-424-2407
24 hour Fingerprint Assistance Line			512-424-5248

CRIME INFORMATION BUREAU

Randy Batten	Manager	randy.batten@txdps.state.tx.us	512-424-2734
Pam Pierce	TCIC Systems Analyst	pam.pierce@txdps.state.tx.us	512-424-2898
Vacant	TCIC Operations Supervisor		512-424-7659
Diane Wells	TCIC Training Supervisor	diane.wells@txdps.state.tx.us	512-424-2982
Janet Raeke	TCIC Audit Supervisor	janet.raeke@txdps.state.tx.us	512-424-2897
Jill Gajkowski	TCIC Control Room Supervisor	jill.gajkowski@txdps.state.tx.us	512-424-2152
Alison Price	Program Administrator, HEAT	alison.price@txdps.state.tx.us	512-424-2962
Rosemary Webb	Program Administrator, UCR	rosemary.webb@txdps.state.tx.us	512-424-2418
Linda Carter	Supervisor, UCR Clerical Supervisor	linda.carter@txdps.state.tx.us	512-424-3646
Tom Jenkins	Supervisor, UCR Field Reps	tom.jenkins@txdps.state.tx.us	512-424-2983
Pam Nickel	IBR Supervisor, UCR	pam.nickel@txdps.state.tx.us	512-424-2979
Vincent Castilleja	Sex Offender Reg. Coordinator	vincent.castilleja@txdps.state.tx.us	512-424-2279

CRS LEGAL STAFF

Louis Beaty	Manager	louis.beaty@txdps.state.tx.us	512-424-5836

CRS SUPPORT BUREAU

Desiree Taylor	Manager	desiree.taylor@txdps.state.tx.us	512-424-2968
Jim Phillips	Program Specialist	jim.phillips@txdps.state.tx.us	512-424-7794
Jimmy Guckian	Program Specialist	jimmy.guckian@txdps.state.tx.us	512-424-7915
Michelle Farris	Project Specialist	michelle.farris@txdps.state.tx.us	512-424-7130
Jennifer Norton	Budget Analyst	jennifer.norton@txdps.state.tx.us	512-424-7793
Rochelle Gutierrez	Billing Technician	rochelle.gutierrez@txdps.state.tx.us	512-424-2912
Tierra Heine	Fingerprint Card Supplies	**Fax order form to**	**512-424-5599**
		Order Forms located at ftp://crspub.txdps.state.tx.us/	

TCIC/NCIC ENTRIES OF VEHICLES STOLEN IN MEXICO

(Continued from page 1)

> *"7. In addition, data of investigative interest pertaining to stolen vehicles, vehicle parts, or related vehicle titles stolen abroad and transported into the United States may be entered by an agency having sufficient documentation to be responsible for the record. Vehicle parts may include blank, stolen, or counterfeit documents relating to the registration of the vehicle abroad or subsequent to its invalid titling in the United States, as well as license plates issued on the basis of fraudulent proof of ownership." (NCIC Operating Manual; Vehicle File)*

In light of the potential use of vehicles stolen in Mexico for the movement of persons or contraband back into the United States, or for their use by transnational gangs in acts of crime or terrorism, the DPS recognizes an inherent investigative interest for their entry into TCIC/NCIC. While the policy for entry refers to the vehicles having been transported back into the United States, that fact will normally remain unknown if the record is not entered into TCIC/NCIC. As a result, DPS does not require that an agency wanting to make an entry actually know that the vehicle or vehicle part has already been transported back into this country.

TCIC POLICY STATEMENT

In light of the above considerations, DPS will consider the below bullets to constitute "sufficient documentation" and will allow entries into TCIC/NCIC of vehicles and vehicle parts stolen in Mexico, under the following conditions:

- The person making the theft report in the U.S. must be the registered owner of the vehicle.
- The registered owner must present to the Texas entering agency a theft report from the Mexican law enforcement agency where the theft occurred, showing that the theft was reported to the jurisdiction of the incident in Mexico.
- The Texas entering agency must create a theft report on the vehicle or vehicle part.
- The Texas entering agency must follow Validation, Hit Confirmation, and all TCIC/NCIC policies for the record.
- The record is entered as a stolen vehicle or stolen vehicle part (MKE/EV or MKE/EP), and must state "Stolen in Mexico" in the Miscellaneous Field.

(Continued on page 7)

TCIC/NCIC ASSOCIATE TRAINER REPORTING

ATTENTION: TCIC/NCIC ASSOCIATE TRAINERS

In 2007, the Crime Records Service, TCIC Training Unit, advised associate trainers that all TCLEOSE reports of NCIC/TCIC classroom training were required to be sent to the TCIC Training Unit to be entered by the DPS academy.

Effective September 1, 2008, NCIC/TCIC associate trainers will once again have the authority to submit training hours directly to TCLEOSE either through an academy or through an agency that has a TCLEOSE Provider Number. **Trainers that enter hours directly to TCLEOSE MUST submit a copy of the reports to TCIC Training within five (5) days from the date of training.** TCIC Training will update the OMNIXX student database and grant permissions to the student to access the OMNIXX system.

Associate trainers that are unable to report credit hours directly to TCLEOSE, will still be able to submit the reports to TCIC Training. The reports will be entered by the DPS academy into TCLEOSE. **The reports MUST be received no later than five (5) days from the date of training in order to receive credit.** Reports can be sent by fax to: (512) 424-7164, Attention: TCIC Training or email: tcic.training@txdps.state.tx.us .

All reports are required to have the social security number (SSN) of the students in attendance. This will grant students access into the OMNIXX system. **Failure to report the SSN will deny the student access to TLETS through the OMNIXX system.** Student information missing the SSN will be submitted to the DPS academy for TCLEOSE credit hours. However, TCIC Training **will not update the OMNIXX student database without the SSN. The student cannot be entered into OMNIXX without the SSN.**

In addition, the TCLEOSE Personal Identification Number (P_ID) is required in order for the DPS training academy to submit the hours to TCLEOSE. The DPS academy will not enter the hours if the P_ID is missing from the report. The P_ID must be verified prior to submittal.

Associate trainers who submit reports directly to TCLEOSE must also send the information to TCIC Training in order for the student information to be updated in the OMNIXX system.

All reports sent to TCIC Training **MUST** be submitted within five (5) days from the date of training. Reports that are not submitted in a timely fashion may lead to the student being denied access into the OMNIXX system and NCIC/TCIC databases.

For further assistance please contact TCIC Training at: 512 424-2832, or email: tcic.training@txdps.state.tx.us . Your cooperation is greatly appreciated.

DATA PROTECTION PROCEDURES FOR RETIRED CJIS EQUIPMENT

After receiving a new computer with all the peripherals, one spends considerable time setting it up and getting the data moved from the old system to the new one. Everything will be humming along fine and someone will suggest reusing or recycling the old system, which in times of tight budgets and overflowing landfills sounds like a reasonable consideration. One often thinks about destroying old paper media containing Criminal Justice data by shredding or incinerating, but what about the electronic media? The old computer could have sensitive CJIS data stored on it and should be properly sanitized. The requirements for this can be found in the *CJIS Security Policy*, version 4.4, sections 4.6 Disposal of All Media and 4.7 Media Reuse.

CJIS data could be stored on hard drives, floppies, tapes, CDs, DVDs, PDAs, compact flash, memory sticks, Jump Drives, etc., all of which will require proper sanitizing before being allowed outside your secure location and possibly used for another purpose. Agencies should check their organization's policies on data retention and disposal before sanitizing equipment. The most important thing to remember is that simply running the *delete* or *format* command on a hard drive or other media will not be enough to definitively destroy the information. It is crucial that sensitive criminal justice data not be inadvertently put into an unauthorized user's possession. Accidental release could lead to unauthorized information disclosure.

Reusing and recycling computer equipment can be accomplished by properly sanitizing the equipment before reuse within the agency or disposal outside the agency. Two common methods for media sanitization are overwriting data and physical destruction. To reuse media like hard drives, the information it contains should be destroyed with software that essentially writes over the data several times ensuring that the data cannot be retrieved and reconstructed. Permanent destruction of media could involve physically breaking the device or rendering it unusable. Some other methods of sanitization include degaussing, incinerating, pulverizing, shredding, and sanding. If you have any questions about media sanitization or destruction, please contact the CJIS Security Office at the Texas Department of Public Safety. To read more about media sanitization visit the NIST website http://csrc.nist.gov/publications/PubsSPs.html or http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

ANTI-VIRUS PROTECTION

Is your PC suddenly running slower or acting “different”? One of the first things that come to mind is your PC has a virus, but you’re not connected to the Internet. How can that happen? Do you have antivirus protection on your PC? The answer should be “Yes.” Particularly since Section 7.12 of the CJIS Security Policy states “*All IT systems with CJIS connectivity shall employ virus protection software*.”

A common belief is that if you’re not connected to the Internet, then your PC isn’t exposed to being infected with “malware”. Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. Computer viruses are just one of many malware programs.

So, just how did that virus get there? Did you recently play a music CD a friend made for you? What about the thumb drive you used to copy pictures of your grandkids? Perhaps a file was infected and copied itself onto your PC. If so, it may have spread to the TLETS network and could be attempting to infect other PCs. If you had antivirus protection, chances are it would have been detected and deleted or quarantined.

Here are a few tips to help protect your PC:

Scan files for viruses before using them. This is always important, but especially if you are using a disc or flash memory to carry information between one computer and another. You could easily pick up a virus from a corrupted file and introduce it into your system. Running a virus scan before launching any of new files will prevent infection.

Don't boot from an unknown data CD. Data CDs are one of the most common ways viruses are transmitted. If you are using a data CD while working on your computer, remove it when you shut the machine off or the computer may automatically try to boot from the disc, perhaps launching or installing bad programs or files on your computer.

Get immediate protection. Configure your antivirus software to run automatically on start-up and continue to run at all times. This will still provide you protection in case you forget to scan an attachment, or decide not to. And in case you forget to start up your antivirus software, configuring it to start by itself will ensure you get immediate protection always.

Install reliable antivirus software. Antivirus software scans files regularly for unusual changes in file size, programs that match the software's database of known viruses, suspicious email attachments, and other warning signs. There are hundreds of new viruses released every day, so it is important to select a program that receives updates on a regular basis, preferably automatically.

(Continued on page 7)

ANTI-VIRUS PROTECTION

(Continued from page 6)

The bottom line is your PC *must* run antivirus software if you have CJIS connectivity.

If you have any questions, feel free to contact the CJIS Security Office at the TXDPS.

To read more about malware, how to prevent it and incident handling, refer to NIST Special Publication 800-83 “Guide to Malware Incident Prevention and Handling” at http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

TCIC/NCIC ENTRIES OF VEHICLES STOLEN IN MEXICO

(Continued from page 3)

ADDITIONAL CONSIDERATIONS

There is no requirement that an agency make these entries. That decision remains with the agency.

The registered owner does not have to be a resident of the jurisdiction of the Texas agency making the entry. The entering agency may consider entries for persons from other cities, counties, or states.

This policy is written for vehicles and vehicle parts stolen in Mexico, but may be applied for vehicles and vehicle parts stolen in other countries, as long as the Texas entering agency perceives an investigative interest in placing the record into TCIC/NCIC.

For questions about this policy, please contact the TCIC Control Room at (512) 424-2088 or Mnemonic Address “CRDP”.

CJIS REPORTING

Attention County & District Clerks!!!!

There are a few different ways to report the nondisclosures to the Crime Records Service. Counties that are EDR (Electronic Disposition Reporting) should continue to report using the CDN 401 & CPN of 392. If you have any questions regarding how to report nondisclosures and you are an EDR county, please contact Ursula Cook at 512/424-2407 or email ursula.cook@txdps.state.tx.us. Counties that utilize the paper CR-44 Court supplemental should continue and use the CDN 401 & CPN of 392 and mail the form to CRS. Copies of the order may be mailed to CRS but if you prefer to scan the file and email it to us instead of US Post, you may use the newly created email box: NonDisclosures@txdps.state.tx.us.

DPS IDENTIFICATION SUPPLIES ORDER FORM

TO: CRIME RECORDS SERVICE
TEXAS DEPARTMENT OF PUBLIC SAFETY
PO BOX 4143
AUSTIN TX 78765-4143 Date:________________________
FAX: 512-424-5599
Please furnish the following supplies:

FORM NIUMBER	DESCRIPTION	# PER PACKAGE	QUANTITY ORDERED
CR-6	DPS Applicant Card*	250 p/pkg	
CR-12	DPS Identification Supplies Order Form	100 p/pad	
CR-23	Out of State Probation/Parole Supervision Card	Single cards	
CR-26	Death Notice Form	100 p/pad	
CR-42	Request for Criminal History Check	100 p/pad	
CR-43	Adult Criminal History Reporting Form **with** Preprinted TRN and Fingerprint Card Attached*	100 p/pkg	
CR-43	Adult Criminal History Reporting Form with Fingerprint Card Attached*	100 p/pkg	
CR-43J	Juvenile Criminal History Reporting Form **with** Preprinted TRN and Fingerprint Card Attached*	100 p/pkg	
CR-43J	Juvenile Criminal History Reporting Form with Fingerprint Card Attached*	100 p/pkg	
CR-43P	Adult Probation Supervision Reporting From **with** TRN Numbers	200 p/pkg	
CR-43P	Adult Probation Supervision Reporting Form **without** TRN numbers	200 p/pkg	
CR-44	Adult Supplemental Reporting Form	100 p/pkg	
CR-44J	Juvenile Supplemental Reporting Form	100 p/pkg	
CR-44S	Adult Supplemental Court Reporting Form	100 p/pad	
CR-45	Adult DPS Fingerprint Card*	250 p/pkg	
CR-45J	Juvenile DPS Fingerprint Card*	250 p/pkg	
FD-249	FBI Arrest & Institution Fingerprint Card (Felony Card)*	500 p/pkg	
FD-258	FBI Applicant Fingerprint Card*	500 p/pkg	
FD-353	FBI Personal Identification Fingerprint Card*	500 p/pkg	
R-84	FBI Final Disposition Notice	500 p/pkg	
	Fingerprint Card Return Envelopes (For Arresting Agency Only)	100 p/box	

***DPS does not pre-stamp the agency ORI on any fingerprint card. Overnight services are available at ordering agency's expense.**

NOTE: Please order minimum of three weeks supply. Please submit order at least 4 weeks prior to depletion of your supplies.

NOTICE: Provide a complete shipping address (PO box (s) are acceptable).

AGENCY NAME____

STREET ADDRESS____

COUNTY____________________________CITY____________________________________STATE TX ZIP___________

ATTENTION____PHONE NO. (_____)______-______