Security and Privacy Training For Non-Certified Users

Revised November 5, 2013

Table of Contents

INTRODUCTION

The following document is a brief overview of information regarding Security and Privacy information for the non-certified user of the DCI Network. This document is not all-inclusive, and further information is available in the North Carolina Administrative Code Title 12 Department of Justice Chapter 4, Division of Criminal Information, henceforth referred to as the Administrative Procedures. A copy of the administrative procedures may be located by contacting your Point of Contact (POC), Terminal Agency Coordinator (TAC) or the TAC at your Servicing Agency. A copy of Administrative Procedures may be found in the following locations:

- the reference section of the Terminal Agency Coordinator Manual
- Omnixx Force/Links/Compliance/NCAC Reference

A Point of Contact (POC) is an individual designated by the agency head to act as a liaison between the SBI and the agency receiving and/or entering Criminal Justice Information (CJI). The person assigned to this position is to ensure compliance with state and national regulations pertaining to the access and use of CJI.

A Terminal Agency Coordinator (TAC) is an individual designated by the agency head to act as a liaison between the agency and the CIIS staff as required by the Federal Bureau of Investigation. The person assigned to this position is to ensure compliance with state and national regulations pertaining to the use of the criminal justice computer system - (DCIN and the systems it accesses). Each agency having access to DCIN/NCIC must appoint a Primary TAC and may appoint an Assistant TAC (ATAC).

As a user of the information provided through the DCI Network, you assume responsibility for utilizing information within the boundaries of the rules and regulations pertaining to the access, use and dissemination of information received through DCIN and the systems it accesses.

DCI certified operators, vendors, city/town/county IT personnel will be required to complete security awareness training every three years or if a new employee, with DCIN access, within 6 months of employment.

Due to highly publicized court cases and numerous special audits across the state, it has become evident that many users are not aware of the rules regarding appropriate access and dissemination of information through the DCI Network.

This guide is provided as general information and as a reference tool for official law enforcement use only. For detailed information refer to the noted documents.

Section I – Rules Regarding Access

The use of information obtained through the DCIN and the systems it accesses is regulated by state and federal legislation and administrative code. This information is provided for Law Enforcement and Criminal Justice uses only. Each particular file has its own rules regarding access and copies of appropriate documentation will be provided to you throughout this manual as each section is covered.

The primary rule regarding access to this information is that if the information is not needed for the performance of your official duties; you should not be requesting it. Law enforcement has access to the DMV files to obtain information relating to the performance of their duties; however, a personal desire to know information is not an appropriate use of information. If in doubt about whether or not this is an appropriate use of information, contact your Point of Contact (POC), Terminal Agency Coordinator (TAC) or a fully certified operator.

Section II – Use of Computer Equipment

Operation of computer equipment accessing DCIN files is restricted to those individuals who have been properly certified through a DCIN approved certification class. The one exception to this rule is that while in training to become a certified operator and under the direct supervision of a certified operator; a trainee may utilize the equipment for training purposes. This does not allow for access when not under the supervision of a certified operator.

Section III – DMV

1. Access to DMV information is for criminal justice purposes only. Any other type of request should be carefully reviewed to determine whether or not it meets dissemination criteria. If an individual requests information for a purpose other than specified below, they should be referred to the Department of Transportation Division of Motor Vehicles.

2. Federal Driver's Privacy Protection Act: (Enacted by Congress August, 24 1994)

   Chapter 123, Section 2721 requires that personal information in DMV records be closed to the public. This refers to photos, social security numbers, driver's license numbers, names, addresses, telephone numbers and medical information.

   General Purpose: A State department of motor vehicles, and any officer, employee or contractor, thereof, shall not knowingly disclose or otherwise make available to any person or entity personal information about any individual obtained by the agency in connection with a motor vehicle record.

3. Radio Broadcasts of Driver's History Information:

   SBI's legal counsel with the NC Attorney General's Office has advised that a radio broadcast of driver's history information is not recommended because of the ease by which radio broadcast information may be intercepted by unauthorized entities. It is recommended that radio broadcasts of driver's history information be limited to the items set forth herein: general statements such as "license status," "prior/no convictions," "the number of convictions," or any information to warn an officer of a dangerous individual.

   To provide further necessary information to an officer regarding the details of a driver's history, it is recommended that signal or ten codes be established, such as Signal 13 to identify a suspension for DWI and/or Signal 14 for a suspension for anything other than a DWI. The information may also be relayed to the officer in person or via telephone. (By telephone provided the officer's identity is verified.)

4. Dissemination and logging of Driver's History Information: (Administrative Procedures: T12: 4F.0701)

   Driver history data can only be given to authorized law enforcement or criminal justice personnel unless requests are for approved non-criminal justice uses. Refer to Administrative Code Title 12: 04F.0701 (a) (2). Inquiries run for law enforcement or criminal justice personnel in conjunction with their official duties are not required to be logged. Any authorized non-criminal justice uses must be logged.

Driver history data can only be given to authorized law enforcement/criminal justice personnel unless requests are for approved non-criminal justice uses. Refer to Administrative Code Title 12; 04F.0701 (a) (2).

Approved non-criminal justice uses of driver history data are:

1. Defense attorney access.

2. Authorized licensing/non-criminal justice employment checks. (Examples: ABC permits, taxi permits, etc.)

3. Government employees or applicants who will be required to operate a government owned vehicle. (Examples: School bus drivers, fire truck drivers, rescue squad drivers, etc.)

4. Driver history data used for non-criminal justice purposes (1 - 3 above) are required to be recorded on a one-year log of dissemination.

The SBI does not require driver history data disseminated to law enforcement or criminal justice personnel to be logged.

Driver issuance data may be released at the discretion of the agency and in accordance with the Federal Driver's Privacy Protection Act. Any questions regarding interpretation of this law should be referred to the legal counsel for your department, municipality or county.

Section IV – Criminal History Information

Release of criminal history data is regulated by stringent state and federal legislation and policies and procedures. Access to this information varies based on the purpose for which it is requested. Although the main emphasis for use of this information is for law enforcement and criminal justice purposes, there are a few other purposes that have been approved by SBI/FBI for access to the criminal history files. These other purposes are also strictly regulated. The purpose code used in a request determines what information will be returned in the response, so it is required that the appropriate purpose code be utilized when making an inquiry. It is the agency's responsibility to make sure the request for information meets with SBI/FBI accessibility requirements.

1. **Access to State and National Records**:

CRIMINAL JUSTICE purposes – Purpose Code C is utilized for criminal investigations, bond/probation hearings, security of the criminal justice facility to include vendors or contractors who are NOT involved with the administration of criminal justice, volunteers who are NOT involved with the administration of criminal justice and providing a social or community service, security of a military installation, inmates of a confinement facility, and Defense Attorneys with properly authorized forms containing the original signature of the District Attorney/Asst. District Attorney in the prosecutorial district, etc.

Purpose Code C is used by Governmental Social Services agencies with child protection responsibilities and the National Center for Missing and Exploited Children to access FBI criminal history record information under Section 151 of the Adam Walsh Child Protection and Safety Act of 2006 (Public Law 109-248). An NCIC Originating Agency Identifier (ORI) ending in the alpha character "F" has been established for Section 151 access.

This is the only authorized purpose code allowed for DSS agencies and can only be used when investigating or responding to allegations of abuse, neglect, or exploitation of a minor.

CRIMINAL JUSTICE EMPLOYMENT purposes – Purpose Code J is utilized for background investigations for individuals hired and fired by a criminal justice agency head, vendors or contractors who ARE involved with the administration of criminal justice, and volunteers who ARE involved with the administration of criminal justice and providing a rehabilitative service.

PUBLIC HOUSING purposes – Purpose Code H is utilized by authorized public housing authorities assigned an ORI to request criminal conviction information on adult applicants/tenants of public housing for purposes of applicant screening, lease enforcement, and eviction. Purpose Code H is only allowed with the QH transaction to establish the possible existence of a record. If a possible identification record is found and the complete record is requested, the Public Housing Authority must contact the FBI for the release of the record.

DOMESTIC VIOLENCE and STALKING court related purposes – Purpose Code D is utilized by civil and/or criminal courts, where CCH record information is being requested for domestic violence and stalking court cases.

WEAPON RELATED purposes – Purpose Code F is utilized prior to returning a weapon back to the owner.

2. **Access to State Records Only**:

LICENSING /NON-CRIMINAL JUSTICE EMPLOYMENT purposes – Purpose Code Exx (xx = a numeric code) is utilized for non-criminal justice employment or licensing purposes. Written approval must be obtained from the SBI. A numeric code is assigned to each specific licensing check.

DEFENSE (PRIVATE) ATTORNEY purposes – Purpose Code PA is utilized when the Defense Attorney form does not contain the original signature of the District Attorney/Asst. District Attorney. However, the form must contain the signature of the defense attorney and be notarized.

GUARDIAN AD LITEM purposes – Purpose Code GA is utilized when the agency receives a copy of the court ordered appointment of a Guardian Ad Litem who is taking charge of a child being represented in court for an abuse or neglect case.

Any other types of requests for Criminal History Data are not authorized. If an individual has a desire to review or challenge his/her record, he/she should be advised to contact the SBI Identification Section in Raleigh (919) 662-4500.

All inquiries into the criminal history files are logged by the computer system. Agencies having access to criminal history files are required monthly to inquire into the system, print this log, and review it for any discrepancies, sign and date. For Non-terminal agencies such as DSS, the best practice is to request that the agency who provides you service print the automated logs prior to the end of the next month, which will allow for timely review of the logs. Notify the Compliance Unit of any suspected misuse of the information. The CCH log must be maintained for one year from the date of inquiry. When running the CCH log, a NICs log will also be produced, which reflects any NICs inquiries. NICS is a national computer system implemented and maintained by the Federal Bureau of Investigation (FBI) for quickly obtaining information on individuals who may be prohibited from receiving or possessing a firearm under federal law. The NICS log must be maintained for one year from the date of inquiry. Both logs are subject to audit by SBI/FBI personnel.

NOTE: Criminal History record information obtained from or through DCIN, NCIC or NLETS shall not be disseminated to anyone other than authorized criminal justice agencies without the authority of a federal or state statute.

Section V – Other Computerized Information

1. **Administrative Office of the Courts Files: (Clerk of Court Records)**

- All in-house DCIN devices are authorized to have access to AOC files.

- Operators accessing this information must be DCIN certified in this module.

- Administrative Office of the Courts records are governed by Public Records Law, however, inquiries through DCIN are restricted to law enforcement use only.

- No logging requirements by AOC/SBI.

2. **NICS Checks**:

The National Instant Check system provides for inquiries into the system for background checks for the transfer of firearms. Use of these files is restricted to those agencies that are charged with the issuing of permits to purchase or permits to carry concealed weapons.

3. **Miscellaneous File Restrictions:**

The transmission of messages through the DCIN and NLETS systems is restricted to Law Enforcement/Criminal Justice Purposes.

A. **NLETS Administrative Messages**:

NLETS policy prohibits the system to be used for the following:

1. Recruiting of personnel.
2. Message not pertaining to official business.
3. Incomplete messages (insufficient information).
4. Excessively long messages.
5. Routine messages regarding stolen vehicles, stolen property, and wanted persons, which should be in the NCIC system.
6. Attempt to locate vehicle (unauthorized use of conveyance) without warrant.
7. ROIR (Reply Only if Record) message. All messages requesting information must be sent to a specific agency and should result in response whether information is available or not.
8. Messages in which the complainant is interested only in the recovery of property. For the protection of the arresting officer, messages should not be dispatched until a warrant is secured.

B. **In-State SEND Messages**:

SBI policy prohibits the system to be used for the following:

1. The sale of personal items and/or law enforcement items. (I.e. police dogs, computer equipment, radio equipment, automobiles, etc.)
2. Death and or funeral arrangement notices. (Under special conditions when the death and/or funeral arrangements have statewide impact this message would be permitted.)
3. Holiday greeting messages. (I.e. Merry Christmas, Happy New Year.)
4. Personal messages not law enforcement related. (Arrangement of personal meetings, discussions, and conversations related to personal items only.)
5. Messages attempting to locate specific towns or communities in NC. (I.e. Where is Mayberry NC? Does anyone know where zip code 12345 is? Anyone having the phone prefix of 123 please advise.
6. Message regarding lobbying of legislative proposals.

4. **NC Concealed Handgun Files and NC Sex Offender Files**:

Each of these files has specific regulations with reference to the dissemination of the information they contain.

5. **Access Use and Dissemination of NCIC Record Information**:

A. Although the rules regarding access and dissemination of NCIC records information are not as stringent as the rules regarding other files, your agency should develop a written policy as to who and when the information should be given if providing to non-criminal justice personnel. (For example: Often pawn shops may call to see if the gun being pawned is stolen or not, and while this may work with an understanding between your agency and the pawn shop, it is essential that if there is a hit from the NCIC records on this gun, you would be able to seize the weapon. Many agencies have policies that specify that the pawn shop dealer must either bring the gun to the department or have an officer come by to run the check on the gun to ensure the availability of the weapon for seizure.) Each agency should check their own policy to insure that proper procedures are followed.

B. **Hit Confirmation**: (Administrative Procedures T12: 4F.0203)

Any agency entering record information into the DCIN/NCIC files, or which has a servicing agency enter record information, is required to provide hit confirmation 24 hours a day, 7 days a week. Hit confirmation of DCIN/NCIC records means that an agency receiving a positive DCIN/NCIC response from an inquiry must communicate with the official record holder to confirm the following before taking enforcement action:

- Verify that the person or property inquired upon is identical to the person or property identified in the record.

- Verify that the warrant, missing person report, or theft report is still outstanding.

- Obtain a decision regarding the extradition of a wanted person, information regarding the return of the missing person to the appropriate authorities, or information regarding the return of stolen property to its rightful owner.

The official record holder must respond within ten minutes of receiving an ***Urgent*** hit confirmation request or within 1 hour of receiving a ***Routine*** hit confirmation request with the desired information or a notice of the specific amount of time necessary to confirm or reject the record.

The SBI may cancel an agency's record from the DCIN/NCIC files for failure to respond to a hit confirmation request within the specified time frame.

Failure to properly confirm a hit may result in civil liabilities for your agency.

Section VI – Violations and Penalties

If an agency violates the provisions of the Administrative Procedures or other Policies set forth by the SBI, NCIC or NLETS, sanctions may be imposed upon that agency or operator. For a list of violations or penalties you may wish to refer to the Administrative Procedures T12: 4G.0101.0102.

Information pertaining to the appeals and hearing processes may be found in the Administrative Procedures T12: 4G.0201 and 0301.

Conclusion

This manual is provided to act as a guide to major security and dissemination issues. The manual is not all-inclusive, and you may need to refer to the Administrative Procedures for additional information you may desire. Our intent in providing you with this document is to protect you, your agency, and the SBI from criminal or civil liabilities and associated misuse of information accessed through your DCIN device or through a servicing agreement with a local law enforcement agency.