# TABLE OF CONTENTS

**Outline**

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td><strong>Point of Contact (POC)</strong></td>
<td>5</td>
</tr>
<tr>
<td>POC Responsibilities</td>
<td>5</td>
</tr>
<tr>
<td><strong>POC Administrative Duties</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>Dissemination of Information</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
<td>9</td>
</tr>
<tr>
<td><strong>Training Coordinator</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>Audit Coordinator</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Administrative Duties</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Dissemination</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Information Security</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Training Coordinator</strong></td>
<td>10</td>
</tr>
<tr>
<td><strong>Audit Coordinator</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Eligibility for DCIN Access</strong></td>
<td>11</td>
</tr>
<tr>
<td><strong>Legal Agreements for DCIN Access</strong></td>
<td>12</td>
</tr>
<tr>
<td>Sources of Criminal Records</td>
<td>11</td>
</tr>
<tr>
<td><strong>SBI Criminal/Investigative Records</strong></td>
<td>13</td>
</tr>
<tr>
<td><strong>NCIC Interstate Identification Index (III)</strong></td>
<td>14</td>
</tr>
<tr>
<td><strong>International Justice &amp; Public Safety Information Sharing Network (NLETS)</strong></td>
<td>14</td>
</tr>
<tr>
<td>Additional Files and Available Information</td>
<td>15</td>
</tr>
<tr>
<td><strong>National Crime Information Center (NCIC)</strong></td>
<td>15</td>
</tr>
<tr>
<td><strong>North Carolina Only Files</strong></td>
<td>15</td>
</tr>
<tr>
<td>Authorized DSS Uses of National/State Records</td>
<td>15</td>
</tr>
<tr>
<td><strong>Purpose Code C</strong></td>
<td>15</td>
</tr>
<tr>
<td>Access &amp; Dissemination Requirements for Computerized Criminal History (CCH)/Criminal History Record Information (CHRI)</td>
<td>16</td>
</tr>
<tr>
<td>Access</td>
<td>16</td>
</tr>
<tr>
<td>Dissemination</td>
<td>16</td>
</tr>
<tr>
<td>Definitions</td>
<td>17</td>
</tr>
<tr>
<td>Forms Section</td>
<td>20</td>
</tr>
<tr>
<td><strong>Criminal History Request Form</strong></td>
<td>20</td>
</tr>
<tr>
<td><strong>Sample Servicing Agreement</strong></td>
<td>21</td>
</tr>
<tr>
<td><strong>Error Reporting Notice</strong></td>
<td>25</td>
</tr>
<tr>
<td><strong>Agency Information Change Form</strong></td>
<td>26</td>
</tr>
<tr>
<td><strong>Security &amp; Privacy Manual</strong></td>
<td>27</td>
</tr>
<tr>
<td>Title: Department of Social Services Point of Contact Training</td>
<td></td>
</tr>
<tr>
<td>-------------------</td>
<td>------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Purpose:</td>
<td>To present POC’s an overview of:</td>
</tr>
<tr>
<td></td>
<td>- POC Responsibilities</td>
</tr>
<tr>
<td></td>
<td>- Access to DCIN/NCIC Records</td>
</tr>
<tr>
<td></td>
<td>- Regulations Regarding Documentation</td>
</tr>
<tr>
<td>Training Objectives:</td>
<td>At the end of this instruction, POC’s will be able to achieve the following objectives:</td>
</tr>
<tr>
<td></td>
<td>1. Define Point of Contact (POC) and explain the purpose of the agency POC.</td>
</tr>
<tr>
<td></td>
<td>2. Identify the roles and responsibilities of the POC.</td>
</tr>
<tr>
<td></td>
<td>3. Identify standards and agreements required to be maintained by the Department of Social Services (DSS).</td>
</tr>
<tr>
<td></td>
<td>4. Identify sources of criminal records available to DSS.</td>
</tr>
<tr>
<td></td>
<td>5. Explain the authorized uses of National/State records.</td>
</tr>
<tr>
<td></td>
<td>6. Explain rules and regulations regarding access and dissemination of criminal record information.</td>
</tr>
<tr>
<td>Hours:</td>
<td>Three (3)</td>
</tr>
<tr>
<td>Instructional Method:</td>
<td>Lecture/Discussion</td>
</tr>
<tr>
<td>Training Aids:</td>
<td>Computer Slide Projector</td>
</tr>
<tr>
<td></td>
<td>Computer Slideshow</td>
</tr>
<tr>
<td></td>
<td>Student Outline/Manual</td>
</tr>
<tr>
<td></td>
<td>Security and Privacy Manual</td>
</tr>
<tr>
<td></td>
<td>DCIN Security Awareness Training Log</td>
</tr>
<tr>
<td>Revised By:</td>
<td>Pat Viverette</td>
</tr>
<tr>
<td></td>
<td>District Training Specialist</td>
</tr>
<tr>
<td></td>
<td>Training Unit</td>
</tr>
<tr>
<td></td>
<td>SBI Criminal Information and Identification Section</td>
</tr>
<tr>
<td>Revised Date:</td>
<td>April 30, 2014</td>
</tr>
<tr>
<td>Revised By:</td>
<td>Jessica Woodard</td>
</tr>
<tr>
<td></td>
<td>District Training Specialist</td>
</tr>
<tr>
<td></td>
<td>Training Unit</td>
</tr>
<tr>
<td></td>
<td>SBI Criminal Information and Identification Section</td>
</tr>
<tr>
<td>Revised Date:</td>
<td>November 8, 2013</td>
</tr>
<tr>
<td>Revised By:</td>
<td>Jessica Woodard</td>
</tr>
<tr>
<td></td>
<td>District Training Specialist</td>
</tr>
<tr>
<td></td>
<td>Training Unit</td>
</tr>
<tr>
<td></td>
<td>SBI Criminal Information and Identification Section</td>
</tr>
<tr>
<td>Revised Date:</td>
<td>October 24, 2013</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Revised By:</td>
<td>Jessica Woodard</td>
</tr>
<tr>
<td></td>
<td>District Training Specialist</td>
</tr>
<tr>
<td></td>
<td>Training Unit</td>
</tr>
<tr>
<td></td>
<td>SBI Criminal Information and Identification Section</td>
</tr>
<tr>
<td>Revised Date:</td>
<td>August 9, 2013</td>
</tr>
<tr>
<td></td>
<td>Jessica Woodard</td>
</tr>
<tr>
<td></td>
<td>District Training Specialist</td>
</tr>
<tr>
<td></td>
<td>Training Unit</td>
</tr>
<tr>
<td></td>
<td>SBI Criminal Information and Identification Section</td>
</tr>
<tr>
<td></td>
<td>June 17, 2013</td>
</tr>
</tbody>
</table>
I. Introduction

A. What is a Point of Contact (POC)?

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.

1. The POC should be knowledgeable of State and National policies and procedures regarding access and dissemination.

2. The POC should be someone who can be allowed adequate time and attention to performing the functions of the position and who is authorized to enforce regulatory compliance within the agency.

II. POC Responsibilities

A. POC Administrative Duties

As your agency POC, you will have many responsibilities.

1. ON-SITE EXPERT IN POLICY AND PROCEDURES REGARDING ACCESS

Being assigned as the POC for your agency, you must be familiar with all policies and procedures enforced by NCIC, DCIN and your agency.

a) The Administrative Code Title 12 Chapter 4 Sections E, F and G are the Codes that authorize the SBI and are used as a foundation for policies and procedures enforced in NC for the operation of the DCIN.

b) The Security and Privacy Training Manual for Non-Certified users is available to assist your agency with important Security Training for all non-certified users accessing Criminal Justice Information (CJI).

c) A mandatory Security Awareness Training video has been prepared by NC DOJ/ITD to ensure the confidentiality, integrity, and availability of Criminal Justice Information System (CJIS) data and systems throughout the user community.
d) Your agency should adopt written Standard Operating Procedures concerning access to the information received through the DCI Network.

2. **ENSURE ALL POLICIES ARE ADHERED TO BY ALL AGENCY PERSONNEL**
   Each criminal justice and non-criminal justice agency authorized to access CJI shall have a **written policy** for the discipline of CJI policy violators.

3. **REVIEW AND MAINTAIN ALL CCH/NICS LOGS**
   a) Logs are used to comply with NCIC/DCIN rules regarding access and dissemination.
   b) Logs are created automatically as inquiries are performed.
   c) Logs must be obtained for each DSS ORI. If no Computerized Criminal History (CCH) inquiries are made within a specific month, a log must still be printed by the agency providing the service and maintained by DSS.
   d) A monthly summary log is available on the first day of the following month.
   e) Logs are available only for the previous eighteen months.
   f) Responses provide a listing of all criminal/investigative inquiries made at a specific devise; including rejected transactions and National Instant Criminal Background Check System (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.
   g) A monthly audit must be conducted at each agency. 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.
   h) CCH logs must be signed by the DSS Director or a designated representative and dated indicating a monthly review has occurred.
   i) Both the CCH and the NICS logs must be maintained on file for one year.
j) Review of the log

(1) Once the automated log has been printed:

(a) Agency personnel must review the log to verify compliance with DCIN/NCIC regulations.

(b) The individual reviewing the log should verify the following:

(i) Purpose codes and transaction codes should match when run on the same individual. (i.e. If two transactions are run on the same individual for the same purpose, both transactions should utilize the same purpose code.) **Purpose code C is the only allowable purpose code for DSS.**

(ii) Requestors should be verified as appropriate requestors for records and may assist in assuring the proper purpose codes and message keys were used.

(iii) Secondary Dissemination should appear on the transactions for records that are shared with someone outside of your agency and include the name of the person or agency the record was disseminated to.

(c) Once the review has been completed, the automated CCH & NICS logs should be signed, dated and kept on file for one year from the date of inquiry and are subject to audit by the Compliance Unit and FBI.

4. REPORT NON-COMPLIANCE ISSUES WITHIN THE AGENCY

a) The POC should email the Compliance Unit at ARAHELP@NCDOJ.GOV with any discrepancies or errors found during the monthly review. In the body of the email explain in detail the error that was found. In the event of an operational error such as improper purpose code use, the servicing agency is responsible for reporting the error. The Error Reporting Notice is located in the Forms Section of this manual.

5. NOTIFY SBI/CIIS OF UPDATES AND CHANGES TO AGENCY STAFF
a) **Agency Head Change** – If the agency head leaves that position, the acting or permanent agency head must re-sign the User Agreement and any Servicing Agreements that are in place.

(1) Written notification should be in the form of a letter or email sent to the Compliance Unit or through the completion of the Agency Information Change form located in the Forms section of this manual.

(2) The POC will make sure a new Servicing Agreement is signed by the new agency head for the agency as well as the servicing agency. This is a legal binding contract with the new agency head. Once a new Servicing Agreement is signed, a copy shall be sent to the SBI Compliance Unit and to each agency affected by the agreement.

b) **Changes in POC Appointment** – The POC may designate one or more assistant POCs (APOC) to assist in the duties of the POC role. In the event the POC/APOC of an agency leaves the position and a new POC/APOC is approved, an email should be sent to the Compliance Unit (ARAHELP@NCDOJ.GOV) notifying them of the change.

(1) The exiting POC or a POC from another DSS office will be responsible for training the new POC/APOC.

6. **NOTIFY SBI/CIIS OF ADDRESS, PHONE, FAX OR EMAIL CHANGES**

a) **Change of Address** – If the address for your agency changes, an email should be sent to the Compliance Unit (ARAHELP@NCDOJ.GOV) notifying them of the change.

b) **Phone and Fax Number Changes** – If the phone or fax number changes for a non-device agency, it is the POC’s responsibility to notify the SBI in writing of these changes.

c) **Changes in Agency Name or County** – If the agency name changes or the agency moves to a different county, the POC must notify the Compliance Unit in writing of the change. This may be accomplished in the form of an email to ARAHELP@NCDOJ.GOV or completion of the Agency Information Change form located in the Forms section of the manual.

7. **YEARLY NCIC/NLETS ORI VALIDATIONS**
The Originating Routing Identifier (ORI) files give users nationwide the capability to inquire upon any ORI to receive its translation and other information. Each agency nationwide is required to maintain accurate information in their ORI files. All ORIs must be validated every year.

a) NCIC ORI files can be modified at any time by the servicing agency. Corrections can be made using the Modify NCIC ORI Record (MO) transaction.

b) To make corrections to your NLETS ORI file, contact the Compliance Unit (ARAHELP@NCDOJ.GOV).

B. Dissemination of Information

1. Security and Privacy Training Manual – The Security and Privacy Manual for Non-Certified Users was developed to provide additional training in the use of information obtained through the DCIN and the systems accessed through DCIN. A copy of the manual is located in the Forms Section of this manual.

NOTE: This manual is available to assist with the Security and Privacy training, but is not required. The Security Awareness Training Video is required by DCIN/CJIS policy and must be viewed every two (2) years.

2. The Security Awareness Training Video is required by the CJIS Security Policy and must be provided every two (2) years to all personnel who manage or have access to FBI CJIS Systems or information.

   a) All new employees shall receive security awareness training within six (6) months of their appointment or assignment.

   b) All contractors and vendors including IT personnel that have access to CJIS systems shall receive security awareness training within six (6) months of their appointment or assignment.

   c) Documentation pertaining to the materials used and those employees which receive the training must be maintained in a current status.

   d) The Security Awareness Training Video Log must be signed by each employee and contractor or vendor that completes this training and kept on file for two (2) years. The logs are subject to audit.

C. Information Security

9
1. Ensure that all state and federal regulations are adhered to.

2. Ensure all criminal history record information (CHRI) is kept in secure locations and is disseminated only for criminal justice purposes.
   a) Criminal history record information may be incorporated into the DSS case file provided that security measures are taken to ensure no unauthorized disclosure occurs.
   b) Basic, non-personal identifying information may be summarized from CHRI results and included in the case file. (For example, the agency would not be permitted to include the FBI number, NC SID number, Social Security number or date of birth obtained via DCIN, but the agency would be able to include basic information like a 1984 theft or shoplifting charge.) Neither the FBI nor the SBI should be identified as the source of the information.
   c) Records shall be stored in a physically secure location. A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personal security controls sufficient to protect Criminal Justice Information (CJI) and associated information systems.
   d) Criminal history record information may be used only by employees of the NC governmental social service agencies when investigating or responding to allegations of abuse, neglect, or exploitation of a minor. This may include case workers, supervisors, and etc. Sharing CHRI with other states social service employees is PROHIBITED.
   e) CHRI must not be provided to the subject of the record, other adults in the household or children.

   NOTE: Criminal history inquiries should be limited to authorized inquiries only. Never use yourself, the new employee or any other person for training purposes.

3. Notify servicing agency when a DSS employee leaves the agency.
   a) Provide servicing agency with a frequently updated list of employees who can request criminal record information. Any employee who leaves the agency will no longer be able to request criminal history information.

D. Training Coordinator
1. **INDOCTRINATION**

   It is the responsibilities of the agency’s POC to ensure new employees receive appropriate indoctrination training on the proper use, access, and dissemination of CHRI prior to having access to CJI. Indoctrination of an employee should include, but is not limited to the following:


   b) Watch the Security Awareness Training Video and sign the log indicating this has been completed.

   c) Review the DSS Manual.

   **E. Audit Coordinator**

   1. The POC will be the contact person for biennial audits conducted by the SBI. The Compliance Unit will send an email to the POC and Agency Head with the audit packet attached. It is the responsibility of the POC to ensure the appropriate documentation is available for inspection and all paperwork is submitted before the end of the audit cycle.

   2. The POC should be available to work with SBI staff during the audit. If the POC is unavailable during the audit cycle, arrangements should be made for appropriate personnel to assist SBI staff with questions or requests.

   3. Coordinate agency’s response to any non-compliance issues noted in the audit and monitor adherence to resulting policy changes.

**III. Standards and Agreements**

Due to the vast amount of information available through the Division of Criminal Information Network (DCIN), the integrity, confidentiality and proper use of the system is essential. To achieve these desired goals, the SBI has drafted and implemented standards and agreements to be conformed to by all users.

*NOTE: It is the POC’s responsibility to ensure that all agreements in place are kept up-to-date.*

**A. Eligibility for DCIN Access**

1. Eligibility for DCIN access is restricted to agencies authorized by the North Carolina Attorney General’s Office, the National Crime
Information Center and/or the International Justice and Public Safety Information Sharing Network.

B. Legal Agreements for DCIN Access

1. USER AGREEMENT
   a) The head of each agency with access to DCIN & CJI shall sign a User Agreement certifying that he/she has read and understood the agreement and requirements for security of the DCIN system.
   b) The User Agreement outlines managerial control, physical security, system discipline, data collection and storage, and the system access requirements.
   c) The User Agreement is emailed to the agency head and POC of each DSS office accompanied by a cover page with instructions.
   d) The User Agreement shall be signed by the agency head indicating he/she has read and understands the requirements outlined in the agreement. The original signature page must be returned by mail or scanned and emailed to the SBI, Criminal Information and Identification Section (CIIS), Compliance Unit.
   e) After the signature page is reviewed and signed by the SBI, it will be scanned into an electronic file by the Compliance Unit and then emailed back to the agency head and POC.
   f) Agencies must maintain a copy of the signed User Agreement on file and have it available for review during an audit.
   g) The User Agreement must always reflect the current agency head’s name and signature.

2. SERVICING AGREEMENT
   a) Any agency providing indirect access to DCIN to another agency shall enter into a Servicing Agreement with the recipient agency head. Said Servicing Agreement shall cover all services your agency will receive from the servicing agency. Servicing Agreements may be needed or requested for device and/or non-device agencies to provide continuous access to DCIN.
   b) Three originals of each Servicing Agreement shall be disseminated and maintained as follows:
- Original 1 of this agreement shall be forwarded to the SBI/CIIS Compliance Unit for inclusion in the agency file.
- Original 2 shall be maintained by your agency.
- Original 3 shall be maintained by the agency providing service to your agency.

c) Service Agreements will be reviewed during the audit process. A sample Servicing Agreement is located in the forms section of this manual.

**NOTE: Specifications for such an agreement may be found in the Administrative Procedures, Subchapter 4E section .0303.**

### IV. Sources of Criminal Records

The SBI maintains a computerized network (DCIN) linking local, state and national criminal justice agencies for the collection, organization and retrieval of data on crimes and criminals 24 hours a day.

#### A. SBI Criminal/Investigative Records

1. NC Computerized Criminal History File (CCH).
   - a) Criminal records of individuals who have been arrested and the SBI has received a valid criminal fingerprint card; these records are identified with a NC SID Number ending with “A”.
   - b) Historical misdemeanor fingerprint submissions to AFIS, which will provide the identification record only.
     - (1) An AOC inquiry must be performed to obtain the arrest and court data.
     - (2) These records are identified with a NC SID Number ending with “H”.

2. Juvenile Investigative Records
   - a) Juveniles who have been adjudicated delinquent and fingerprinted in accordance with NCGS 7B-2102.
   - b) Only juveniles who were 10 years old or older at the time they allegedly committed the offense that would be a Class A, B, C, D, or E felony if committed by an adult.
   - c) These records are identified with a NC SID Number ending with “J”.
B. **NCIC Interstate Identification Index (III)**

1. National name index for which the FBI has received a valid criminal fingerprint card.

2. Includes:
   a) Criminal records of all persons born in 1956 or later with a FBI record.
   b) Persons born prior to 1956 whose first arrest fingerprint card was submitted to the FBI on July 1, 1974 or later.
   c) Numerous older records converted to the automated system since III was implemented.

3. Includes identification information with an automatic pointer to the state(s) or federal agency housing the computerized record.

4. NC Historical and Juvenile Investigative records are not indexed in III.

C. **International Justice & Public Safety Information Sharing Network (NLETS)**

1. Computer switching center for the exchange of law enforcement and criminal justice information between states and/or Canada.

2. Includes:
   a) Other State Repositories.
      (1) Computerized files maintained at the state level only.
      (2) May include various types of records such as criminal, arrest, etc.
   b) Canadian Police Information Center (CPIC).
      (1) Name index and complete criminal history records for Canada.
      (2) Response(s) may be reviewed by Canadian Police Information Center (CPIC) before being returned to the requestor.

   c) Criminal History Record Information (CHRI) - local agencies in other states and/or Canada.
(1) Records which may or may not be documented by fingerprint cards.

(2) Referred to as criminal history record information (CHRI).

V. Additional Files and Available Information

A. National Crime Information Center – NCIC

Responses from these sources may also include hits from the following NCIC files:


B. North Carolina Only Files

1. NC Sex Offender File

2. NC Concealed Handgun File

3. NC Department of Correction File

VI. Authorized DSS Uses for National/State Records

A. Purpose Code C

1. Used by Governmental Social Service 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.

2. This is the only authorized purpose allowed for DSS agencies.
VII. Access & Dissemination Requirements for CCH/CHRI

A. Access

1. Access is restricted to authorized purposes and only on a need to know basis for DSS personnel.

2. In order to access CCH/CHRI information, each DSS office with an ORI, must utilize and maintain the Criminal History Request Form capturing the requesting agency information, the search being requested and the processing agency information. A copy of the Criminal History Request Form is located in the Forms section of this manual.

3. **Accessing the DCIN for reasons not outlined under Section 151 of the Adam Walsh Child Protection & Safety Act of 2006 could subject the requestor to criminal charges under NC General Statute 14-454.1, Accessing Government Computers.**

B. Dissemination

1. The SBI stores an automated log of all criminal/investigative record inquiries.

2. Automated log will contain the information supplied by the operator in the inquiry transaction.

3. Secondary Dissemination is dissemination to any person outside the initial requesting agency. This must be indicated in the inquiry screen and in the case file pertaining to that record. This field may also be utilized to indicate the purpose of the request or a file number. For example, DSS Investigation, Arrest or list the appropriate DSS case file number.

4. Criminal history record information may be used only by employees of the NC governmental social services agencies when investigating or responding to allegations of abuse, neglect, or exploitation of a minor.

5. Sharing criminal history record information with other state’s social services agencies or their personnel is PROHIBITED.
Definitions

A. **APOC** - Assistant Point of Contact

B. **CCH** – Computerized Criminal History

C. **CHRI** - Criminal History Record Information

D. **CIIS** - Criminal Information and Identification Section. CIIS is the section of the State Bureau of Investigation that operates under the NC Department of Justice. CIIS is responsible for the collection, storage and dissemination of information that will assist criminal justice and law enforcement agencies in the performance of their duties.


F. **CJI** - Criminal Justice Information

G. **CJIS** – Criminal Justice Information System

H. **CPIC** – Canadian Police Information Center

I. **DCIN** – Division of Criminal Information Network. DCIN is the computer system maintained by the SBI/CIIS to provide for the collection, storage and dissemination of information that will assist criminal justice and law enforcement agencies in the performance of their duties.

J. **FBI** - Federal Bureau of Investigation

K. **III** – NCIC Interstate Identification Index

L. **NCAC** – NC Administrative Code

M. **NCIC** – National Crime Information Center. NCIC is a section of the Federal Bureau of Investigation. This agency acts as a national repository for Criminal History Information Indexing and the various Hot Files and Investigative Files entered by local, state and federal law enforcement agencies.

N. **NICS** – National Instant Criminal Background Check System

O. **NLETS** – International Justice & Public Safety Information Sharing Network. NLETS is a criminal justice data communications system that allows device agencies to communicate directly with law enforcement/criminal justice agencies nationwide and in Canada.
P. **ORI** – Originating Routing Identifier. This is the number assigned by NCIC to law enforcement/criminal justice and other approved agencies to identify the agency and type for access to criminal justice information.

Q. **POC** – Point of Contact

R. **SBI** – NC State Bureau of Investigation

S. **SID** – State Identifying numbers which are assigned when valid criminal fingerprint cards are received.
DSS Point of Contact
Training

Forms Section
### Requesting Agency

**Date of Request:** ____________________  
**Requesting Agency:** ___________________________________  **ORI:** ________________________  
**Requested By:** ________________________________________  **Telephone Number:** ____________  
**E-Mail Address:** _______________________________________  **Case Number:** ________________  
**Purpose of Request:** __________________________________________________________________  

**Certification:**  
1. This request is for investigating or responding to reports of child abuse, neglect or exploitation only, and not placement, pursuant to Public Law 109-248, Section 151 ("Adam Walsh Child Protection and Safety Act of 2006").  
2. Dissemination of Criminal History Record Information (CHRI) is governed by statutes, laws and regulations and as the requestor, I will comply with and be subject to the provisions of both state and federal law and regulations, including, but not limited to Public Law 109-248, 12 NCAC 04F .0401 (Dissemination of CCH Records).  
3. I understand this form should be maintained by the Requesting Agency, available for review by state and federal regulating authorities at various times, including state and federal compliance audits.  
4. That information obtained will not be disclosed to the individual that is the subject of the records check.  
5. That I am requesting and will use this information only in my official capacity with my agency.  

**Signature:** ____________________________________________________  **Date:** ____________________________

### Search Requested (Subject of Records Check):

**Last Name**  
**First Name**  
**Middle Name**  
**Suffix**  
**Maiden/Aliases Name**  
**Aliases**  
**Race**  
**Sex**  
**Date of Birth**  
**SSN (optional)**  
**Driver's License Number/State**  
**Place of Birth**  
**Current Address**

**Type of CHRI Search Requested:**  
___ State Only  
___ State and National

### Processing Agency

**Processing Agency:** ____________________________________________  **ORI:** ________________________  
**Processed By:** ______________________________________________  **Telephone Number:** ______________  

**Information Disseminated:**  
___ No Record  
___ Criminal Record Attached

**Based on the Following Identifiers:** (choose all that apply)  
___ Name  ___ Date of Birth  ___ SSN  
___ Race  ___ Sex  ___ Maiden/Aliases

**Certification:**  
1. I have determined that the above request meets state and federal regulations for access and dissemination.  
2. That this request is being made only for investigating or responding to reports of child abuse, neglect or exploitation and not placement, Pursuant to Public Law 109-248, Section 151.  
3. I understand this form should be maintained by the Processing Agency, available for review by state and federal regulating authorities at various times, including state and federal compliance audits.  

**Signature:** ____________________________________________________  **Date:** ____________________________

---

DSS/Criminal Justice Use Only  
April 30, 2014
Sample Servicing Agreement

Between

_________________________________  Servicing Agency Name & ORI

And

_________________________________  Recipient Agency Name & ORI

The purpose of this Servicing Agreement between ___________________ (Servicing Agency) and ___________________ (Recipient Agency) is to enumerate the terms, conditions, duties and responsibilities of each entity regarding records transactions to the North Carolina State Bureau of Investigation Division of Criminal Information (DCI), the International Justice & Public Safety Network (Nlets), and the Department of Motor Vehicles (DMV).

Department of Motor Vehicle Files

A. Responsibilities of Servicing Agency

The Servicing Agency agrees to provide DCI access for DMV Information to the Recipient Agency. This service includes:

1. To disseminate driver history information to authorized Recipient Agency upon receipt of required information.
2. Provide Recipient Agency with a copy of transactions made through the DCI system on behalf of the Recipient Agency (if requested).

B. Responsibilities of Recipient Agency

The Recipient Agency agrees to comply with the following policies and procedures:

1. Only request a driver’s history record pursuant to enforcing laws and ordinances.
2. Only use obtained information for the requested purpose and agrees not to re-disseminate such information for any other purpose.
3. The Recipient Agency shall be held liable for any misuse or unauthorized dissemination of driver history record information obtained by the Servicing Agency and may be subjected to penalties applied by DCI.
4. Acknowledges that it is aware of those regulations of the Division of Criminal Information in Title 12, Chapter 4 of the North Carolina Administrative Code pertaining to driver history records and agrees that it is bound to the current provisions and any subsequent revisions.
Computerized Criminal History Information

A. Responsibilities of Servicing Agency

The Servicing Agency agrees to provide DCI access for Computerized Criminal History Information to the Recipient Agency. This service includes:

1. To disseminate computerized criminal history information to authorized Recipient Agency upon receipt of required information.

2. Provide Recipient Agency with a copy of transactions made through the DCI system on behalf of the Recipient Agency (if requested).

B. Responsibilities of Recipient Agency

The Recipient Agency agrees to comply with the following policies and procedures:

1. Only request a computerized criminal history record pursuant to enforcing laws and ordinances.

2. Only use obtained information for the requested purpose and agrees not to re-disseminate such information for any other purpose.

3. The Recipient Agency shall be held liable for any misuse or unauthorized dissemination of computerized criminal history information obtained by the Servicing Agency and may be subjected to penalties applied by DCI.

4. Acknowledges that it is aware of those regulations of the Division of Criminal Information in Title 12, Chapter 4 of the North Carolina Administrative Code pertaining to computerized criminal history information and agrees that it is bound to the current provisions and any subsequent revisions.
A. Responsibilities of Servicing Agency

The Servicing Agency agrees to provide DCI access for Processing NCIC Record Entries for
the Recipient Agency. This service includes:

1. To enter NCIC Records upon receipt of required information.

2. Provide Recipient Agency with a copy of transactions made through the DCI system on
behalf of the Recipient Agency (if requested).

3. Entering complete and accurate data into the DCI/NCIC files as provided by the recipient
agency.

4. Making all transactions to the DCI system in a timely manner, which means immediately
following receipt of request and all necessary information.

5. Verifying and documenting any NCIC record entries, cancellations, clears, or modifications
made with recipient agency’s ORI number.

6. Providing Hit Confirmation transactions for records entered in NCIC files for recipient
agency as described below:

B. Responsibilities of Recipient Agency

The Recipient Agency agrees to comply with the following policies and procedures:

1. Provide data to the Servicing Agency to be entered into DCI that is complete, accurate and
substantiated by a written report.

2. All requests for transactions to the DCI system should be made immediately after receiving
valid reports.

3. A copy of all record transactions made by the Servicing Agency on behalf of the Recipient
Agency should be verified by the Recipient Agency for accuracy and completeness.

4. NCIC record validations should be performed using the EVOLVE system by the Recipient
Agency. A copy of the validations will be provided to the Servicing Agency after the
validation is performed in order for the Servicing Agency to verify their records and make
any necessary modifications to the NCIC record.

Either agency may terminate this agreement upon determining that an applicable law, rule or
regulation has been violated and/or the terms of this agreement have been violated. It is
further agreed that transactions made to the Division of Criminal Information on behalf of the Recipient Agency are provided as a service and this service may be discontinued by the Servicing Agency if at any time this service becomes a burden due to personnel manpower or computer system availability.

I certify by signing below that I have read and understand the requirements for this agreement, and I will uphold this agreement. This agreement becomes effective on ____________, 20__. In witness whereof the parties hereto have caused to be affixed their signatures and seals by and through officers having authority to bind the agencies party to this agreement, this the _______ day of ____________, 20__.  

<table>
<thead>
<tr>
<th>Servicing Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature of Servicing Agency Head</td>
</tr>
<tr>
<td>Title and Name of Servicing Agency Head</td>
</tr>
<tr>
<td>Sworn to and subscribed before me this _____ day of __________<strong>, 20</strong></td>
</tr>
<tr>
<td>Notary Public</td>
</tr>
<tr>
<td>My Commission Expires:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Recipient Agency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature of Recipient Agency Head</td>
</tr>
<tr>
<td>Title and Name of Recipient Agency Head</td>
</tr>
<tr>
<td>Sworn to and subscribed before me this _____ day of __________<strong>, 20</strong></td>
</tr>
<tr>
<td>Notary Public</td>
</tr>
<tr>
<td>My Commission Expires:</td>
</tr>
</tbody>
</table>
Error Reporting Notice

TAC/POCs must report to the SBI Compliance Unit (by email) errors found during the TAC/POC monthly review of agency CHRI/CCH Logs. Authority: 12 NCAC 04 F .0401, Dissemination of CCH Records (f), (1), (2), (3).

To streamline this process for agencies the following format should be used.

Agency Instructions:

1. Email the Compliance Unit at ARAhelp@ncdoj.gov when errors are found.

2. In the email subject line, enter:
   Error Reporting Notice: <<insert full agency name>>

3. In the body of the email explain in detail the errors that were found. Details should include but are not limited to the following:
   - Agency Name
   - ORI Involved
   - Incident Date
   - Operator/User Involved
   - Explanation of Error
   - Corrective Measures Taken

4. Maintain a copy of the Error Reporting Notice email in agency files. If error is linked to a CCH Log maintain a copy with the appropriate log for the next on-site audit.

Terminology:

CCH  Computerized Criminal History
CHRI  Criminal History Record Information
NCAC  North Carolina Administrative Code
POC  Point of Contact
TAC  Terminal Agency Coordinator
AGENCY INFORMATION CHANGE FORM

CURRENT INFORMATION

Agency Name: _____ County: _____ ORI: NC_____ TID: _____

Type of Agency: _____ Device Agency   _____ Non-Device Agency

Main Phone: _____-_____ - _____    Main Fax: _____ - _____ - _____

Mailing Address: ______ City: _____ Zip: ______

Street Address: ______ City: _____ Zip: ______

Agency Head: _____

Agency Head Email: _____

TAC/POC: ______ Email: _____

ATAC: _____ Email: _____

INFORMATION TO BE CHANGED

Agency Name: _____County: _____

Main Phone: _____-_____ - _____    Main Fax: _____ - _____ - _____

Mailing Address: ______ City: _____ Zip: ______

Street Address: ______ City: _____ Zip: ______

New Agency Head: _____

Agency Head Email: _____

TAC/POC: ______ Email: _____

Submitted By: ______

Date Submitted: _____
Security and Privacy Training
For Non-Certified Users
Table of Contents

Introduction ........................................................................................................................ Page 29
Section I – Rules Regarding Access ........................................................................ Page 30
Section II – Use of Computer Equipment ................................................................. Page 31
Section III – DMV .................................................................................................. Page 32
Section IV – Criminal History Information .............................................................. Page 33
Section V – Other Computerized Information ......................................................... Page 36
Section VI – Violations and Penalties ................................................................... Page 39
Conclusion .............................................................................................................. Page 40
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.

DCIN certified operators, vendors, city/town/county IT personnel will be required to complete security awareness training every two 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 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**:

*LICENSENG /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 which 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.

4. **NC Concealed Handgun Files, NC Sex Offender Files and NC Department of Corrections:**

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 some NCIC records 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 ensure 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.