Wilmington Police Department
Directive: .10.02
DCI and Computerized Records Procedures

CALEA Standards: 41.2.5, 74.1.3, 82.1.7
NCLEA Standards: 8.07

I. Purpose

The purpose of this directive is to define the department's role in ensuring compliance with the North Carolina Division of Criminal Information (DCI) operations and security procedures. This directive also establishes procedures for handling requests, dissemination, and operator certification requirements in accordance with applicable federal and state laws pertaining to the State Bureau of Investigation (SBI) Criminal Information and Identification Section (CIIS) DCI network information and operations, and the Federal Bureau of Investigation (FBI) Criminal Justice Information Service (CJIS) Division information and operations.

II. Definitions

A. Criminal Information and Identification Section (CIIS) – A branch of the North Carolina State Bureau of Investigation that maintains North Carolina's statewide computer network for the exchange of law enforcement/criminal justice information: **Division of Criminal Information Network (DCI/DCIN).**

B. NC Department of Transportation/Division of Motor Vehicles (DMV) - A branch of the NC Government Computerized Files.

C. Criminal History Record Information (CHRI) – SBI is the North Carolina's central repository for CHRI based on fingerprint identification. CHRI information is collected by and maintained in the files of criminal justice agencies concerning individuals, consisting of identifiable descriptions, notations of arrest, detentions, indictments or other formal criminal charges. This includes any disposition, sentencing, correctional supervision, and release information.

D. National Crime Information Center (NCIC) System- A nationwide computerized information system that is operated by the Federal Bureau of Investigation (FBI). The NCIC System can best be described as an index of documented criminal justice information concerning crimes and criminals of nationwide interest and a locator file for missing and unidentified persons.

E. Criminal Justice Information Service (CJIS) – A division of the FBI that maintains data necessary for law enforcement agencies to perform their mission and enforce laws, including biometric information, identity history person, organization, property, and case or incident history data.

F. Interstate Identification Index (III) – National name index of criminal records substantiated by fingerprint cards.

G. **International Justice and Public Safety Network (NLETS) -** Non-profit organization of law enforcement agencies which partner with public safety companies to provide a national computer switching center for the exchange of law enforcement and criminal justice information between states and/or Canada.

H. **National Instant Criminal Background Check System (NICS)** - NICS is the national computer system maintained by the FBI for obtaining information on individuals who may be prohibited from receiving or possessing firearms under federal law.

I. **NIC Number** – A number generated by the National Crime Information Center to identify articles, persons or vehicles entered into the NCIC System or used to query any entry in NCIC.

J. **Originating Agency Case Number (OCA)** – A case number generated by WPD or other agency which is required before any entry can be made into NCIC.

K. **Authorized Requestors and Recipient -** Those persons who are members of The Wilmington Police Department or an Agency with whom we have a current DCI Servicing Agreement.

L. **"Need to Know" -** Applies to purposes of the administration of criminal justice and/or criminal justice agency employment.

M. **"Packing the Record" -** Ensuring an NCIC record is complete and accurate by adding all available information, including supporting documentation, to maximize the likelihood of a successful "hit" (identification).

N. **Hot File -** Files available for entry of stolen property, wanted or missing persons, and files for information on dangerous person or groups.

O. **DCI Terminal** - Applies to any device that is capable of communicating with DCIN.

P. **DCIN User -** A person who has been certified through the DCI certification process.

Q. **Dissemination -** Any transfer of information, whether orally, in writing, or by electronic means.

R. **Hiring Manager –** The person responsible for filling open positions within the department, often serving as a civilian supervisor or commander of a division.

S. **TAC –** Terminal Agency Coordinator.

T. **ATAC –** Assistant Terminal Coordinator.

U. **Vendor –** Organization contracted by a criminal justice agency to provide support or services that involve access to or handling of CJI.

V. **Support Personnel -** Individuals who are authorized to access and use criminal justice information, and who must adhere to strict security protocols and training requirements to protect the confidentiality and integrity of that data.

III. Procedures

A. System Security – Access, Use and Dissemination

1. The Chief, or their designee, will designate an individual, under their direct management and control, as a TAC. The TAC will serve as the point of contact at the User Agency for matters relating to DCIN access and training.

2. The Administrative Services Division Commander, or their designee, is responsible for ensuring that computerized criminal history record equipment in the Administrative Services Division is being operated properly. DCI terminals located outside of the Administrative Services Division shall be the responsibility of the Division Commander where the terminal is assigned.

3. The Administrative Services Division Commander, or their designee, is responsible for maintaining the sensitivity and confidentiality of DCIN information and for safeguarding the devices that access DCIN and CJIS information.

4. The TAC is responsible for:

    a. Ensuring that all state and federal regulations are adhered to, and that the agency is in compliance with all rules and regulations.
    b. Ensuring all criminal history record information is kept in secure locations and is disseminated only for criminal justice purposes.
    c. It is the responsibility of the TAC to notify the CIIS/Compliance Unit of any violations of these rules and regulations at any time they may occur.
    d. The TAC may designate one or more ATAC to assist in the duties of the TAC role.
    e. The TAC shall perform an account validation by reviewing the agency's DCI User list on an annual basis and remove any users that no longer require DCI access. The results of this validation shall remain on file for a period of one year.
    f. The TAC or ATAC will remove users from the agency access list within 24 hours of being notified of the operator's separation or termination from the agency, in accordance with DCI policies and procedures.

5. DCI network users will not share or use another network user's password. In the event a network user forgets their assigned password, the TAC or ATAC should be notified immediately to request a password change or contact.

6. Only DCI certified users are allowed to use DCI terminals (and those in training under the supervision of a certified operator for a maximum of 120-day period).

7. When NCIC/DCI information is requested over the telephone, the NCIC/DCI operator is responsible for ensuring the identity of the person requesting information prior to any information being provided. Authorized criminal justice personnel may obtain NCIC/DCI information only, when necessary, in performing their official law enforcement duties.

8. DCI Users will not broadcast DCI network records information over the police radio unless the information is necessary to protect an officer or citizen from immediate danger. The information may be relayed to the officer in person or via telephone. (Note: Exceptions include the following information pertaining to driving records that may be broadcast over the radio:

    a. Prior, current, or limited revocation or suspension of driving privileges for Driving While Impaired (DWI) and corresponding date(s).
    b. Prior, current or limited revocation or suspension of driving privileges for any other violation and corresponding date(s).
    c. License pick up.

9. All DCIN Users are required to comply with the SBI CIIS DCI Network Personnel Security Agreement and shall abide by all NCIC/DCI operational standards and procedures.

10. Employees are responsible for seeing that DCI printouts in their possession are secured and not accessible to unauthorized persons. Any DCI printouts that are no longer needed shall be destroyed using departmental shredders.

11. Any access of these systems and or dissemination of information obtained for non-criminal justice purposes are considered a misuse of the system.

12. Unauthorized requests, receipt, release, interception, dissemination or discussion of FBI CJIS Data/CHRI could result in criminal prosecution and discipline action as outlined in WPD Directive .04.02 – Employee Discipline.

13. Any application or file that contains CJIS information must be kept out of the view of all visitors.

14. All authorized personnel with access to (physical or logical) Criminal Justice Information (CJI) must receive Security Awareness Training (SAT). This includes vendors and anyone who works on and or maintains a technical component that is used to send, receive, process or route a transaction to or from systems that processes or maintains FBI CJIS data.

    a. This training requirement will be satisfied through use of the CJIS Training Portal.

15. All visitors who have not had a fingerprint-based records check will be escorted while inside the secure portions of the police department.

16. Visitor's Access Log – **WPD-35 Form**

    a. Log will be maintained at the front desk.
    b. All unknown visitors must present government issued photo identification. Exception: Office of the Chief's discretion, Media, City employees wearing city badge or when circumstance prevents visitor from presenting government issued photo identification and identification can be confirmed by another source.
    c. All visitors must be issued temporary visitor passes and escorted while inside the secure portion of the police department.
    d. All visitors must wear, and display Visitor Pass at all times.
    e. Lost/Stolen Visitor Passes will be reported to Front Desk Supervisor immediately and a WPD Loss Report will be filled out by personnel responsible for collection.
    f. Log will include the following information: Date, Visitor Name, Agency, if applicable, ID Used, Phone Number, Purpose of Visit, WPD Employee Visited, Time in/out, Visitor Badge number issued and Desk Personnel's initial who logged in and out visitor.
    g. Front Desk Administrative Support Specialist is responsible for reviewing Visitor's Access Log quarterly. Completed logs will be kept in a file labeled Visitor's Access Log for a minimum of 12 months. Any discrepancies will be forwarded to the Front Desk Administrative Support Supervisor immediately.

17. All Wilmington Police Department employees who have had a fingerprint-based records check may be issued an Identification Badge to access authorized areas within the police facility unescorted.

18. Authorized access areas will be assigned by an employee's title and/or security clearance level. The Administrative Services Division

Commander, or their designee, shall determine which employee titles are authorized access to specific areas.

19. Access to specific or sensitive areas is based on a "need to know" principle, an employee restricted from a limited access area is required to obtain permission from a unit member prior to entry. Unauthorized access may result in disciplinary action.

20. The Administrative Services Division Commander, or their designee, will ensure authorization is removed if an employee is transferred to a section requiring different security access. An employee shall report to the Administrative Services Division Commander, or their designee, to have their identification access card issued with current title and clearance.

21. Prior to entering the facility, all personnel other than sworn uniformed personnel will display their identification access card upon their person and will ensure that it is plainly visible.

22. The Administrative Services Division Commander, or their designee, may grant authorization for City of Wilmington support personnel who have had a fingerprint-based records check to access authorized areas within the police facility unescorted.

    a. All support personnel must sign-in at the front desk and receive a City Employee Visitor's Pass. Exception: *Facility Manager employed by City of Wilmington and assigned to building*.
    b. All access should be restricted once authorized personnel are no longer providing authorized services to the department.
    c. The Administrative Services Division Commander, or their designee, is responsible for destruction of identification.
    d. The Administrative Services Division Commander, or their designee, is responsible for generating and maintaining a list documenting the names of support personnel who are authorized to access the police facility unescorted. The list should be reviewed quarterly.

23. Media Sanitation and Destruction refer to WPD Directive .10.05.

B. Network Diagram/Technical Security

1. The Police Records Supervisor/IT Local Agency Security Officer (LACO) shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status (SOURCE: CJIS Manual). The network topological drawing shall include the following:

a. All communications paths, circuits, and other components used for interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point.

b. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient.

c. "For Official Use Only" (FOUO) markings.

d. The agency name and date (day, month, and year) the drawing was created or updated.

C. NCIC Entries (General Information)

1. NCIC records must be kept accurate and up-to-date. Agencies that enter records in the NCIC System are responsible for their accuracy, timeliness, and completeness. To facilitate compliance with hit confirmation requirements, the originating agency must be available 24 hours a day to confirm its record entries.

2. Any record entered into NCIC files must be documented and maintained on all entries for the entire retention period of the record. All information must be documented by a written report. All information must come from a verifiable source such as:
   a. Victim
   b. Department of Motor Vehicles inquiries
   c. National, state & local criminal record inquiries
      1) e-Warrants
      2) AOC records via DCIN transactions **OR** eCourts searches
      3) Internal, Jail, CAD entries, or CJLeads

3. All DCI/NCIC entries must be complete and accurately reflect the information contained in our Agency's investigative documentation at the point of initial entry (NCIC Policy Manual Section 3.2 -Maintaining the Integrity of NCIC Records). Complete records include all critical information on the person or property at the time of entry. NCIC record "Hot File" should mirror all information in case file. This process must be checked by a second party who will initial and date a copy of the NCIC inquiry printout indicating that accuracy has been determined. The Second Party Check:

   a. Must be completed by an NCIC Specialist certified in modules 1, 2, and 3.
   b. Be someone other than the person that entered the record.
   c. Must correct any inaccurate information.

d. Must be completed every time the record is changed (modified or supplemented).

4. NCIC Specialists will store, within access of their terminals, copies of reports for stolen property/missing persons that are entered into NCIC. NCIC Specialists will also have immediate 24 hours per day access to original felony warrants entered into NCIC. The purpose of such storage will be to perform "hit confirmations" within 10 minutes of "Stolen, Wanted Persons, Missing Persons" inquiries from other agencies via DCI Terminals who may have located a wanted subject or stolen item.

5. Felony Warrants obtained by Wilmington Police Officers will be entered and scanned into the Department Records Management Software for instant retrieval capability. NCIC Specialist may distribute wanted persons information as well as bolo information on missing persons to department personnel via the email marked "Protected". Officers who have taken out a felony warrant may relay the information via email also.

6. DCIN/NCIC information cannot be sent to an officer's MDT. All other warrants and orders for arrest are maintained in eWarrant database, which is accessible to applicable personnel 24 hours a day.

D. Validation

1. In accordance with our DCIN Access Agreement signed by the Chief requires all NCIC records to be complete, accurate, and still outstanding as an active case.

2. Validation procedures will be carried out by, or under the guidance of the Terminal Agency Coordinator (TAC). NCIC is responsible for logging into CJIS Validations System (Evolve) and comparing each record on the monthly validation list with its source documents and supplemental reports.

3. Validation is accomplished by reviewing the entry, current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, nonterminal agency, or other appropriate source or individual. In the event the ORI is unsuccessful in its attempts to contact the victim, complainant, etc., the entering authority must make a determination based on the best information and knowledge available whether or not to retain the entry in the file. Contributors have 30 days from the date of notification to complete their NCIC record validations.

4. Completed validation indicates the following:

   a. Records have been reviewed.

b. Invalid records have been removed.
c. Records that remain are valid and active.
d. Records contain all available and current information.
e. The information is accurate and complete.
f. Entry mirrors record.
g. The validation has been recorded using EVOLVE or a NCIC/DCIN Modify Transaction.
h. WPD Validation Report has been updated. Date, Time, method of contact, who is attempting the contact, and the results of the contact should be notated on this form in accordance with State and Federal regulations.

5. The Federal Bureau of Investigation (FBI) audits National Crime Information Center (NCIC) records every two years. It is the NCIC coordinator's responsibility to ensure that all records entered into NCIC are complete and accurate. This includes the addition of AKAs and numeric identifiers.

E. NCIC Entry Requests

Any request for NCIC entries must be submitted to NCIC Specialist along with the appropriate NCIC entry requirement that coincides with the entry type.

1. **NCIC Wanted Person** – Form WPD-40

a. NCIC policy allows entry of all warrants for arrest (criminal whether felony or misdemeanor).
b. All felony warrants are required to be entered into NCIC per WPD Policy.
c. Warrant entry is the responsibility of the case officer and must take place within three days (72 hours) following receipt of the warrant.
d. Only a District Attorney or an Assistant District Attorney is authorized to approve an out-of-state extradition. A letter from DA's Office must be attached to the NCIC entry.
   1) **Wanted Person Detainer/Extradition –** Extends the retention of the record. NCIC Extradition Liaison will contact DA's Office Extradition Liaison to get confirmation on extradition. If the DA's Office declines to extradite, **and** the "holding agency" performed a "Located", NCIC Extradition Liaison shall "Clear" the entry and Re-"Enter" the record. *Documentation of the cancel and re-entry must be documented in a supplement.*
e. Retention —Indefinitely until located, cleared, or canceled.

2. **Juvenile Secure Custody Order (JSCO) –** Office of Juvenile Justice

   a. Juvenile Secure Custody Order delivered to NCIC Specialist should include the following:
      1) Original Secure Custody Order
      2) Certified Copy
      3) Juvenile Petition
   b. NCIC Specialist are responsible for confirming address for service is within city limits, completing the JSCO Drop Off Sheet, obtaining a new case number, if applicable, entering JSCO into RMS.
   c. Once JSCO is entered into RMS, NCIC Specialist shall scan the front and back of the JSCO and the Petition under the Warrant Module.
   d. NCIC Specialist will send a protected email to Police/Non-Civilian and cc: the WPD Juvenile Social Worker advising of the JSCO.
      1) Subject Line: Protected: Juvenile Secure Custody Order/ (Name of Juvenile)
      2) Information on Juvenile.
      3) Instructions when located and served.
      4) Case number.
      5) OOJ information
   e. Original JSCO, certified copies and petition should be placed in a hot file at the front desk.
   f. The original JSCO will only be released to the officer who takes the individual into custody; copies will be given for attempts.
   g. NCIC Specialist will update record in RMS when an individual is served.
   h. NCIC Specialist will send an email to Police/Non-Civilian, WPD Juvenile Social Worker and OJJ officer that dropped off paperwork once individual is served.
   i. Returned served original JSCO.

3. **NC Blue Alert Notification** – https://nccmp.ncdps.gov/

   a. NCGS § 143B-1023 created the Blue Alert Notification System to provide rapid dissemination of information to the public, media, and law enforcement agencies about a violent person who meets **all three** statutory criteria:
      1) Has killed or inflicted serious bodily injury — as defined in NCGS § 14-32.4(a)—to a law enforcement officer **–AND–**
      2) Poses a threat to the public or other officers **–AND–**
      3) Is at large, whereabouts unknown.

b. **Only the head of a law enforcement agency with investigatory jurisdiction may request a Blue Alert to be issued by the NC Center for Missing Persons.**
c. In addition, the requesting law enforcement agency must perform the following:
    1) Initiate a statewide bulletin "Be On the Look Out" (BOLO) to all law enforcement agencies.
    2) Provide a 24-hour phone number to receive calls during the investigation.
d. The Blue Alert is active for a period of 24-hours. It may be extended for an additional 24-hour period upon agency request and NCCMP review.

4. **NCIC Missing Person –** Supporting Documentation and ONESolution MFR Missing Person/Runaway Report Tab.

    a. Compliance with **NCGS § 143B-1015 and WPD Directive 7.05**
    b. The minimum information required for entry into NCIC is as follows:
        1) Name.
        2) Date of birth (if the reporting party does not have this information, another numeric identifier, such as a social security number, is acceptable for entry).
        3) Physical identifiers: race, height, weight, eye color, and hair color.
        4) Date of the last contact.
        5) Case number (OCA)
    c. Missing persons must be entered into NCIC immediately once the minimum mandatory data is obtained.
        1) Missing persons **under twenty-one (21) must** be entered within **two (2) hours of obtaining the mandatory data.** The time in which the minimum mandatory data is obtained by the initial report taker shall be noted in the missing person report. It shall be the responsibility of the on-duty supervisor to see that this 2-hour time period requirement is met.
        2) Initial report taker shall contact NCIC for entry.
            i. Initial report taker shall note in their missing person report the NCIC Specialist they notified for entry and the method in which they were contacted.
        3) The initial report taker shall ask the reporting party for a current photo and permission to disseminate photo. Must be noted in the ONESolution MFR Missing Person/Runaway Report Tab.
        4) If no photo is unavailable, NCIC may use DMV photo for entry and LEO dissemination only. Noted: When using out of state DMV, check restriction.

d. NCIC Specialist will review the record to ensure minimum mandatory data was obtained and will begin "packing the record" by adding all relevant information to the record, including supporting documentation, to ensure it is as complete and accurate as possible.
e. Once entry NCIC Specialist will immediately inform Public Information Officer (PIO) by phone or email. Attach all missing person's photos (adult and juvenile) to PIO email. Include any pertinent information such as where the image was taken, date the image was taken and if the report person authorized release of the photo. Decisions to use local media and which photos are used will be made by the Public Information Lieutenant, or their designee.
f. Protected email will be sent to Police Non-Civilian and Sting Center with all pertinent information received from initial report taker.
    1) NCIC Specialist shall use SEND transaction with the routing list of MISSPER to initiate a statewide BOLO. Information obtained through DCIN/NCIC will not be included in email to POI or via email to Police Non-Civilian.
    2) NCIC Specialist assigned to Persons Validation shall enter missing persons that are missing longer than 90 days into NAMUS.
    3) Quality Control Notifications received after missing person is on file for 30 days will be forwarded to Sergeant of Violent Crimes for review and a copy placed in Hot File.
    4) NCIC Cross Search Notifications will be reviewed by receiving NCIC Specialist to determine likelihood of match. If a match is likely, forward notification to Sergeant of Violent Crimes. NCIC Specialist determining the likelihood shall note the course of action taken, along with initialing and dating the notification. Notification shall be placed in Hot File.
g. **Missing Persons Alerts -** The investigating officer must notify and obtain approval from the on-duty Watch Commander before submitting a request to activate an alert.
    1) **Amber Alert** – Release of Information Form NC Center for Missing Persons Amber Alert - https://nccmp.ncdps.gov/
        i. Missing juvenile meets the following criteria (N.C. Gen. Stat. § 143B-1021).
    2) **Ashanti Alert** – Release of Information Form NC Center for Missing Persons – Ashanti Alert - https://nccmp.ncdps.gov/
        i. When an adult between eighteen (18) and sixty-four (64) has been identified as a missing individual; **and**
        ii. The adult is missing under circumstances that indicate the physical safety of the missing adult may be endangered; **or**

iii. The disappearance of the missing adult may not have been voluntary, including abduction or kidnapping.

3) **Missing Endangered Alert** - Release of Information Form NC Center for Missing Persons – Missing Endangered Alert - https://nccmp.ncdps.gov/
   i. The person has been reported missing to law enforcement within seventy-two (72) hours.
   ii. The person is believed to be suffering from dementia, Alzheimer's disease, or a cognitive impairment (not medical) that requires the person or child to be protected from potential abuse, physical harm, neglect, or exploitation.
4) NCIC Specialist shall print off NCCMP activation response and place it in "Hot File".
5) Retention – Indefinitely until cleared or canceled.

5. **NCIC Unidentified Persons –** Supporting documentation.

6. **NCIC Gang File –** Supporting documentation and Form WPD - 108.

7. **NCIC Violent Person –** Supporting documentation and Form WPD-70.
   a. The purpose of this file is to:
      1) Alert law enforcement officers when they encounter a person with a violent criminal history or who has previously threatened law enforcement.
      2) Enhance officer safety.
   b. Entry should be made into the VPF when at least one of the following criteria is met:
      1) Convicted offender for assault or murder/homicide of a law enforcement officer, fleeing or resisting arrest, or any such statute which involves violence against law enforcement.
      2) Convicted offender for a violent offense against a person to include homicide and attempted homicide.
      3) Convicted offender for a violent offense against a person where a firearm or weapon was used.
      4) An individual who expressed his or her intent to commit an act of unlawful violence against a member of the law enforcement or criminal justice community, and the law enforcement agency, based on its official investigatory duties, reasonably believes that threat to be serious and documents its reasons.
   c. Retention — Indefinitely until cancelled.

8. **NCIC Identify Theft –** Supporting documentation and Identity Theft File Consent Document Waiver https://www.ncsbi.gov/

a. Documentation for entry must meet the following criteria before an entry can be made.
   1) Someone is using a means of identification of the victim as any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual.
   2) The identity of the victim is being used without the victim's permission.
   3) The victim's identity is being used or intended to be used to commit unlawful activity.
   4) The victim must sign a consent waiver prior to the information being entered.
b. Retention — 5 years from the date of entry or until the Date of Purge (DOP) is equal to the current date.

9. **NCIC Vehicle Entry –** Supporting documentation.
   a. **Stolen Entry**
      1) NC DMV Enforcement receives a copy of all NC Stolen Vehicle entries and requests that the current owner's name/address be placed in Miscellaneous Field.
      2) Rental Property – Equipment/Vehicles (if a signature was obtained)
      3) The investigating officer shall get the approval of a detective and/or supervisor prior to submitting the incident report to NCIC for entry and must be noted in case file.
      4) If determination is made that vehicle is not stolen, after entry has been made, it is the investigating officer's responsibility to notify NCIC and submit a supplement for removal.
      5) The investigating officer shall notify NCIC if entry should be flagged with caution indicators.
      6) The investigating officer shall notify NCIC if vehicle should be held for Latent Prints.
      7) **Retention** - Year of entry plus 4 years; records not containing VIN/OAN only 90 days.
         Note: Stolen Vehicle entries shall be emailed to the Sting Center for Daily Information Report in a protected email. Sting Center personnel shall follow all CJIS requirements related to NCIC information.
   b. **Felony Entry -** Supporting documentation and Form WPD-31, if applicable.
      1. Vehicle, which is not stolen, is used in the commission of a felony, and its whereabouts are unknown that can be identified by License Plate or VIN.
      2. Seizure entries under G.S. 20-28.3
         1. The "Seizing Officer" shall submit an AOC-CR-323B Form - **Officer's Affidavit for Seizure and Impoundment and**

Magistrate's Order - Felony Speeding to Elude if vehicle has not yet been seized to NCIC.

3. NCIC Specialist is responsible for entering the vehicle into Felony Vehicle file.
4. A copy of the Order shall be retained at the front desk.
5. Order is only valid in North Carolina. If seizure is made outside New Hanover County, NCIC will notify the recovering county that the vehicle needs to be towed pursuant to G.S. 20-28.3 (c). Copy of Order will be sent to agency, and supplement will be completed by NCIC Specialist.
6. "Seizing Officer" is responsible for communicating to NCIC if an Order is no longer valid.
7. NCIC Specialist shall confirm with "Seizing Officer" every 90 days, before vehicle file purges, if vehicle shall remain in NCIC. If "Seizing Officer" request the vehicle to remain in NCIC, it shall be reentered into NCIC and documented. If "Seizing Officer" request the vehicle to purge, NCIC Specialist shall document the request and allow the vehicle to purge.
8. Retention – 90 days.

c. **Stolen License Plates** – Supporting documentation.
   1) License plate which has been removed and stolen separately from a vehicle.
   2) Lost license plates will not be entered into NCIC. Owner will be instructed to contact DMV to report the lost tag.
   3) **Retention** – Year of entry plus 4 years.

d. **Stolen Parts**- Supporting documentation.
   1) Any serially numbered component that has been stolen from a vehicle or boat and ownership documentation for a vehicle or boat.
   2) **Retention** – Year of entry plus 4 years.

e. **Recovered Vehicle**– Supporting Documentation.
   1) DCIN file for vehicle in the possession of Wilmington Police Department that is not reported stolen, and the owner is unknown/cannot be contacted.
   2) This file is NOT for a stolen vehicle that has been recovered.
   3) **Retention** – Year of entry plus 4 years.

f. **Stolen Boats** – Supporting documentation.
   1) A vessel for transport by water, constructed to provide buoyancy by excluding water and shaped to give stability and permit propulsion; must have registration, owner applied, or hull number; examples include jet skis, canoes, sail boats, etc.
   2) **Retention** – Year of entry plus 4 years.

10. **NCIC Guns-** Supporting documentation.

a. Any weapon that is designed to or may be readily converted to expel a projectile by air, carbon dioxide, or the action of an explosive, e.g. pistols, rifles, shotguns, etc. (BB guns and paintball guns are excluded and may be entered into the Article File).
b. All gun entries must contain serial numbers.
    1) Do not use model number, stock number, or owner applied number as the serial number.
    2) If more than one serial number appears on the gun, use the frame number as the serial number.
c. **Stolen Gun**
    1) Serially numbered weapon.
    2) **Retention** — Indefinitely until action is taken to clear or canceled.
d. **Lost Entry**
    1) Serially numbered lost or missing weapon.
    2) **Retention** — Indefinitely until action is taken to clear or canceled.
e. **Recovered Entry**
    1) Serially numbered weapon (abandoned, seized, or found) for which no stolen or lost gun report exists and must be in possession of entering agency or readily available for examination.
    2) If entering agency loses custody, record must be canceled.
    3) Investigating officer shall submit an incident report to NCIC for submission.
    4) Property Section shall notify and submit a supplement to NCIC if ownership is determined and weapon needs to be removed from NCIC.
    5) **Retention** — Remainder of year entered plus 2 years.
f. **Felony Gun Entry**
    1) Serially numbered weapon believed to have been used in the commission of a felony and the location of the weapon is unknown.
    2) **Retention** — Indefinitely until action is taken to clear or canceled.
g. Stolen/Lost/Recovered Weapons entries shall be emailed to the Sting Center for Daily Information Report in a protected email. Sting Center personnel shall follow all CJIS requirements related to NCIC information.

11. **NCIC Articles Entry** –
    a. Stolen property identified by unique serial number and/or owner applied number.
        1) OLN and SSN will not be entered into NCIC UNLESS instructed by investigating officer due to public safety.

b. Must use unique serial number or owner applied number. If available, enter both serial number and owner applied number.
c. **Retention** — Year of entry plus 1 year with some exceptions.

12. **NCIC Stolen Securities**
    a. Securities have actual financial value and are printed with serial numbers and the name of the issuer. Securities can be:
        1) Currency — Federal Reserve Notes, Silver Certificates, U.S. Notes, Canadian Notes, and other foreign currency.
        2) Documents or certificates that are generally considered to be evidence of debt — Treasury-issued bills, bonds, and notes.
        3) Municipal and corporate bonds
        4) Debentures (company-issued long-term bond or unsecured loan) and other non-personal notes)
        5) Ownership of property — common or preferred stock **excluding vehicle or boat ownership documents**.
        6) Documents which represent subscription rights (stock warrants, stock rights) and other types traded in securities exchanges in the United States, except for commodities futures.
        7) Postal and other types of money orders, traveler's checks, warehouse receipts, savings certificates, and interest coupons on stocks and bonds.
    b. **Do not enter** into any NCIC file: personal notes (IOUs), bank drafts, cashier's checks, bank officer's checks, certified checks, personal checks, company checks, U.S. Treasury checks, other types of government checks, lost or stolen credit cards, gold or silver coins, and savings or checking account passbooks.
    c. Type of Security (TYP) is a required field for entry. However, cases of kidnapping, ransomware, human trafficking may involve securities. For example, the use of "bait money" for enticement or exploitation, or in cases of counterfeit.
    d. **Retention** — Year of entry plus 4 years for stolen, embezzled, or counterfeited securities' records.
        1) Traveler's checks and money orders are retained for the balance of the year of entry plus 2 years. Example: Stolen traveler's checks entered October 15, 2023 would be retained until December 31, 2025 and then would be retired (purged from NCIC).
        2) Entry of **R-Ransom** in RMI Field results in unlimited retention period.

13. **Criminal History (CCH) Request** – WPD-5 and Waiver, if applicable
    a. Provides an index of subjects matching inquiry and includes information regarding where the record is maintained. A positive

response contains additional identifying data to associate the record with the person of the inquiry (height, weight, race, fingerprint classification, tattoos, etc.). With this information, an agency can decide whether to request the record.

b. Form WPD-5 must be completed by a requestor and kept on file for each inquiry made into CCH for one (1) year.
c. If requestor is unable to complete Form WPD-5, NCIC Specialist may receive the information from the requestor and complete the form for them. The NCIC Specialist will note on the WPD-5 the way the information was received. i.e. phone, MCT, radio, etc.
    1) Exemption: Any requestor receiving a hard copy and/or electronic copy of a CCH MUST physically sign Form WPD-5.
d. It is the responsibility of the Terminal Operator:
    1) To determine specific reason for the request.
    2) Choose appropriate transactions and purpose code for the given reason.
    3) Indicate if a secondary dissemination will be made.
    4) Report any errors, misuse, or possible violations to the TAC immediately and document on WPD-5.
e. Waivers must be attached to Form WPD-5 for all CCH Requests that is requested for a reason other than "criminal". i.e. Application, ride-a-longs, interns, defense class, etc.

F. Miscellaneous Information

1. When "Packing the Record" for entry into the Persons File, NCIC Specialist should use many identifiers as available from the following resources: RMS, P2P, Department of Corrections, NC Department of Motor Vehicles, Criminal History Report, CJLeads, and eCourts.

2. The "Hot File" must contain complete information and be available to be reviewed at all times.

3. NCIC Specialists shall follow the established DCI procedures which they have been trained to perform. Any action that requires the NCIC Specialist to perform an action should be documented.

4. The increase in the amount of information available through NCIC files has tremendously increased. All positive responses must be read carefully, and data compared to determine if the person in the NCIC response and the person encountered by the officer are the same.

5. Any officer who receives a positive response to an NCIC inquiry must confirm the "hit" before taking any action such as arresting the wanted person, detaining a missing person, or seizing the stolen property. Confirming a hit means to contact the agency whose ORI

appears on the record to ensure that the person or property inquired upon is identical to the person or property identified in the record, ensure that the warrant, missing person or theft report is still outstanding, and to obtain a decision regarding the extradition of the wanted person, information regarding the return of the missing person, information regarding the return of stolen property to the rightful owner.

6. A record may be modified as long as the record is in active status. Once an entry has been cleared from NCIC, a verification of the clear shall be performed and printed as part of the case file. A query of the NIC number through the appropriate form shall be completed to verify there is "no record" for that NIC number.

7. All Quality Control and Serious Error messages received by a DCIN User shall be printed out and/or forwarded to the TAC or ATAC for review.

G. NICS

1. Access to NICS Indices is restricted to personnel certified in Modules 1, 2 & 7.

2. The use of NICS for any other purpose is strictly prohibited. Misuse may result in administrative sanctions, suspension, or termination of NICS access, fines up to $10,000, and/or criminal charges being filed by the FBI.

3. NICS Purpose IDs for returning firearms to owners:
   a. Return of a **Handgun** — Purpose ID **Code 22**
      A Handgun is a firearm such as a revolver or pistol designed to be held and fired with one hand.
   b. Return of a **Long Gun** — Purpose ID **Code 23**
      A long gun is a shoulder weapon such as a rifle or shotgun with a barrel length of at least 16 inches.
   c. Return of **Other** — Purpose ID **Code 24**
      For example, a frame or receiver from a firearm.

4. Prior to returning a firearm to the owner or transferee, a Query Disposition of Firearms – (QDOF) will be completed to determine eligibility to receive or possess a firearm.

5. Property & Evidence Division is responsible for verifying the descriptive information provided by the owner or transferee with a government-issued photo identification and submitting the required information on a Firearm Disposition (NICS) Request – Form WPD-80 to a NCIC Specialist. Required information includes Requester 's Name, OCA#, Name of Owner/Transferee, Race/Sex, Date of Birth, SS#, Type of Firearm, Citizenship status, and State of Residence. If

Owner/Transferee is Non-US Citizen, the Country of Citizenship, Place of Birth, and Miscellaneous Number are required for inquiry and a mandatory - Supplemental Questions for Non-US Citizens form.

6. Form WPD-80 must be completed by a requestor and kept on file for each inquiry made into QDOF for one (1) year.

7. The NCIC Specialist shall follow the established DCI procedures which they have been trained to perform. The full NICS Specific Record will be sent to the Property & Evidence Division for review.

8. In compliance with federal law, the Property & Evidence Division will query eCourts for any court records prior to return of firearms.

9. QDOF response from NICS will include a NICS Transaction Number (NTN). The NTN must be used in any subsequent transactions (record retrieval, denial notification, etc.). Both the NTN and the OCA will be utilized for auditing purposes by NICS. The identifiers should be maintained with the agency's case file. Both identifiers will be displayed on the automated NICS Log.

10. If the individual is prohibited from receiving or possessing a firearm due to state or federal prohibitor(s), the Property & Evidence Division shall notify the TAC or ATAC. The TAC or ATAC is responsible for performing the Enter State Denial Notification (NDN) transaction. If the agency should need to overturn the denial, NICS will be contacted by using the State Denial Overturned Message (NDO) transaction.

11. Copies of all NICS Indices transactions should be printed and maintained in the related file for future reference.

12. **Denial Notification**
    a. In accordance with the NICS Denial Notification Act (NDNA), firearms background check Denial Notifications FBI NICS ($.H. NDN) received through DCIN/NCIC will be converted into PDF and forwarded to the Gun Task Force Unit by the NCIC Specialist receiving the notification. A review of the notification will occur by the Gun Task Force Unit to determine if follow-up is necessary. NCIC Specialist will place their initials and date on the $.H. and file denial in filing cabinet under the corresponding month and year received.
    b. Denial notifications will be held for two (2) years.

13. **NICS U21 Notification**
    a. In accordance with the Bipartisan Safer Communities Act (BSCA), if a person under the age 21 attempts to purchase a firearm from a Federal Firearms Licensee and provides an address within our jurisdiction a NICS U21 Notification ($.H.U21) will be received

through DCIN/NCIC. The NCIC Specialist receiving the $.H.U21 message shall place the notification in the Record Supervisor's box. It will be the decision of the agency and Record Supervisor whether to disclose juvenile information.

H. Record Review by Public

1. Review of Record—An individual requesting to review their DCI, SBI, or FBI criminal history record will be referred to an SBI district office or the SBI/Identification Division for such review. The SBI/Identification Division has adopted administrative procedures for such review. The procedures include the subject being fingerprinted and completing an "Application for Right to Review".

I. Access to Computerized Criminal History by a Defense Attorney

1. A defense attorney requesting CCH or driver's history from the department must submit the form signed by a District or Assistant District Attorney in the prosecutorial district where the case is to be tried. The form shall be completely filled out in order to perform the records check.