12 NCAC 04H .0102 is adopted with changes as published in 28:10 NCR 1008 as follows:

SUBCHAPTER 4H – ORGANIZATIONAL FUNCTIONS AND DEFINITIONS

SECTION .0100 – GENERAL PROVISIONS

12 NCAC 04H .0101 SCOPE

(a) The rules in this Chapter are the rules of the North Carolina State Bureau of Investigation, Division of Criminal Information (DCI).

(b) The FBI Criminal Justice Information Services (CJIS) Security Policy is incorporated by reference herein and shall automatically include any later amendments or editions that may be published by the FBI. The policy is available at no charge on the FBI website: ~~http://www.fbi.gov.~~ http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014

12 NCAC 04H .0102 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0102 DEFINITIONS

As used in this Chapter:

(1) "ACIIS" means Canada's Automated Criminal Intelligence and Information System.

(2) "Administration of ~~Criminal Justice~~ criminal justice" means the:

(a) detection of accused persons or criminal offenders;

(b) apprehension of accused persons or criminal offenders;

(c) detention of accused persons or criminal offenders;

(d) pretrial release of accused persons or criminal offenders;

(e) post-trial release of accused persons or criminal offenders;

(f) prosecution of accused persons or criminal offenders;

(g) adjudication of accused persons or criminal offenders;

(h) correctional supervision of accused persons or criminal offenders;

(i) rehabilitation of accused persons or criminal offenders;

(j) collection of criminal history record information;

(k) storage of criminal history record information;

(l) dissemination of criminal history record information;

(m) screening of persons for the purpose of criminal justice employment; or

(n) administration of crime prevention programs to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or safe house programs) and the result of such checks will not be disseminated outside the law enforcement agency.

(3) "Advanced ~~Authentication~~ authentication" means an alternative method of verifying the identity of a computer system user. Examples include software tokens, hardware tokens, and biometric systems. These alternative methods are used in conjunction with traditional methods of verifying identity such as user names and passwords.

(4) "AOC" means the North Carolina Administrative Office of the Courts.

(5) "Authorized ~~Recipient~~ recipient" means any person or organization who is authorized to receive state and national criminal justice information by virtue of being:

(a) a member of a law enforcement/criminal justice agency approved pursuant to Rule .0201 of this Subchapter; or

(b) a non-criminal justice agency authorized pursuant to local ordinance or a state or federal law.

(6) "CCH" means computerized criminal history record information. CCH can be obtained through DCIN or through N-DEx.

(7) "Certification" means documentation provided by CIIS showing that a person has been trained in the abilities of DCIN devices, and has knowledge for accessing those programs that are developed and administered by CIIS for local law enforcement and criminal justice agencies.

(8) "CHRI" means ~~Criminal History Record Information.~~ criminal history record information. CHRI is information 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. ~~This term does not include identification information such as fingerprint records or other biometric data to the extent that such information does not indicate formal involvement of the individual in the criminal justice system.~~

(9) "CIIS" means Criminal Information and Identification Section. CIIS is a section of DCI that manages all CJIS programs within North Carolina, including DCIN.

(10) "CJI" means ~~Criminal Justice Information.~~ criminal justice information. CJI is all of the FBI CJIS provided 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. In addition, CJI refers to FBI CJIS provided data necessary for civil agencies to perform their mission including data used to make hiring decisions.

(11) "CJIS" means Criminal Justice Information Services. CJIS is the FBI division responsible for the collection, warehousing, and dissemination of relevant criminal justice information to the FBI and law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

(12) "CJIS Security Policy" means a document published by the FBI CJIS Information Security Officer that provides criminal justice and non-criminal justice agencies with a ~~minimum~~ set of security requirements for the access to FBI CJIS systems to protect and safeguard criminal justice information whether in transit or at rest.

(13) "Class B ~~Misdemeanor~~ misdemeanor" ~~means an act committed or omitted in violation of any common law, criminal statute, or criminal traffic code of this state that is classified as a Class B Misdemeanor as set forth in the Class B Misdemeanor Manual as published by the North Carolina Department of Justice which is hereby incorporated by reference and shall automatically include any later amendments and editions of the incorporated material as provided by G.S. 150B-21.6. "Class B Misdemeanor" also~~ includes any act committed or omitted in violation of any common law, duly enacted ordinance, criminal statute, or criminal traffic code of any jurisdiction other than North Carolina, either civil or military, for which the maximum punishment allowable for the designated offense under the laws, statutes, or ordinances of the jurisdiction in which the offense occurred includes imprisonment for a term of more than six months but not more than two years. Specifically excluded ~~from this grouping of "Class B Misdemeanor" criminal offenses for jurisdictions other than North Carolina,~~ are motor vehicle or traffic offenses designated as being misdemeanors under the laws of ~~other jurisdictions~~jurisdictions other than the State of North Carolina with the following exceptions: ~~Class B Misdemeanor does expressly include,~~ either first or subsequent offenses of driving while impaired if the maximum allowable punishment is for a term of more than six months but not more than two years, and driving while license permanently revoked or permanently suspended ~~and those~~

~~traffic offenses occurring in other jurisdictions which are comparable to the traffic offenses specifically listed in the Class B Misdemeanor Manual~~. "Class B Misdemeanor" shall also include acts committed or omitted in North Carolina prior to October 1, 1994 in violation of any common law, duly enacted ordinance, criminal statute, or criminal traffic code of this state for which the maximum punishment allowable for the designated offense included imprisonment for a term of more than six months but not more than two years.

(14) "Convicted" or "conviction" means, for purposes of DCIN user certification, the entry of:

(a) a plea of guilty;

(b) a verdict or finding of guilt by a jury, judge, magistrate, or other adjudicating body, tribunal, or official, either civilian or military; or

(c) a plea of no contest, nolo contendere, or the equivalent.

(15) "Criminal ~~Justice Agency~~ justice agency" means the courts, a government agency, or any subunit thereof which performs the administration of criminal justice pursuant to statute or executive order and which allocates more than 50 percent of its annual budget to the administration of criminal justice. State and federal Inspector General Offices are included in this definition.

(16) "Criminal ~~Justice Board~~ justice board" means a board composed of heads of law enforcement or criminal justice agencies that have management control over a communications center.

(17) "CSA" means CJIS System Agency. The CSA is a state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice agency users with respect to the CJIS data from various systems managed by the FBI. In North Carolina, the CSA is the SBI.

(18) "CSO" means CJIS System Officer. The CSO an individual located within the CSA responsible for the administration of the CJIS network on behalf of the CSA. In North Carolina, the CSO is employed by the SBI.

(19) "DCI" means the Division of Criminal Information. DCI is the agency established by the Attorney General of North Carolina in accordance with Article 3 of Chapter 114 of the North Carolina General Statutes. The North Carolina State Bureau of Investigation's Criminal Information and Identification Section is a part of DCI.

(20) "DCIN" means the Division of Criminal Information Network. DCIN is the computer network used to collect, maintain, correlate, and disseminate information collected by CIIS under Article 3 of Chapter 114 of the North Carolina General Statutes. DCIN also provides access to information collected by other ~~Federal, State,~~ federal, state, and local entities necessary for the administration of criminal justice.

(21) "DCIN ~~User~~ user" means a person who has been certified through the DCIN certification process.

(22) "Device" means an electronic instrument used by a DCIN user to accomplish message switching, DMV inquiries, functional messages, or DCIN, NCIC, Nlets on-line file transactions.

(23) "Direct ~~Access~~ access" means having the authority to:

(a) access systems managed by the FBI CJIS Division, whether by manual or automated means, not requiring the assistance of, or intervention by, any other party; or

(b) query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

(24) "Disposition" means information on any action that results in termination or indeterminate suspension of the prosecution of a criminal charge.

(25) "Dissemination" means any transfer of information, whether orally, in writing, or by electronic means.

(26) "DMV" means the North Carolina Division of Motor Vehicles.

(27) "DMV ~~Information~~ information" includes vehicle description and registration information, and information maintained on individuals to include name, address, date of birth, license number, license issuance and expiration, control number issuance, and moving vehicle violation or convictions.

(28) "DOC" means North Carolina Department of Adult Correction.

(29) "End ~~User Interface~~ user interface" means software that is utilized by a certified user to connect to DCIN and perform message or file transactions.

(30) "Expunge" means to remove criminal history record information from the DCIN and FBI computerized criminal history and identification files pursuant to state statute.

(31) "FBI" means the Federal Bureau of Investigation.

(32) "FFL" means ~~Federal Firearm Licensee.~~ federal firearm licensee. A FFL is any individual, corporation, company, association, firm, partnership, society, or joint stock company that has been licensed by the federal government to engage in the business of importing, manufacturing, or dealing in firearms or ammunition in accordance with 18 USC § 923.

(33) "III" means Interstate Identification Index. III is the FBI CJIS service that manages automated submission and requests for criminal history record ~~information that is warehoused subsequent to the submission of fingerprint information.~~ information.

(34) "Inappropriate ~~Message~~ message" means any message that is not related to the administration of criminal justice.

(35) "Incident ~~Based Reporting~~ based reporting" or "I-Base" is a system used to collect criminal offense and arrest information for each criminal offense reported.

(36) "INTERPOL" means International Criminal Police Organization.

(37) "N-DEx" means Law Enforcement National Data Exchange. N-DEx is the repository of criminal justice records, available in a secure online environment, managed by the FBI Criminal Justice Information Services (CJIS) Division. N-DEx is available to criminal justice agencies throughout North Carolina, and its use is governed by federal regulations.

(38) "NCIC" means National Crime Information Center. NCIC is an information system maintained by the FBI that stores criminal justice information which can be queried by ~~Federal,~~ federal, state, and local law enforcement and other criminal justice agencies.

(39) "NFF" means the National Fingerprint File. NFF is an FBI maintained enhancement to the Interstate Identification Index whereby only a single fingerprint card is submitted per state to the FBI for each offender at the national level.

(40) "Need-to-know" means for purposes of the administration of criminal justice, for purposes of criminal justice agency employment, or for some other purpose permitted by local ordinance, state statute, or federal regulation.

(41) "NICS" means the National Instant Criminal Background Check System. NICS is the system mandated by the Brady Handgun Violence Protection Act of 1993 that is used by ~~Federal Firearms Licensees (FFLs)~~ FFLs to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922(g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer's criminal history. In North Carolina, NICS is used by sheriff's offices throughout the state to assist in determining an individual's eligibility for either a permit to purchase a firearm or a concealed handgun permit.

(42) "Nlets" means the International Justice and Public Safety Network.

(43) "~~Non-Criminal Justice Agency~~ Non-criminal justice agency" or "NCJA" means any agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may need to process criminal justice information. A NCJA may be public or private. An example is a 911 communications center that performs dispatching functions for a criminal justice agency (government), a bank needing access to criminal justice information for hiring purposes (private), or a county school board that uses criminal history record information to assist in employee hiring decisions (public).

(44) "~~Non-Criminal Justice Information~~ Non-criminal justice information" means any information or message that does not directly pertain to the necessary operation of a law enforcement or criminal justice agency. Examples of messages that are non-criminal justice ~~include, but are not limited to:~~ include:

(a) accessing any DMV file for:

(i) political purposes;

(ii) vehicle repossession purposes; and

(iii) to obtain information on an estranged spouse or romantic interest;

(b) a message to confirm meal plans;

(c) a message to have a conversation; and

(d) a message to send well wishes during a holiday or birthday.

(45) "Official ~~Record Holder~~ record holder" means the agency that maintains the master documentation and all investigative supplements of a restricted file entry or unrestricted file entry.

(46) "Ordinance" means a rule or law promulgated by a governmental authority including one adopted and enforced by a municipality or other local authority.

(47) "ORI" means Originating Agency Identifier, which is a unique alpha numeric identifier assigned by NCIC to each authorized criminal justice and non-criminal justice agency, identifying that agency in all computer transactions.

(48) "Private ~~Contractor~~ contractor" means any non-governmental non-criminal justice agency that has contracted with a government agency to provide services necessary to the administration of criminal justice.

(49) "Re-certification" means renewal of a user's initial certification every two years.

(50) "Restricted ~~Files~~ files" means those files maintained by NCIC that are protected as criminal history record information (CHRI), which is consistent with Title 28, Part 20 of the United States Code of Federal Regulations (CFR). Restricted files consist of:

(a) Gang Files;

(b) Known or Appropriately Suspected Terrorist (KST) Files;

(c) Supervised Release File;

(d) Immigration Violator Files;

(e) National Sex Offender Registry Files;

(f) Historical Protection Order Files of the NCIC;

(g) Identity Theft Files;

(i) Protective Interest File; and

(j) Person With Information (PWI) data within the Missing Person File.

(51) "Right-to-review" means the right of an individual to inspect his or her own criminal history record information.

(52) "SAFIS" means Statewide Automated Fingerprint Identification System. SAFIS is a computer-based system for reading, encoding, matching, storing, and retrieving fingerprint minutiae and images.

(53) "SBI" means the North Carolina State Bureau of Investigation.

(54) "Secondary ~~Dissemination~~ dissemination" means the transfer of CCH/CHRI information to anyone legally entitled to receive such information that is outside the initial user agency.

(55) "SEND message" means messages that may be used by DCIN certified users to exchange official information of an administrative nature between in-state law enforcement/criminal justice agencies and out-of-state agencies by means of Nlets.

(56) "Servicing ~~Agreement~~ agreement" means an agreement between a terminal agency and a non-terminal agency to provide DCIN terminal services.

(57) "State" means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico and any territory or possession of the United States.

~~(58) "State Automated Fingerprint Identification System" or "SAFIS" means a computer-based system for reading, encoding, matching, storage and retrieval of fingerprint minutiae and images.~~

~~(59)~~(58) "Statute" means a law enacted by a state's legislative branch of government.

~~(60)~~(59) “TAC” means Terminal Agency Coordinator. A TAC is an individual who serves as a point of contact at a local agency in matters relating to DCIN or CJIS information systems. A TAC administers CJIS and CIIS system programs within the local agency and oversees the agency’s compliance with both CIIS rules and CJIS system policies.

~~(61)~~(60) "Terminal ~~Agency~~ agency" means any agency that has a device under its management and control that is capable of communicating with DCIN.

~~(62)~~(61) “Training ~~Module~~ module” means a manual containing guidelines for users on the operation of DCIN and providing explanations as to what information may be accessed through DCIN.

~~(63)~~(62) "UCR" means the Uniform Crime Reporting program whose purpose it is to collect a summary of criminal offense and arrest information.

~~(64)~~(63) “Unrestricted ~~Files~~ files” means those files that are maintained by NCIC that are not considered “Restricted Files.”

~~(65)~~(64) "User ~~Agreement~~ agreement" means an agreement between a terminal agency and CIIS whereby the agency agrees to comply with all CIIS rules.

~~(66)~~(65) "User ~~Identifier~~ identifier" means a unique identifier assigned by an agency’s Terminal Agency Coordinator to all certified DCIN users that is used for gaining access to DCIN and for ~~the identification of~~ identifying certified users.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0103 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0103 FUNCTION OF DCIN

~~(a) DCIN provides linkage with the following computer systems:~~

~~(1) National Crime Information Center (NCIC);~~

~~(2) International Justice and Public Safety Network (Nlets);~~

~~(3) North Carolina Division of Motor Vehicles (DMV);~~

~~(4) North Carolina Department of Adult Correction (DOC);~~

~~(5) North Carolina Administrative Office of the Courts (AOC);~~

~~(6) National Instant Criminal Background Check Service (NICS);~~

~~(7) Canada's Automated Criminal Intelligence and Information System (ACIIS); and~~

~~(8) International Criminal Police Organization (INTERPOL)~~

~~(b)~~ Users of DCIN may:

(1) transmit or receive any criminal justice related message to or from any device connected to DCIN;

(2) enter into or retrieve information from North Carolina's:

(A) recovered vehicle file;

(B) sex offender registry; and

(C) concealed handgun permit file

(3) enter into or retrieve information from DCIN user certification and class enrollment files;

(4) enter into or retrieve information from NCIC's restricted and unrestricted files;

(5) access NCIC's criminal history ~~data referred to as the Interstate Identification Index (III);~~ data;

(6) obtain, on a need-to-know basis, the criminal record of an individual by inquiring into the state Computerized Criminal History (CCH) file maintained by CIIS, or CCH files maintained by other states and the Federal Bureau of Investigation (FBI) through III;

(7) communicate with devices in other states through Nlets with the capability to exchange automobile registration information, driver's license information, criminal history record information, corrections information, and other law enforcement related information;

(8) obtain information on North Carolina automobile registration, driver's license information and driver's history by accessing DMV maintained files;

(9) obtain registration information on all North Carolina registered boats, and inquire about aircraft registration and aircraft tracking;

(10) obtain information on those individuals under the custody or supervision of DOC; and

(11) access, enter, and modify information contained within the National Instant Criminal Background Check System (NICS).

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0201 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0200 – REQUIREMENTS FOR ACCESS

12 NCAC 04H .0201 ELIGIBILITY FOR ACCESS TO DCIN

(a) Only agencies that have obtained an ORI and have complied with Rule .0202 of this Section may access DCIN.

(b) Any agency in North Carolina desiring an ORI shall make a written request to DCI. DCI shall ~~obtain~~ request an ORI from NCIC. ~~If the request is denied by NCIC, DCI shall provide written findings to the requesting agency outlining the necessary elements to obtain an ORI.~~

(c) If the request is denied by NCIC, DCI shall provide written findings to the requesting agency detailing the reasons for the denial and providing the requesting agency information on the necessary elements to obtain an ORI.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0202 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0202 MANAGEMENT CONTROL REQUIREMENTS

Each device with access to DCIN and those personnel who operate devices with DCIN access must be under the direct and immediate management control of a criminal justice agency, criminal justice board or an FBI approved non-criminal justice agency. The degree of management control shall be such that the agency head, board or approved agency has the authority to:

(1) set policies and priorities concerning the use and operation, configuration, or maintenance of devices or computer networks accessing DCIN;

(2) hire, supervise, suspend or dismiss those personnel who will be connected with the operation, configuration, maintenance, or use of devices or computer networks accessing DCIN;

(3) restrict unauthorized personnel from access or use of devices accessing DCIN; and

(4) assure compliance with all rules and regulations of the FBI and SBI in the operation of devices with access to DCIN or use of all information received through DCIN.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0203 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0203 NON-TERMINAL ACCESS

(a) A non-terminal criminal justice agency may gain access to DCIN through a criminal justice agency ~~which~~ that has direct access to the network. The servicing agency (agency providing access) shall enter into a servicing agreement with the non-terminal agency (agency receiving service) as described in Rule .0303 of this Subchapter.

~~(b) Any servicing agency which fails to enforce penalties that are placed upon the non-terminal agency is in violation of this Rule and subject to the provisions of 12 NCAC 04J .0102 (e).~~

(~~c~~ b) The agreement shall:

(1) authorize access to specific data;

(2) limit the use of data to purposes for which given;

(3) insure the security and confidentiality of the data consistent with these procedures and;

(4) provide sanctions for violation thereof.

(~~d~~ c) Access shall be granted only if the terminal agency agrees.

(d) Any servicing agency which fails to enforce penalties that are placed upon the non-terminal agency is in violation of this Rule and subject to the provisions of 12 NCAC 04J .0102 (e).

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0302 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0302 SERVICING AGREEMENT

(a) Any agency authorized pursuant to ~~12 NCAC 04H .0201~~ Rule .0201 of this Subchapter with a DCIN device ~~which~~ that provides access to a non-terminal agency shall enter into a written servicing agreement with the serviced agency. The agreement shall include the following information:

(1) the necessity for valid and accurate information being submitted for entry into DCIN;

(2) the necessity for documentation to substantiate data entered into DCIN;

(3) the necessity of adopting timely measures for entering, correcting or canceling data in DCIN;

(4) validation requirements pursuant to ~~12 NCAC 04I .0203;~~ Rule 04I .0203 of this Chapter;

(5) the importance of confidentiality of information provided via DCIN;

(6) liabilities;

(7) the ability to confirm a hit 24 hours a day;

(8) the necessity of using the ORI of the official record holder in record entries and updates; and

(9) the necessity of using the ORI of the initial user when making inquiries.

(b) The servicing agreement must be signed by the head of the servicing agency and the head of the non-terminal agency, notarized, and a copy must be forwarded to CIIS by the non-terminal agency.

(c) DCI shall be notified of any cancellations or changes made in servicing agreements by the party making the cancellation or changes.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0303 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0303 CONTROL AGREEMENTS

(a) A non-criminal justice agency designated to perform criminal justice functions for a criminal justice agency is eligible for access to DCIN.

(b) A written management control agreement shall be entered into between a law enforcement agency and a 911 communications center when management control of the 911communications center will be under an entity other than the law enforcement agency. The agreement shall state that requirements of Rule .0202 of this Subchapter are in effect, and shall stipulate the management control of the criminal justice function remains solely with the law enforcement agency.

(c) A written management control agreement shall be entered into between a law enforcement agency and their governmental information technology (IT) division when the information technology role will be under an entity other than the law enforcement agency. The agreement shall state that the requirements pursuant to ~~12 NCAC 04H .0202~~ Rule .0202 of this Subchapter are in effect, and shall stipulate that the management control of the criminal justice function remains solely with the law enforcement agency.

(d) A written agreement shall be entered into between a law enforcement agency and a private contractor when the private contractor configures or supports any device or computer network that stores, processes, or transmits criminal justice information. The written agreement must incorporate the most current version of the CJIS Security Addendum. The CJIS Security Addendum may be found in the current CJIS Security Policy.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0304 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0304 DISCLOSURE AGREEMENT

(a) A written disclosure agreement shall be entered into between the SBI and any individual or agency seeking access to DCI-maintained criminal justice information for purposes of research.

(b) The disclosure agreement shall state that each participant and employee of every program of research with ~~authorized~~ access to computerized information is aware of the issues of ~~privacy,~~ privacy and the limitations regarding the use of accessed information, and that ~~they agree to abide~~ he or she is bound by CIIS rules concerning these issues pursuant to ~~12 NCAC 04I .0407.~~ Rule 04I .0407 of this Chapter.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0401 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0400 – STANDARDS AND CERITIFICATION AS A DCIN USER

12 NCAC 04H .0401 DCIN USERS

(a) Prior to receiving certification as a DCIN user, and as a condition for maintaining certification as a DCIN user, each applicant or user shall be a citizen of the United States.

(b) The applicant or certified user shall be at least 18 years of age.

(c) An individual is eligible to attend certification class and become a DCIN user only if employed by and under the management control of an agency as described in Rule .0201 of this Subchapter and only after the individual has had a fingerprint-based criminal records search completed by the employing agency indicating that the individual has not been convicted of a criminal offense described in (d) or (e) of this Rule.

(d) A conviction of a felony renders an applicant or certified DCIN user permanently ineligible to hold such certification.

(e) A conviction of a crime or unlawful act defined as a Class B ~~Misdemeanor~~ misdemeanor renders an applicant ineligible to become certified as a DCIN user when such conviction is within 10 years of the applicant's date of request for DCIN certification. Existing DCIN users convicted of a crime or unlawful act defined as a Class B Misdemeanor while holding certification are ineligible to maintain such certification for a period of 10 years following such conviction. An applicant or certified DCIN user is permanently ineligible to hold such certification upon conviction of two or more Class B misdemeanors regardless of the date of conviction.

(f) No applicant for certification as a DCIN user is eligible for certification while the applicant is subject to pending or outstanding criminal charges, ~~which, if adjudicated,~~ that, if the applicant were convicted, would disqualify the applicant from holding such certification.

(g) No DCIN user is eligible to access DCIN while the user is subject to pending or outstanding criminal charges, ~~which, if adjudicated,~~ that, if the applicant were convicted, would disqualify the user from access.

(h) An employee assigned as a DCIN user and who currently holds valid certification as a sworn law enforcement officer with the powers of arrest through either the North Carolina Criminal Justice Education and Training Standards Commission or the North Carolina Sheriff's Education and Training Standards Commission is not subject to the criminal history record and background search provisions of this Rule.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0402 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0402 CERTIFICATION AND RECERTIFICATION OF DCIN USERS

(a) Personnel who are assigned the duty of using a DCIN device shall be certified within 120 days from employment or assignment to user duties. Certification shall be awarded based on achieving a test score of 80 percent or greater in each training module for which the user is seeking certification.

(b) All DCIN users shall be certified by DCI. The initial certification of a user shall be awarded upon attending the "DCIN/NCIC General Inquiries" module class, and achieving a passing score on the accompanying test offered through the DCIN end user interface. A student may also take one or more additional module training classes offered by DCI, which teach the specific functions of DCIN applicable to their job duties. A user may perform only those functions in which they have been trained and certified.

(c) Tests for modules in which a student is seeking initial certification shall be taken within 15 days of the end of the class, and may be open-book. If a student fails the initial certification test they shall have until the 15th day to pass the test, but shall wait at least 24 hours between the failed test and the next attempt. A student shall have a maximum of three attempts to pass the test. If the student fails to achieve a passing score after the third attempt the user shall re-take the module training class.

(d) Recertification requires achieving a test score of 80 percent or higher on the test corresponding to the module for which the user is seeking recertification, and may be accomplished by taking the test through the DCIN end user interface. Recertification is required every two years for each module in which the user is certified and may be obtained any time 30 days prior to or 90 days after expiration.

(e) Tests for modules in which the user is seeking recertification shall be taken within 30 days prior to expiration or within 90 days after expiration, and may be open-book. If the user fails the recertification test the user shall have up to the 90th day after expiration to pass the test, but shall wait at least 24 hours between the failed test and the next attempt. A user shall have a maximum of three attempts to pass the test. If the user fails to achieve a passing score after the third attempt the user shall re-take the training module class. If a user fails to recertify in any module after the 90th day the user must attend the module training class for the module in which the user seeks recertification and achieve a passing score on the test.

(f) ~~New personnel~~ Personnel newly hired or ~~personnel newly~~ assigned to duties of a terminal user shall receive an indoctrination ~~and hands-on training~~ on the basic functions and terminology of DCIN by their own agency prior to attending an initial certification class. Such personnel may operate a ~~terminal~~ DCIN device ~~accessing DCIN while obtaining training~~ during the indoctrination if ~~such personnel~~ they are directly supervised by a certified user and are within the 120-day training period. ~~After receiving hands on training new personnel shall take a test provided by the SBI to confirm indoctrination, and must achieve a score of 80 percent or higher.~~

(g) Any user whose Module 1 certification has expired may recertify up to 90 days after the user's expiration. The individual shall not use any device connected to DCIN during the time between expiration and passing the recertification test(s). Any user whose Module 1 certification has expired more than 90 days shall attend and successfully complete the " DCIN/NCIC General Inquiries" class.

(h) When a DCIN certified user leaves the employment of an agency, the TAC shall notify DCI within 24 hours, and disable the user's user identifier. DCI shall move user's user identifier to an inactive status until such time the user is employed by another agency.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04H .0403 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0403 ENROLLMENT

(a) Enrollment is necessary for student attendance at any training for DCIN users. Enrollment shall be requested and approved by the agency ~~Terminal Agency Coordinator (TAC)~~ TAC and personnel must meet the management control requirements outlined in Section .0200 of this Subchapter.

(b) DCI shall maintain enrollment for all certification classes.

(c) Enrollment shall be done ~~in~~ by an automated method provided by DCI.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0101 is adopted with changes as published in 28:10 NCR 1008 as follows:

SUBCHAPTER 4I – SECURITY AND PRIVACY

SECTION .0100 – SECURITY AT DCIN DEVICE SITES

12 NCAC 04I .0101 SECURITY OF DCIN DEVICES

Agencies ~~who~~ that have management control of a DCIN device shall institute controls for maintaining the sensitivity and confidentiality of all criminal justice information (CJI) provided through DCIN. These controls include the following:

(1) a DCIN device and any peripheral or network-connected printer shall be within a physically secure location, as defined by the FBI CJIS Security Policy, accessible only to authorized personnel. Any DCIN device not located within a physically secured location shall have advanced authentication measures installed and enabled; and

(2) DCIN training module documents shall be located in a physically secure location accessible only by authorized personnel.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0102 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0102 OFFICIAL USE OF DCIN

(a) DCIN shall be used for ~~appropriate~~ criminal justice and law enforcement purposes only. All traffic generated over the network shall be made in the performance of an employee's or agency's official duties as they relate to the administration of criminal justice.

(b) Transmission of non-criminal justice information through DCIN is prohibited.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0103 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0103 PERSONNEL SECURITY

(a) Agencies that have management control of DCIN devices shall institute procedures to ensure those non-DCIN certified individuals with direct access to their DCIN devices or any network that stores, processes, or transmits criminal justice information have been properly screened.

(b) This Rule includes:

(1) individuals employed by a municipality or county government who configure or support devices that:

(A) store criminal justice information;

(B) process criminal justice information; or

(C) transmit criminal justice information; and

(2) individuals employed by private vendors or private contractors who configure or support devices that:

(A) store criminal justice information;

(B) process criminal justice information; or

(C) transmit criminal justice information.

(c) To ensure proper background screening an agency shall conduct both state of residence and national fingerprint-based background checks for personnel described in Paragraphs (a) and (b) of this Rule.

(d) Applicant fingerprint cards shall be submitted by an agency to the SBI to conduct the check. Once the check has been completed the SBI shall send notice to the submitting agency as to the findings of the check.

(e) Personnel described in Paragraphs (a) and (b) of this Rule must meet the same requirements as those described in 12 NCAC 04H .0401 (c).

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0104 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0104 SECURITY AWARENESS TRAINING

(a) Security awareness training is required within six months of initial assignment and every two years ~~thereafter,~~ thereafter for any personnel who have access to DCIN devices or any network that stores, processes, or transmits criminal justice information.

(b) This Rule also applies to any individual described in Rule .0103 of this Subchapter who is responsible for the configuration or support of devices or computer networks that store, process, or transmit criminal justice ~~information as described in Rule .0103 of this Subchapter.~~ information.

(c) Security awareness training shall be facilitated by CIIS.

(d) Records of security awareness training shall be documented, kept current, and maintained by the criminal justice agency.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0201 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0200 – ~~NCIC~~ RESTRICTED AND RESTRICTED FILES

12 NCAC 04I .0201 DOCUMENTATION AND ACCURACY

(a) Law enforcement and criminal justice agencies may enter stolen property, recovered property, wanted persons, missing persons, protection orders, or convicted sex offenders into NCIC restricted and unrestricted files. Any record entered into NCIC files must be documented. The documentation required is:

(1) a theft report of items of stolen property;

(2) an active warrant for arrest or order for arrest for the entry of wanted persons;

(3) a missing person report and, if a juvenile, a written statement from a parent, spouse, family member, or legal guardian verifying the date of birth and confirming that a person is missing;

(4) a medical examiner's report for an unidentified dead person entry;

(5) a protection order or ex parte order (for "temporary orders") issued by a court of competent jurisdiction for a protection order entry; or

(6) a judgment from a court of competent jurisdiction ordering an individual to register as a sex offender.

(b) All NCIC file entries must be complete and accurately reflect the information contained in the agency's investigative documentation at the point of initial entry or modification. NCIC file entries must be checked by a second party who shall initial and date a copy of the record indicating accuracy has been confirmed.

(c) The following key searchable fields shall be entered for person-based NCIC file entries, if available, and shall accurately reflect the information contained in the entering agency's investigative documentation:

(1) Name (NAM);

(2) Date of Birth (DOB);

(3) Sex (SEX);

(4) Race (RAC);

(5) Social Security Number (SOC), for any person-based NCIC file entry other than sex offenders;

(6) Aliases (AKA);

(7) FBI Number (FBI);

(8) State Identification Number (SID); and

(9) Agency's file number (OCA).

Other data elements may be required for entry ~~in to~~ into the NCIC. Those additional data elements shall accurately reflect an agency's investigative file.

(d) Searchable fields that are required by the DCIN end user interface shall be entered for property-based NCIC file entries, and shall accurately reflect the information contained in the entering agency's investigative documentation.

(e) An agency must enter any additional information that becomes available later.

History Note: *Authority G.S. 114-10; 114-10.1.*

Eff. July 1, 2014.

12 NCAC 04I .0202 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0202 TIMELINESS

(a) Law enforcement and criminal justice agencies shall enter records within three days when conditions for entry are met except when a federal law, state statute, or documentation exists to support a delayed entry. Any decision to delay entry under this exception shall be documented.

(b) Timeliness can be defined based on the type of record entry being made:

(1) Wanted Person File - entry of a wanted person shall be made immediately after the decision to arrest or to authorize arrest has been made, and the decision to extradite has been made. "Immediately" is defined as within three days.

(2) Missing Person File - entry of a missing person shall be made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) and the appropriate record documentation are available. For missing persons under age 21, a NCIC Missing Person File record shall be entered within two hours of receiving the minimum data required for entry.

(3) Article, Boat, Gun, License Plate, Securities, Vehicle Part, Boat Part, Vehicle, Protection Order, and Sex Offender Registry ~~files~~ Files - entry is made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) and the record documentation are available. Information about stolen license plates and vehicles shall be verified through the motor vehicle registration files prior to record entry if possible. However, if motor vehicle registration files are not accessible, the record shall be entered into NCIC and verification shall be completed when the registration files become available.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0203 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0203 VALIDATIONS

(a) Law enforcement and criminal justice agencies shall validate all record entries, with the exception of articles, made into the NCIC restricted and unrestricted files.

(b) Validation shall be accomplished by reviewing the original entry and current supporting documents. Stolen vehicle, stolen boat, wanted person, missing person, protection order, and sex offender file entries require consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files or other appropriate source or individual in addition to the review of the original file entry and supporting documents.

(c) Validations shall be conducted through the CIIS automated method.

(d) Any records containing inaccurate data shall be modified and records which are no longer current or cannot be substantiated by a source document shall be removed from the NCIC.

(e) Any agency ~~which~~ that does not properly validate its records shall have their records purged for that month by NCIC. An agency shall be notified of the record purge through an NCIC-generated message sent to the agency's main DCIN device. An agency may re-enter the cancelled records once the records have been validated.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0204 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0204 HIT CONFIRMATION

(a) Any agency entering record information into the NCIC restricted and unrestricted files, or which has a servicing agency enter record information for its agency, shall provide hit confirmation 24 hours a day. Hit confirmation of NCIC records means that an agency receiving a positive NCIC response from an inquiry must communicate with the official record holder to confirm the following before taking a person or property into custody:

(1) the person or property inquired upon is the same as the person or property identified in the record;

(2) the warrant, missing person report, theft report, or protection order is still outstanding; or

(3) a decision regarding the extradition of a wanted person has been made; the return of a missing person to the appropriate authorities is still desired; the return of stolen property to its rightful owner is still desired; or the terms, conditions, or service of a protection order still exist.

(b) The official record holder must respond after receiving a hit confirmation request with the desired information or a notice of the amount of time necessary to confirm or reject the record.

(c) An agency that is the official record holder shall have 10 minutes to respond to a hit confirmation request with a priority level of "urgent." If the agency fails to respond after the initial request, the requesting agency shall send a second hit confirmation request to the official record holder. Any subsequent hit confirmation requests shall also be at 10-minute intervals.

(d) An agency shall have one hour to respond to a hit confirmation request with a priority level of "routine." If the agency fails to respond after the initial request, the requesting agency shall send a second hit confirmation request to the official record holder. Any subsequent hit confirmation requests shall also be at one-hour intervals.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0301 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0300 – SUBMISSION OF DATA FOR CRIMINAL HISTORY RECORDS

12 NCAC 04I .0301 ARREST FINGERPRINT CARD

(a) Fingerprint cards submitted in accordance with G. S. 15A – 502 must contain the following information on the arrestee in order to be processed by the SBI ~~and~~ or FBI:

(1) ORI number and address of arresting agency;

(2) complete name;

(3) date of birth;

(4) race;

(5) sex;

(6) date of arrest;

(7) criminal charges; and

(8) a set of fingerprint impressions and palm prints if the agency is capable of capturing palm prints.

(b) Any fingerprint cards physically received by the SBI that do not meet these requirements shall be returned to the submitting agency to be corrected and resubmitted. Any fingerprint cards that have been submitted electronically to the SBI that do not meet these standards shall not be accepted. The submitting agency shall receive electronic notification that the prints did not meet minimum standards through the agency's LiveScan device.

~~(b)~~ (c) The arrest and fingerprint information contained on the arrest fingerprint card shall be added to the North Carolina's CCH files, and electronically forwarded to the FBI's Interstate Identification Index (III) for processing.

~~(c)~~ (d) Criminal fingerprint cards shall be submitted in the following ways:

(1) electronically through the agency's LiveScan device to North Carolina's Statewide Automated Fingerprint Identification System (SAFIS); or

(2) mail addressed to:

North Carolina State Bureau of Investigation
Criminal Information and Identification Section
3320 Garner Road
Raleigh, North Carolina 27626
Attention: AFIS & Technical Search Unit

History Note: *Authority G.S. 15A-502; 15A-1383.*
Eff. July 1, 2014.

12 NCAC 04I .0401 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0400 – USE AND ACCESS REQUIREMENTS FOR CRIMINAL HISTORY RECORD INFORMATION, NICS INFORMATION, AND N-DEX INFORMATION

12 NCAC 04I .0401 DISSEMINATION AND LOGGING OF CHRI AND NICS RECORDS

(a) Criminal history record information (CHRI) obtained from or through DCIN, NCIC, N-DEx, or Nlets shall not be disseminated to anyone outside of those agencies eligible under 12 NCAC 04H .0201(a) except as provided by Rules ~~.0402,~~ .0403, ~~.0404,~~ .0405, .0406, and .0409 of this Section. Any agency assigned a limited access ORI shall not obtain CHRI. Any agency requesting CHRI that has not received an ORI pursuant to 12 NCAC 04H .0201(a) shall be denied access and referred to the North Carolina ~~CJIS System Officer (CSO).~~ CSO.

(b) CHRI is available to eligible agency personnel only on a "need-to-know" basis as defined in 12 NCAC 04H .0104.

(c) The use or dissemination of CHRI obtained through DCIN or N-DEx for unauthorized purposes is a violation of this Rule ~~and subject to the provisions of 12 NCAC 04J .0102(c) and (d)~~.

(d) CIIS shall maintain an automated log of CCH/CHRI/National Instant Criminal Background Check System (NICS) inquiries for a period of not less than one year from the date of inquiry. The automated log shall contain the following information as supplied by the user on the inquiry screen and shall be made available on-line to the inquiring agency;

(1) date of inquiry;

(2) name of record subject;

(3) state identification number (SID) or FBI number of the record subject;

(4) message key used to obtain information;

(5) purpose code;

(6) user's initials;

(7) (Attention field) name of person and agency requesting information who is the initial user of the record;

(8) (Attention 2 field) name of person and agency requesting information who is outside of the initial user agency. If there is not a second individual receiving the information, information indicating why the information is requested may be placed in this field; and

(9) if applicable, NICS Transaction Number (NTN) for NICS logs only.

(e) Criminal justice agencies making secondary disseminations of CCH, CHRI, N-DEx, or NICS information obtained through DCIN shall maintain a log of the dissemination in a case. This log must identify the name of the recipient and their agency.

(f) Each criminal justice agency obtaining CHRI through a DCIN device shall conduct an audit of their automated CCH log as provided by DCIN once every month for the previous month. The audit shall take place within 15 business days of the end of the month being reviewed. This audit shall include a review for unauthorized inquiries and disseminations, improper use of agency ORI's, agency names, and purpose codes. These logs must be maintained on file for one year from the date of the inquiry, and may be maintained electronically by the criminal justice agency. Any violation of CIIS rules must be reported by an agency representative to CIIS within 20 business days of the end of the month being reviewed. On those months that do not contain 20 business days, any violations of CIIS rules must be reported by an agency representative to CIIS by the first

business day of the following month, at the latest. If an agency does not have a device connected to DCIN that can receive CHRI, this audit is not required.

(g) Each criminal justice agency obtaining information from NICS or N-DEx shall conduct the same monthly audit as those for CHRI logs. The audit shall take place within 15 business days of the end of the month being reviewed. This audit shall include a review for unauthorized inquiries or disseminations and improper use of purpose codes. These logs must be maintained on file for one year from the date of inquiry, and may be maintained electronically by the criminal justice agency. Any violation of CIIS rules must be reported by an agency representative to CIIS within 20 business days of the end of the month being reviewed. On those months that do not contain 20 business days, any violations of CIIS rules must be reported by an agency representative to CIIS by the first business day of the following month, at the latest.

(h) DCIN automated CCH logs, automated NICS logs, and any secondary dissemination logs shall be available for audit or inspection by the CSO or his designee as provided in 12 NCAC 04I .0801.

(i) Out of state agencies requesting a statewide criminal record check shall utilize NCIC.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0402 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0402 ACCESSING OF CCH RECORDS

Any accessing of or inquiry into CCH records must be made with an applicable purpose code. An "applicable purpose code" ~~is defined as~~ means a code that conveys the reason for which an inquiry is made.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0403 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0403 USE OF CHRI FOR CRIMINAL JUSTICE EMPLOYMENT

(a) Agencies must submit an applicant fingerprint card on each individual seeking criminal justice employment, and the card must contain the following information in order to be processed by DCI and FBI:

(1) complete name;

(2) date of birth;

(3) race;

(4) sex;

(5) position applied for;

(6) hiring agency; and

(7) a set of legible fingerprint impressions.

Any fingerprint cards that do not meet these requirements shall be returned by DCI to the submitting agency for correction and resubmitted.

(b) For sworn and telecommunicator positions the response and the fingerprint card ~~will~~ shall be forwarded to the appropriate training and standards agency. For non-sworn positions, the response shall be returned to the submitting agency. DCI shall not maintain the cards or responses.

(c) Agencies may submit the information in Paragraph (a) in an electronic method to CIIS for processing. Any fingerprints and associated information not meeting the requirements in Paragraph (a) shall not be accepted. An electronic notification shall be sent by DCI to the submitting agency indicating the submitted information did not meet minimum requirements.

History Note: *Authority G.S. 114-10; 114-10.1; 114-16; 114-19.*
Eff. July 1, 2014.

12 NCAC 04I .0404 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0404 RIGHT TO REVIEW

(a) An individual may obtain a copy of his or her own criminal history record by submitting a written request to the North Carolina State Bureau of Investigation Criminal Information and Identification Section, Attention: Applicant Unit – Right to Review, 3320 Garner Road, Raleigh, North Carolina 27626. The written request must be accompanied by a certified check or money order in the amount of fourteen dollars ($14.00) payable to the North Carolina State Bureau of Investigation, and must contain proof of identity to include:

(1) complete name and address;

(2) race;

(3) sex;

(4) date of birth;

(5) social security number; and

(6) a legible set of fingerprint impressions.

(b) The response ~~will~~ shall be submitted only to the individual. Copies of the response ~~cannot~~ shall not be provided by DCI to a third party.

(c) The accuracy or completeness of an individual's record may be challenged by submitting the "Right to Review Request Criminal History Written Exception" form available from DCI.

(d) Upon receipt of the "Right to Review Request Criminal History Written Exception", the CIIS shall initiate an internal record audit of the challenger's record to determine its accuracy. If any potential inaccuracies or omissions are discovered, DCI shall coordinate with the arresting agency to review the charge information previously submitted by that agency. Appropriate action shall be taken based on, in part, information provide by the arresting agency. DCI shall inform the challenger in writing of the results of the audit.

(e) If the audit fails to disclose any inaccuracies, or if the challenger wishes to contest the results of the audit, he or she is entitled to an administrative hearing pursuant to G.S. 150B-23.

History Note: *Authority G.S. 114-10; 114-10.1; 114-19.1.*
Eff. July 1, 2014.

12 NCAC 04I .0405 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0405 CCH USE IN LICENSING AND NON-CRIMINAL JUSTICE EMPLOYMENT PURPOSES

(a) Criminal justice agencies authorized under 12 NCAC 04H .0201 which issue licenses or approve non-criminal justice employment and want to use computerized criminal history information maintained by DCI for licensing, permit, and non-criminal justice employment purposes shall submit to CIIS a written request listing the types of licenses, permits, and employment for which they desire to use computerized criminal history information. A copy of the local ordinance or a reference to the North Carolina General Statute giving authority to issue a particular permit or license must be included in the written request.

(b) Authorization to use computerized criminal history information for licensing, permit, or employment purposes may be given only after the DCI and the North Carolina Attorney General's Office have evaluated and granted authorization based upon the authority of the North Carolina General Statutes or local ordinance pertaining to the issuance of that particular license or permit for employment.

(c) Once authorization has been given, DCI shall provide the agency an access agreement, which outlines the guidelines for information usage. The access agreement shall also include information on billing mechanisms. DCI shall bill the agency fourteen dollars ($14.00) for a check of North Carolina computerized criminal history files, and thirty-eight dollars ($38.00) for a search of both the North Carolina computerized criminal history files and a search of the FBI's Interstate Identification Index (III) files. DCI shall send an invoice to the requesting agency to collect these fees.

(d) The access agreement shall be signed by the requesting agency's head, and returned to DCI.

(e) The agency's terminal, if applicable, shall receive the capability to use the purpose code "E" in the purpose field of the North Carolina CCH inquiry screens for employment or licensing once the agency head has signed the access agreement and returned it to DCI. Once an agency has received this capability, it shall use the purpose code "E", the proper two character code, and ~~recipient of the record's name.~~ the name of the person receiving the record. A log of all primary and any secondary dissemination must also be kept for one year on all responses received from this type of inquiry.

(f) Criminal justice agencies may also gain access by submission of non-criminal justice applicant fingerprint cards. Approval must be obtained pursuant to the procedure in Paragraph (a) of this Rule. One applicant fingerprint card must be submitted on each individual. The fingerprint card must contain the following information on the applicant in order to be processed by DCI and the FBI:

(1) complete name;
(2) date of birth;
(3) race;
(4) sex;
(5) reason fingerprinted to include the N.C.G.S. or local ordinance number;
(6) position applied for;
(7) the licensing or employing agency; and
(8) a set of legible fingerprint impressions.

DCI shall return the letter of fulfillment to the submitting agency indicating the existence or absence of a criminal record.

(g) Requests from non-criminal justice agencies or individuals to use criminal history information maintained by DCI for licensing and employment purposes shall be treated as a fee for service request pursuant to G.S. 114-19.1 or any other applicable statute. The process for approval for non-criminal justice agencies or individuals shall be the same process as in Paragraph (a) of this Rule.

(h) Upon being approved, the requesting agency shall submit its requests to the North Carolina State Bureau of Investigation, Criminal Information and Identification Section, Special Processing Unit, 3320 Garner Road, Raleigh, North Carolina 27626. Each request shall include a fee in the form of a certified cashier's check, money order, or direct billing of ten dollars ($10.00) for a name-only check, fourteen dollars ($14.00) for a state-only fingerprint based check, or thirty-eight dollars ($38.00) for a state and national fingerprint based check ~~(if applicable)~~ (if applicable). ~~in the form of a certified cashier's check, money order, or direct billing.~~

(i) Criminal history record information accessible pursuant to this Rule shall be North Carolina criminal history record information, and FBI III information if permitted by statute.

History Note: *Authority G.S. 114-10; 114-10.1; 114-19.1.*
Eff. July 1, 2014.

12 NCAC 04I .0408 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0408 LIMITATION REQUIREMENTS

Research designs must preserve the anonymity of all subjects. The following requirements are applicable to all such programs of research and each criminal justice agency or researcher is responsible for their implementation:

(1) Computerized criminal history records furnished for purposes of any program of research shall not be used to the detriment of the person(s) to whom such information relates.

(2) Criminal history records furnished for purposes of any program of research shall not be used for any other purpose; nor may such information be used for any program of research other than that authorized by the North Carolina CJIS System Officer (CSO).

(3) Each researcher or anyone having access to the computerized criminal history shall, prior to having such access, sign a Disclosure Agreement with the CSO incorporating the requirements of ~~12 NCAC 04H .0305.~~ Rule .04H .0304 of this Chapter.

(4) The authorization for access to computerized criminal history records shall assure that the criminal justice agency and CIIS have rights to monitor the program of research to assure compliance with this Rule. Such monitoring rights include the right of CIIS staff to audit and review such monitoring activities and also to pursue their own monitoring activities.

(5) CIIS and the criminal justice agency involved may examine and verify the data generated as a result of the program, and, if a material error or omission is found to have occurred, may order the data not be released for any purpose unless corrected to the satisfaction of the agency and CIIS.

History Note: *Authority G.S. 114-10; 114-10.1; 114-19.1.*
Eff. July 1, 2014.

12 NCAC 04I .0409 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0409 ACCESS TO CHRI BY ATTORNEYS

(a) An attorney must have entered in to a proceeding in accordance with G. S. 15A-141 in order to access CHRI. The attorney may have access to the CHRI of only the defendant he or she is representing. The prosecuting District Attorney must approve the request.

(b) If, during a proceeding, an attorney desires CHRI of an individual involved in the proceeding other than the attorney's client, the attorney shall make a motion before the court indicating the desire for the CHRI.

(c) In order to maintain compliance with state and federal requirements an attorney shall disclose the purpose for any request of CHRI.

(d) CIIS shall provide a form to be utilized by any DCIN user when fulfilling a request for CHRI by an attorney. This form shall help ensure compliance with state and federal rules regarding access to and dissemination of CHRI.

(e) The attorney must fill out all applicable fields of the form and return it to the DCIN user to process the request. The attorney shall provide:

(1) the client's name;

(2) docket number for the matter;

(3) prosecutorial district in which the matter is being tried; and

(4) the next date on which the matter is being heard.

(f) The attorney may submit requests for CHRI only within the prosecutorial district of the District Attorney that is prosecuting the defendant(s). If a change of venue has been granted during a proceeding, this rule still applies, and the attorney must still seek the CHRI from the prosecutorial district within which the proceeding originated.

(g) Records of requests and dissemination to attorneys must be kept by the disseminating agency for a period of one year.

(h) Requests for North Carolina-only CHRI may be notarized in lieu of approval from the ~~DA or ADA.~~ District Attorney.

History Note: *Authority G.S. 114-10; 114-10.1; 15A-141.*
Eff. July 1, 2014.

12 NCAC 04I .0601 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0600 – STATEWIDE AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

12 NCAC 04I .0601 STATEWIDE AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

(a) Agencies which meet the requirements of 12 NCAC 04H .0201(a) may access the North Carolina Statewide Automated Fingerprint Identification System for criminal justice purposes.

(b) The acronym used for the Statewide Automated Fingerprint Identification System shall be ~~the~~ SAFIS.

History Note: *Authority G.S. 15A-502; 114-10; 114-10.1; 114-16.*
Eff. July 1, 2014.

12 NCAC 04I .0602 is adopted with changes as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0602 AVAILABLE DATA

(a) The following data is available through SAFIS and may be used to make comparisons and obtain CCH data:

(1) fingerprint images; and

(2) state identification number.

(b) When the state identification number is used to obtain CCH data, dissemination requirements outlined in Rule .0401~~(c) and (d)~~ of this Subchapter must be followed.

History Note: *Authority G.S. 15A-502; 114-10; 114-10.1; 114-16.*
Eff. July 1, 2014.

12 NCAC 04I .0701 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0700 – DIVISION OF MOTOR VEHICLE INFORMATION

12 NCAC 04I .0701 DISSEMINATION OF DIVISION OF MOTOR VEHCILES INFORMATION

(a) DMV information obtained from or through DCIN shall not be disseminated to anyone outside those agencies eligible under 12 NCAC 04H .0201(a) unless obtained for the following purposes:

(1) in the decision of issuing permits or licenses if statutory authority stipulates the non-issuance or denial of a permit or license to an individual who is a habitual violator of traffic laws or who has committed certain traffic offenses and those licensing purposes have been authorized by CIIS and the Attorney General's Office;

(2) by governmental agencies to evaluate prospective or current employees for positions involving the operation of publicly owned vehicles; or

(3) by a defendant's attorney of record in accordance with G.S. 15A-141.

(b) Each agency disseminating driver history information to a non-criminal justice agency for any of the purposes listed in Paragraph (a) shall maintain a log of dissemination for one year containing the following information:

(1) date of inquiry for obtaining driver's history;

(2) name of terminal operator;

(3) name of record subject;

(4) driver's license number;

(5) name of individual and agency requesting or receiving information; and

(6) purpose of inquiry.

(c) Driver history information obtained from or through DCIN shall not be released to the individual ~~of~~ named in the record. An individual seeking his or her own driver history information shall be instructed to contact DMV.

(d) DMV information obtained for any purpose listed in Paragraph (a) of this Rule shall be used for only that ~~official internal~~ purpose and shall not be redisseminated or released for any other purpose.

(e) Nothing in this rule shall prevent an attorney from discussing the contents of driver history information with the individual named in the record if the attorney is representing the individual in accordance with G.S. 15A-141.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04I .0801 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0800 - AUDITS

12 NCAC 04I .0801 AUDITS

(a) CIIS shall biennially audit criminal justice information entered, modified, cancelled, cleared and disseminated by DCIN users. Agencies subject to audit include all agencies that have direct or indirect access to information obtained through DCIN.

(b) CIIS shall send designated representatives to selected law enforcement and criminal justice agency sites to audit:

(1) criminal history usage and dissemination logs;

(2) NICS usage and dissemination logs;

(3) driver history dissemination logs;

(4) security safeguards and procedures adopted for the filing, storage, dissemination, or destruction of criminal history records;

(5) physical security of DCIN devices in accordance with the current FBI CJIS Security Policy;

(6) documentation establishing the accuracy, validity, and timeliness of the entry of records entered into NCIC wanted person, missing person, property, protection order, and DCIN and NCIC sex offender files;

(7) the technical security of devices and computer networks connected to DCIN in accordance with the current FBI CJIS Security Policy;

(8) user certification, status, and background screening;

(9) user agreements between the agency and North Carolina's ~~CJIS System Agency (CSA);~~ CSA;

(10) servicing agreements between agencies with DCIN devices and agencies without DCIN devices (when applicable);

(11) use of private contractors or governmental information technology professionals for information technology support along with the proper training and screening of those personnel; and

(12) control agreements between agencies and entities providing information technology support (when applicable).

(c) The audits shall be conducted to ensure that the agencies are complying with state and federal regulations, as well as federal and state statutes on security and privacy of criminal history record information.

(d) CIIS shall provide notice to the audited agency as to the findings of the audit. If discrepancies or deficiencies are discovered during the audit they shall be noted in the findings along with possible sanctions for any deficiencies or rule violations.

(e) If applicable, CIIS shall also biennially audit agencies' N-DEx access and usage. CIIS shall audit:

(1) network security;

(2) N-DEx transactions performed by agency personnel; and

(3) user certification and status

(f) Audits of N-DEx usage ~~will~~ shall occur concurrently with an agency's DCIN audit, and shall ensure compliance with state and federal regulations on security and privacy of criminal justice information contained within N-DEx.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04J .0101 is adopted with changes as published in 28:10 NCR 1008 as follows:

SUBCHAPTER 4J - PENALTIES AND ADMINISTRATIVE HEARINGS

SECTION .0100 - DEFINITIONS AND PENALTY PROVISIONS

12 NCAC 04J .0101 DEFINITIONS

As used in this Subchapter:

(1) "Revocation of ~~Certification"~~ certification" means a DCIN user's certification is canceled for a period not to exceed one year. At the end of the revocation period the user must attend the DCIN Module 1 certification class. Notification of the revocation shall be sent by DCI via certified mail to the DCIN user and the user's agency head.

(2) "Suspension of ~~Certification"~~ certification" means a DCIN user is prohibited from operating a DCIN device for a period not to exceed 90 days. Notification of the suspension shall be sent by DCI via certified mail to the DCIN user's agency head and to the DCIN user. The agency shall be audited within 90 days of reinstatement of a user's certification.

(3) "Suspension of ~~Services"~~ services" means an agency's direct access to DCIN is suspended for a period not to exceed two weeks after the North Carolina ~~CJIS System Officer's (CSO)~~ CSO's finding of fault, and the agency head must then appear before the CSO to respond to the cited violation. This suspension may be limited to certain files or may include a complete suspension of services, depending on the administrative procedure violated. The agency is subject to a re-audit after 90 days of reinstatement. Further violations of the same regulation, within two years from the date of the suspension, or failure to appear before the CSO to respond to the cited violation is grounds to cancel the user agreement with the agency.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. July 1, 2014.

12 NCAC 04J .0301 is adopted with changes as published in 28:10 NCR 1008 as follows:

SECTION .0300 - INFORMAL ~~HEARINGS~~ PROCEDURES

12 NCAC 04J .0301 INFORMAL ~~HEARING~~ PROCEDURE

(a) In accordance with G.S. 150B-22 ~~Any~~ any agency or DCIN user may request ~~an informal~~ a hearing before the North Carolina CSO within 30 days after receipt of written notification from DCI of an adverse action. A request for ~~an informal~~ a hearing shall be made by certified mail to the North Carolina State Bureau of Investigation Division of Criminal Information, Post Office Box 29500, Raleigh, North Carolina 27626.

(b) Upon receipt of a request for an informal hearing, the ~~North Carolina CJIS System Officer (CSO)~~ CSO shall conduct a hearing and consider the positions of the parties. The CSO shall notify the parties of his or her decision within two weeks following the informal hearing and provide information to the parties of their further appeal rights in accordance with G.S. 150B-23.

History Note: *Authority G.S. 114-10; 114-10.1; 150B-3(b); 150B-22; 150B-23(f).*
Eff. July 1, 2014.

Brincefield, Julie

From: Hickman, Joshua <JHICKMAN@ncdoj.gov>
Sent: Friday, May 09, 2014 1:38 PM
To: Deluca, Joe
Cc: Vojtko, Dana; Brincefield, Julie; Reeder, Amanda J; Hammond, Abigail M; Cronk, Amber
Subject: Re: Status report for DCI rules

Hey Joe,
Sorry for the delay.

Due to other obligations/duties associated with my new position I will not be able to make the deadline for our rule submissions for this month. I am aiming for next month's meeting.

I am about halfway through the technical changes. I'll let you know when I get them completed/delivered.

Joshua Hickman
Special Agent
Computer Crimes Unit
North Carolina State Bureau of Investigation
Mobile: 919-538-1448
jhickman@ncdoj.gov

On May 9, 2014, at 11:30 AM, "Deluca, Joe" <joe.deluca@oah.nc.gov> wrote:

> Josh,
>
> This is a reminder that you need to send me some notice that you will not be able to make the changes to your rules until next month.
>
> ***Joe DeLuca***
> ***Commission Counsel***
> ***N.C. OAH - Rules Review Commission***
>
> 919-431-3081 (Direct)
> 919-971-7268 (C)
> 919-431-3104 (F)
> 919-571-0500 (H)
>
>

STATE OF NORTH CAROLINA
OFFICE OF ADMINISTRATIVE HEARINGS

Mailing address:
6714 Mail Service Center
Raleigh, NC 27699-6714

Street address:
1711 New Hope Church Rd
Raleigh, NC 27609-6285

April 17, 2014

Joshua Hickman
Department of Justice / Division of Criminal Information
Sent via email attachment to Jhickman@ncdoj.gov

Re: 12 NCAC 04H, 04I, and 04J – All Rules Filed

Dear Mr Hickman:

At its meeting today, the Rules Review Commission extended the period of review on the above captioned rules in accordance with G.S. 150B-10. It did this in order to give you more time to complete the requested technical changes and perhaps make any other necessary changes in your rules.

The Commission hopes to complete action on these rules at its next meeting on Thursday, May 15, 2014.

If you have any questions concerning this action please call or email me.

Sincerely,

Joseph J DeLuca
Commission Counsel

Administration	Rules Division	Judges and Assistants	Clerk's Office	Rules Review Commission	Civil Rights Division
919/431-3000	919/431-3000	919/431-3000	919/431-3000	919/431-3000	919/431-3036
fax:919/431-3100	fax: 919/431-3104	fax: 919/431-3100	fax: 919/431-3100	fax: 919/431-3104	fax: 919/431-3103

12 NCAC 04H .0101 is adopted as published in 28:10 NCR 1008 follows:

SUBCHAPTER 4H – ORGANIZATIONAL FUNCTIONS AND DEFINITIONS

SECTION .0100 – GENERAL PROVISIONS

12 NCAC 04H .0101 SCOPE

(a) The rules in this Chapter are the rules of the North Carolina State Bureau of Investigation, Division of Criminal Information (DCI).

(b) The FBI Criminal Justice Information Services (CJIS) Security Policy is incorporated by reference herein and shall automatically include any later amendments or editions that may be published by the FBI. The policy is available at no charge on the FBI website: http://www.fbi.gov

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0102 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0102 DEFINITIONS

As used in this Chapter:

(1) "ACIIS" means Canada's Automated Criminal Intelligence and Information System.

(2) "Administration of Criminal Justice" means the:

(a) detection of accused persons or criminal offenders;

(b) apprehension of accused persons or criminal offenders;

(c) detention of accused persons or criminal offenders;

(d) pretrial release of accused persons or criminal offenders;

(e) post-trial release of accused persons or criminal offenders;

(f) prosecution of accused persons or criminal offenders;

(g) adjudication of accused persons or criminal offenders;

(h) correctional supervision of accused persons or criminal offenders;

(i) rehabilitation of accused persons or criminal offenders;

(j) collection of criminal history record information;

(k) storage of criminal history record information;

(l) dissemination of criminal history record information;

(m) screening of persons for the purpose of criminal justice employment; or

(n) administration of crime prevention programs to the extent access to criminal history record information is limited to law enforcement agencies for law enforcement programs (e.g. record checks of individuals who participate in Neighborhood Watch or safe house programs) and the result of such checks will not be disseminated outside the law enforcement agency.

(3) "Advanced Authentication" means an alternative method of verifying the identity of a computer system user. Examples include software tokens, hardware tokens, and biometric systems. These alternative methods are used in conjunction with traditional methods of verifying identity such as user names and passwords.

(4) "AOC" means the North Carolina Administrative Office of the Courts.

(5) "Authorized Recipient" means any person or organization who is authorized to receive state and national criminal justice information by virtue of being:

(a) a member of a law enforcement/criminal justice agency approved pursuant to Rule .0201 of this Subchapter; or

(b) a non-criminal justice agency authorized pursuant to local ordinance or a state or federal law.

(6) "CCH" means computerized criminal history record information. CCH can be obtained through DCIN or through N-DEx.

(7) "Certification" means documentation provided by CIIS showing that a person has been trained in the abilities of DCIN devices, and has knowledge for accessing those programs that are developed and administered by CIIS for local law enforcement and criminal justice agencies.

(8) "CHRI" means Criminal History Record Information. CHRI is information 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. This term does not include identification information such as fingerprint records or other biometric data to the extent that such information does not indicate formal involvement of the individual in the criminal justice system.

(9) "CIIS" means Criminal Information and Identification Section. CIIS is a section of DCI that manages all CJIS programs within North Carolina, including DCIN.

(10) "CJI" means Criminal Justice Information. CJI is all of the FBI CJIS provided 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. In addition, CJI refers to FBI CJIS provided data necessary for civil agencies to perform their mission including data used to make hiring decisions.

(11) "CJIS" means Criminal Justice Information Services. CJIS is the FBI division responsible for the collection, warehousing, and dissemination of relevant criminal justice information to the FBI and law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.

(12) "CJIS Security Policy" means a document published by the FBI CJIS Information Security Officer that provides criminal justice and non-criminal justice agencies with a minimum set of security requirements for the access to FBI CJIS systems to protect and safeguard criminal justice information whether in transit or at rest.

(13) "Class B Misdemeanor" ~~means an act committed or omitted in violation of any common law, criminal statute, or criminal traffic code of this state that is classified as a Class B Misdemeanor as set forth in the Class B Misdemeanor Manual as published by the North Carolina Department of Justice which is hereby incorporated by reference and shall automatically include any later amendments and editions of the incorporated material as provided by G.S. 150B-21.6. "Class B Misdemeanor" also~~ includes any act committed or omitted in violation of any common law, duly enacted ordinance, criminal statute, or criminal traffic code of any jurisdiction other than North Carolina, either civil or military, for which the maximum punishment allowable for the designated offense under the laws, statutes, or ordinances of the jurisdiction in which the offense occurred includes imprisonment for a term of more than six months but not more than two years. Specifically excluded ~~from this grouping of "Class B Misdemeanor" criminal offenses for jurisdictions other than North Carolina,~~ are motor vehicle or traffic offenses designated as being misdemeanors under the laws of ~~other jurisdictions~~jurisdictions other than the State of North Carolina with the following exceptions: ~~Class B Misdemeanor does expressly include,~~ either first or subsequent offenses of driving while impaired if the maximum allowable punishment is for a term of more than six months but not more than two years, and driving while license permanently revoked or permanently suspended ~~and those traffic offenses occurring in other jurisdictions which are comparable to the traffic offenses specifically listed in the Class B Misdemeanor Manual~~. "Class B Misdemeanor" shall also include acts committed or omitted in North Carolina prior to October 1, 1994 in violation of any common law, duly enacted ordinance, criminal statute, or criminal traffic code of this state for which the maximum punishment allowable for the designated offense included imprisonment for a term of more than six months but not more than two years.

(14) "Convicted" or "conviction" means, for purposes of DCIN user certification, the entry of:

(a) a plea of guilty;

(b) a verdict or finding of guilt by a jury, judge, magistrate, or other adjudicating body, tribunal, or official, either civilian or military; or

(c) a plea of no contest, nolo contendere, or the equivalent.

(15) "Criminal Justice Agency" means the courts, a government agency, or any subunit thereof which performs the administration of criminal justice pursuant to statute or executive order and which allocates more than 50 percent of its annual budget to the administration of criminal justice. State and federal Inspector General Offices are included in this definition.

(16) "Criminal Justice Board" means a board composed of heads of law enforcement or criminal justice agencies that have management control over a communications center.

(17) "CSA" means CJIS System Agency. The CSA is a state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice agency users with respect to the CJIS data from various systems managed by the FBI. In North Carolina, the CSA is the SBI.

(18) "CSO" means CJIS System Officer. The CSO an individual located within the CSA responsible for the administration of the CJIS network on behalf of the CSA. In North Carolina, the CSO is employed by the SBI.

(19) "DCI" means the Division of Criminal Information. DCI is the agency established by the Attorney General of North Carolina in accordance with Article 3 of Chapter 114 of the North Carolina General Statutes. The North Carolina State Bureau of Investigation's Criminal Information and Identification Section is a part of DCI.

(20) "DCIN" means the Division of Criminal Information Network. DCIN is the computer network used to collect, maintain, correlate, and disseminate information collected by CIIS under Article 3 of Chapter 114 of the North Carolina General Statutes. DCIN also provides access to information collected by other Federal, State, and local entities necessary for the administration of criminal justice.

(21) "DCIN User" means a person who has been certified through the DCIN certification process.

(22) "Device" means an electronic instrument used by a DCIN user to accomplish message switching, DMV inquiries, functional messages, or DCIN, NCIC, Nlets on-line file transactions.

(23) “Direct Access” means having the authority to:
(a) access systems managed by the FBI CJIS Division, whether by manual or automated means, not requiring the assistance of, or intervention by, any other party; or
(b) query or update national databases maintained by the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.
(24) "Disposition" means information on any action that results in termination or indeterminate suspension of the prosecution of a criminal charge.
(25) "Dissemination" means any transfer of information, whether orally, in writing, or by electronic means.
(26) "DMV" means the North Carolina Division of Motor Vehicles.
(27) “DMV Information” includes vehicle description and registration information, and information maintained on individuals to include name, address, date of birth, license number, license issuance and expiration, control number issuance, and moving vehicle violation or convictions.
(28) “DOC” means North Carolina Department of Adult Correction.
(29) “End User Interface” means software that is utilized by a certified user to connect to DCIN and perform message or file transactions.
(30) "Expunge" means to remove criminal history record information from the DCIN and FBI computerized criminal history and identification files pursuant to state statute.
(31) “FBI” means the Federal Bureau of Investigation.
(32) “FFL” means Federal Firearm Licensee. A FFL is any individual, corporation, company, association, firm, partnership, society, or joint stock company that has been licensed by the federal government to engage in the business of importing, manufacturing, or dealing in firearms or ammunition in accordance with 18 USC § 923.
(33) “III” means Interstate Identification Index. III is the FBI CJIS service that manages automated submission and requests for criminal history record information that is warehoused subsequent to the submission of fingerprint information.
(34) "Inappropriate Message" means any message that is not related to the administration of criminal justice.
(35) "Incident Based Reporting" or “I-Base” is a system used to collect criminal offense and arrest information for each criminal offense reported.
(36) “INTERPOL” means International Criminal Police Organization.
(37) “N-DEx” means Law Enforcement National Data Exchange. N-DEx is the repository of criminal justice records, available in a secure online environment, managed by the FBI Criminal Justice Information Services (CJIS) Division. N-DEx is available to criminal justice agencies throughout North Carolina, and its use is governed by federal regulations.
(38) “NCIC” means National Crime Information Center. NCIC is an information system maintained by the FBI that stores criminal justice information which can be queried by Federal, state, and local law enforcement and other criminal justice agencies.
(39) “NFF” means the National Fingerprint File. NFF is an FBI maintained enhancement to the Interstate Identification Index whereby only a single fingerprint card is submitted per state to the FBI for each offender at the national level.
(40) "Need-to-know" means for purposes of the administration of criminal justice, for purposes of criminal justice agency employment, or for some other purpose permitted by local ordinance, state statute, or federal regulation.
(41) “NICS” means the National Instant Criminal Background Check System. NICS is the system mandated by the Brady Handgun Violence Protection Act of 1993 that is used by Federal Firearms Licensees (FFLs) to instantly determine via telephone or other electronic means whether the transfer of a firearm would be in violation of Section 922(g) or (n) of Title 18, United States Code, or state law, by evaluating the prospective buyer’s criminal history. In North Carolina, NICS is used by sheriff’s offices throughout the state to assist in determining an individual’s eligibility for either a permit to purchase a firearm or a concealed handgun permit.
(42) "Nlets" means the International Justice and Public Safety Network.
(43) "Non-Criminal Justice Agency" or “NCJA” means any agency or sub-unit thereof whose charter does not include the responsibility to administer criminal justice, but may need to process criminal justice information. A NCJA may be public or private. An example is a 911 communications center that performs dispatching functions for a criminal justice agency (government), a bank needing access to

criminal justice information for hiring purposes (private), or a county school board that uses criminal history record information to assist in employee hiring decisions (public).

(44) "Non-Criminal Justice Information" means any information or message that does not directly pertain to the necessary operation of a law enforcement or criminal justice agency. Examples of messages that are non-criminal justice include, but are not limited to:

(a) accessing any DMV file for:

(i) political purposes;

(ii) vehicle repossession purposes; and

(iii) to obtain information on an estranged spouse or romantic interest;

(b) a message to confirm meal plans;

(c) a message to have a conversation; and

(d) a message to send well wishes during a holiday or birthday.

(45) "Official Record Holder" means the agency that maintains the master documentation and all investigative supplements of a restricted file entry or unrestricted file entry.

(46) "Ordinance" means a rule or law promulgated by a governmental authority including one adopted and enforced by a municipality or other local authority.

(47) "ORI" means Originating Agency Identifier, which is a unique alpha numeric identifier assigned by NCIC to each authorized criminal justice and non-criminal justice agency, identifying that agency in all computer transactions.

(48) "Private Contractor" means any non-governmental non-criminal justice agency that has contracted with a government agency to provide services necessary to the administration of criminal justice.

(49) "Re-certification" means renewal of a user's initial certification every two years.

(50) "Restricted Files" means those files maintained by NCIC that are protected as criminal history record information (CHRI), which is consistent with Title 28, Part 20 of the United States Code of Federal Regulations (CFR). Restricted files consist of:

(a) Gang Files;

(b) Known or Appropriately Suspected Terrorist (KST) Files;

(c) Supervised Release File;

(d) Immigration Violator Files;

(e) National Sex Offender Registry Files;

(f) Historical Protection Order Files of the NCIC;

(g) Identity Theft Files;

(i) Protective Interest File; and

(j) Person With Information (PWI) data within the Missing Person File.

(51) "Right-to-review" means the right of an individual to inspect his or her own criminal history record information.

(52) "SAFIS" means Statewide Automated Fingerprint Identification System.

(53) "SBI" means the North Carolina State Bureau of Investigation.

(54) "Secondary Dissemination" means the transfer of CCH/CHRI information to anyone legally entitled to receive such information that is outside the initial user agency.

(55) "SEND message" means messages that may be used by DCIN certified users to exchange official information of an administrative nature between in-state law enforcement/criminal justice agencies and out-of-state agencies by means of Nlets.

(56) "Servicing Agreement" means an agreement between a terminal agency and a non-terminal agency to provide DCIN terminal services.

(57) "State" means any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico and any territory or possession of the United States.

(58) "State Automated Fingerprint Identification System" or "SAFIS" means a computer-based system for reading, encoding, matching, storage and retrieval of fingerprint minutiae and images.

(59) "Statute" means a law enacted by a state's legislative branch of government.

(60) "TAC" means Terminal Agency Coordinator. A TAC is an individual who serves as a point of contact at a local agency in matters relating to DCIN or CJIS information systems. A TAC administers CJIS and CIIS system programs within the local agency and oversees the agency's compliance with both CIIS rules and CJIS system policies.

(61) "Terminal Agency" means any agency that has a device under its management and control that is capable of communicating with DCIN.

(62) “Training Module” means a manual containing guidelines for users on the operation of DCIN and providing explanations as to what information may be accessed through DCIN.

(63) "UCR" means the Uniform Crime Reporting program whose purpose it is to collect a summary of criminal offense and arrest information.

(64) “Unrestricted Files” means those files that are maintained by NCIC that are not considered “Restricted Files.”

(65) "User Agreement" means an agreement between a terminal agency and CIIS whereby the agency agrees to comply with all CIIS rules.

(66) "User Identifier" means a unique identifier assigned by an agency’s Terminal Agency Coordinator to all certified DCIN users that is used for gaining access to DCIN and for the identification of certified users.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0103 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0103 FUNCTION OF DCIN

(a) DCIN provides linkage with the following computer systems:

(1) National Crime Information Center (NCIC);

(2) International Justice and Public Safety Network (Nlets);

(3) North Carolina Division of Motor Vehicles (DMV);

(4) North Carolina Department of Adult Correction (DOC);

(5) North Carolina Administrative Office of the Courts (AOC);

(6) National Instant Criminal Background Check Service (NICS);

(7) Canada's Automated Criminal Intelligence and Information System (ACIIS); and

(8) International Criminal Police Organization (INTERPOL)

(b) Users of DCIN may:

(1) transmit or receive any criminal justice related message to any device connected to DCIN;

(2) enter into or retrieve information from North Carolina's:

(A) recovered vehicle file;

(B) sex offender registry; and

(C) concealed handgun permit file

(3) enter into or retrieve information from DCIN user certification and class enrollment files;

(4) enter into or retrieve information from NCIC's restricted and unrestricted files;

(5) access NCIC's criminal history data referred to as the Interstate Identification Index (III);

(6) obtain, on a need-to-know basis, the criminal record of an individual by inquiring into the state Computerized Criminal History (CCH) file maintained by CIIS, or CCH files maintained by other states and the Federal Bureau of Investigation (FBI) through III;

(7) communicate with devices in other states through Nlets with the capability to exchange automobile registration information, driver's license information, criminal history record information, corrections information, and other law enforcement related information;

(8) obtain information on North Carolina automobile registration, driver's license information and driver's history by accessing DMV maintained files;

(9) obtain registration information on all North Carolina registered boats, and inquire about aircraft registration and aircraft tracking;

(10) obtain information on those individuals under the custody or supervision of DOC; and

(11) access, enter, and modify information contained within the National Instant Criminal Background Check System (NICS).

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0201 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0200 – REQUIREMENTS FOR ACCESS

12 NCAC 04H .0201 ELIGIBILITY FOR ACCESS TO DCIN

(a) Only agencies that have obtained an ORI and have complied with Rule .0202 of this Section may access DCIN.
(b) Any agency in North Carolina desiring an ORI shall make a written request to DCI. DCI shall obtain an ORI from NCIC. If the request is denied by NCIC, DCI shall provide written findings to the requesting agency outlining the necessary elements to obtain an ORI.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0202 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0202 MANAGEMENT CONTROL REQUIREMENTS

Each device with access to DCIN and those personnel who operate devices with DCIN access must be under the direct and immediate management control of a criminal justice agency, criminal justice board or a FBI approved non-criminal justice agency. The degree of management control shall be such that the agency head, board or approved agency has the authority to:

(1) set policies and priorities concerning the use and operation, configuration, or maintenance of devices or computer networks accessing DCIN;

(2) hire, supervise, suspend or dismiss those personnel who will be connected with the operation, configuration, maintenance, or use of devices or computer networks accessing DCIN;

(3) restrict unauthorized personnel from access or use of devices accessing DCIN; and

(4) assure compliance with all rules and regulations of the FBI and SBI in the operation of devices with access to DCIN or use of all information received through DCIN.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0203 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0203 NON-TERMINAL ACCESS

(a) A non-terminal criminal justice agency may gain access to DCIN through a criminal justice agency which has direct access to the network. The servicing agency (agency providing access) shall enter into a servicing agreement with the non-terminal agency (agency receiving service) as described in Rule .0303 of this Subchapter.

(b) Any servicing agency which fails to enforce penalties that are placed upon the non-terminal agency is in violation of this Rule and subject to the provisions of 12 NCAC 04J .0102 (e).

(c) The agreement shall:

(1) authorize access to specific data;

(2) limit the use of data to purposes for which given;

(3) insure the security and confidentiality of the data consistent with these procedures and;

(4) provide sanctions for violation thereof.

(d) Access shall be granted only if the terminal agency agrees.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0301 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0300 - AGREEMENTS

12 NCAC 04H .0301 USER AGREEMENT

(a) Each agency receiving access to any data provided by FBI CJIS through DCIN shall sign a user agreement certifying that the agency head has read and understands DCIN, NCIC, CJIS, and other applicable rules and regulations, and that the agency head will uphold the agreement and abide by the rules and regulations. This agreement shall be signed by the agency head and by the North Carolina CJIS System Officer (CSO).

(b) When a new agency head is installed at an agency, a new user agreement shall be signed by the new agency head and the CSO.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0302 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0302 SERVICING AGREEMENT

(a) Any agency authorized pursuant to 12 NCAC 04H .0201 with a DCIN device which provides access to a non-terminal agency shall enter into a written servicing agreement with the serviced agency. The agreement shall include the following information:

(1) the necessity for valid and accurate information being submitted for entry into DCIN;
(2) the necessity for documentation to substantiate data entered into DCIN;
(3) the necessity of adopting timely measures for entering, correcting or canceling data in DCIN;
(4) validation requirements pursuant to 12 NCAC 04I .0203;
(5) the importance of confidentiality of information provided via DCIN;
(6) liabilities;
(7) the ability to confirm a hit 24 hours a day;
(8) the necessity of using the ORI of the official record holder in record entries and updates; and
(9) the necessity of using the ORI of the initial user when making inquiries.

(b) The servicing agreement must be signed by the head of the servicing agency and the head of the non-terminal agency, notarized, and a copy must be forwarded to CIIS by the non-terminal agency.

(c) DCI shall be notified of any cancellations or changes made in servicing agreements by the party making the cancellation or changes.

History: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0303 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0303 CONTROL AGREEMENTS

(a) A non-criminal justice agency designated to perform criminal justice functions for a criminal justice agency is eligible for access to DCIN.

(b) A written management control agreement shall be entered into between a law enforcement agency and a 911 communications center when management control of the 911communications center will be under an entity other than the law enforcement agency. The agreement shall state that requirements of Rule.0202 of this Subchapter are in effect, and shall stipulate the management control of the criminal justice function remains solely with the law enforcement agency.

(c) A written management control agreement shall be entered into between a law enforcement agency and their governmental information technology (IT) division when the information technology role will be under an entity other than the law enforcement agency. The agreement shall state that the requirements pursuant to 12 NCAC 04H .0202 are in effect, and shall stipulate that the management control of the criminal justice function remains solely with the law enforcement agency.

(d) A written agreement shall be entered into between a law enforcement agency and a private contractor when the private contractor configures or supports any device or computer network that stores, processes, or transmits criminal justice information. The written agreement must incorporate the most current version of the CJIS Security Addendum. The CJIS Security Addendum may be found in the current CJIS Security Policy.

History: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0304 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0304 DISCLOSURE AGREEMENT

(a) A written disclosure agreement shall be entered into between the SBI and any individual or agency seeking access to DCI-maintained criminal justice information for purposes of research.

(b) The disclosure agreement shall state that each participant and employee of every program of research with authorized access to computerized information is aware of the issues of privacy, the limitations regarding the use of accessed information, and that they agree to abide by CIIS rules concerning these issues pursuant to 12 NCAC 04I .0407.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0401 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0400 – STANDARDS AND CERITIFICATION AS A DCIN USER

12 NCAC 04H .0401 DCIN USERS

(a) Prior to receiving certification as a DCIN user, and as a condition for maintaining certification as a DCIN user, each applicant or user shall be a citizen of the United States.
(b) The applicant or certified user shall be at least 18 years of age.
(c) An individual is eligible to attend certification class and become a DCIN user only if employed by and under the management control of an agency as described in Rule .0201 of this Subchapter and only after the individual has had a fingerprint-based criminal records search completed by the employing agency indicating that the individual has not been convicted of a criminal offense described in (d) or (e) of this Rule.
(d) A conviction of a felony renders an applicant or certified DCIN user permanently ineligible to hold such certification.
(e) A conviction of a crime or unlawful act defined as a Class B Misdemeanor renders an applicant ineligible to become certified as a DCIN user when such conviction is within 10 years of the applicant's date of request for DCIN certification. Existing DCIN users convicted of a crime or unlawful act defined as a Class B Misdemeanor while holding certification are ineligible to maintain such certification for a period of 10 years following such conviction. An applicant or certified DCIN user is permanently ineligible to hold such certification upon conviction of two or more Class B misdemeanors regardless of the date of conviction.
(f) No applicant for certification as a DCIN user is eligible for certification while the applicant is subject to pending or outstanding criminal charges, which, if adjudicated, would disqualify the applicant from holding such certification.
(g) No DCIN user is eligible to access DCIN while the user is subject to pending or outstanding criminal charges, which, if adjudicated, would disqualify the user from access.
(h) An employee assigned as a DCIN user and who currently holds valid certification as a sworn law enforcement officer with the powers of arrest through either the North Carolina Criminal Justice Education and Training Standards Commission or the North Carolina Sheriff's Education and Training Standards Commission is not subject to the criminal history record and background search provisions of this Rule.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0402 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0402 CERTIFICATION AND RECERTIFICATION OF DCIN USERS

(a) Personnel who are assigned the duty of using a DCIN device shall be certified within 120 days from employment or assignment to user duties. Certification shall be awarded based on achieving a test score of 80 percent or greater in each training module for which the user is seeking certification.

(b) All DCIN users shall be certified by DCI. The initial certification of a user shall be awarded upon attending the " DCIN/NCIC General Inquiries" module class, and achieving a passing score on the accompanying test offered through the DCIN end user interface. A student may also take one or more additional module training classes offered by DCI, which teach the specific functions of DCIN applicable to their job duties. A user may perform only those functions in which they have been trained and certified.

(c) Tests for modules in which a student is seeking initial certification shall be taken within 15 days of the end of the class, and may be open-book. If a student fails the initial certification test they shall have until the 15th day to pass the test, but shall wait at least 24 hours between the failed test and the next attempt. A student shall have a maximum of three attempts to pass the test. If the student fails to achieve a passing score after the third attempt the user shall re-take the module training class.

(d) Recertification requires achieving a test score of 80 percent or higher on the test corresponding to the module for which the user is seeking recertification, and may be accomplished by taking the test through the DCIN end user interface. Recertification is required every two years for each module in which the user is certified and may be obtained any time 30 days prior to or 90 days after expiration.

(e) Tests for modules in which the user is seeking recertification shall be taken within 30 days prior to expiration or within 90 days after expiration, and may be open-book. If the user fails the recertification test the user shall have up to the 90th day after expiration to pass the test, but shall wait at least 24 hours between the failed test and the next attempt. A user shall have a maximum of three attempts to pass the test. If the user fails to achieve a passing score after the third attempt the user shall re-take the training module class. If a user fails to recertify in any module after the 90th day the user must attend the module training class for the module in which the user seeks recertification and achieve a passing score on the test.

(f) New personnel hired or personnel newly assigned to duties of a terminal user shall receive an indoctrination and hands-on training on the basic functions and terminology of DCIN by their own agency prior to attending an initial certification class. Such personnel may operate a terminal accessing DCIN while obtaining training if such personnel are directly supervised by a certified user and are within the 120-day training period. After receiving hands on training new personnel shall take a test provided by the SBI to confirm indoctrination, and must achieve a score of 80 percent or higher.

(g) Any user whose Module 1 certification has expired may recertify up to 90 days after the user's expiration. The individual shall not use any device connected to DCIN during the time between expiration and passing the recertification test(s). Any user whose Module 1 certification has expired more than 90 days shall attend and successfully complete the " DCIN/NCIC General Inquiries" class.

(h) When a DCIN certified user leaves the employment of an agency, the TAC shall notify DCI within 24 hours, and disable the user's user identifier. DCI shall move user's user identifier to an inactive status until such time the user is employed by another agency.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04H .0403 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04H .0403 ENROLLMENT

(a) Enrollment is necessary for student attendance at any training for DCIN users. Enrollment shall be requested and approved by the agency Terminal Agency Coordinator (TAC) and personnel must meet the management control requirements outlined in Section .0200 of this Subchapter.

(b) DCI shall maintain enrollment for all certification classes.

(c) Enrollment shall be done in an automated method provided by DCI.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0101 is adopted as published in 28:10 NCR 1008 as follows:

SUBCHAPTER 4I – SECURITY AND PRIVACY

SECTION .0100 – SECURITY AT DCIN DEVICE SITES

12 NCAC 04I .0101 SECURITY OF DCIN DEVICES

Agencies who have management control of a DCIN device shall institute controls for maintaining the sensitivity and confidentiality of all criminal justice information (CJI) provided through DCIN. These controls include the following:

(1) a DCIN device and any peripheral or network-connected printer shall be within a physically secure location, as defined by the FBI CJIS Security Policy, accessible only to authorized personnel. Any DCIN device not located within a physically secured location shall have advanced authentication measures installed and enabled; and

(2) DCIN training module documents shall be located in a physically secure location accessible only by authorized personnel.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0102 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0102 OFFICIAL USE OF DCIN

(a) DCIN shall be used for appropriate criminal justice and law enforcement purposes only. All traffic generated over the network shall be made in the performance of an employee's or agency's official duties as they relate to the administration of criminal justice.

(b) Transmission of non-criminal justice information through DCIN is prohibited.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0103 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0103 PERSONNEL SECURITY

(a) Agencies that have management control of DCIN devices shall institute procedures to ensure those non-DCIN certified individuals with direct access to their DCIN devices or any network that stores, processes, or transmits criminal justice information have been properly screened.

(b) This Rule includes:

(1) individuals employed by a municipality or county government who configure or support devices that:

(A) store criminal justice information;

(B) process criminal justice information; or

(C) transmit criminal justice information; and

(2) individuals employed by private vendors or private contractors who configure or support devices that:

(A) store criminal justice information;

(B) process criminal justice information; or

(C) transmit criminal justice information.

(c) To ensure proper background screening an agency shall conduct both state of residence and national fingerprint-based background checks for personnel described in Paragraphs (a) and (b) of this Rule.

(d) Applicant fingerprint cards shall be submitted by an agency to the SBI to conduct the check. Once the check has been completed the SBI shall send notice to the submitting agency as to the findings of the check.

(e) Personnel described in Paragraphs (a) and (b) of this Rule must meet the same requirements as those described in 12 NCAC 04H .0401 (c).

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0104 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0104 SECURITY AWARENESS TRAINING

(a) Security awareness training is required within six months of initial assignment and every two years thereafter, for any personnel who have access to DCIN devices or any network that stores, processes, or transmits criminal justice information.
(b) This Rule also applies to any individual who is responsible for the configuration or support of devices or computer networks that store, process, or transmit criminal justice information as described in Rule .0103 of this Subchapter.
(c) Security awareness training shall be facilitated by CIIS.
(d) Records of security awareness training shall be documented, kept current, and maintained by the criminal justice agency.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0201 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0200 – NCIC RESTRICTED AND RESTRICTED FILES

12 NCAC 04I .0201 DOCUMENTATION AND ACCURACY

(a) Law enforcement and criminal justice agencies may enter stolen property, recovered property, wanted persons, missing persons, protection orders, or convicted sex offenders into NCIC restricted and unrestricted files. Any record entered into NCIC files must be documented. The documentation required is:

(1) a theft report of items of stolen property;
(2) an active warrant for arrest or order for arrest for the entry of wanted persons;
(3) a missing person report and, if a juvenile, a written statement from a parent, spouse, family member, or legal guardian verifying the date of birth and confirming that a person is missing;
(4) a medical examiner's report for an unidentified dead person entry;
(5) a protection order or ex parte order (for "temporary orders") issued by a court of competent jurisdiction for a protection order entry; or
(6) a judgment from a court of competent jurisdiction ordering an individual to register as a sex offender.

(b) All NCIC file entries must be complete and accurately reflect the information contained in the agency's investigative documentation at the point of initial entry or modification. NCIC file entries must be checked by a second party who shall initial and date a copy of the record indicating accuracy has been confirmed.

(c) The following key searchable fields shall be entered for person-based NCIC file entries, if available, and shall accurately reflect the information contained in the entering agency's investigative documentation:

(1) Name (NAM);
(2) Date of Birth (DOB);
(3) Sex (SEX);
(4) Race (RAC);
(5) Social Security Number (SOC), for any person-based NCIC file entry other than sex offenders;
(6) Aliases (AKA);
(7) FBI Number (FBI);
(8) State Identification Number (SID); and
(9) Agency's file number (OCA).

Other data elements may be required for entry in to the NCIC. Those additional data elements shall accurately reflect an agency's investigative file.

(d) Searchable fields that are required by the DCIN end user interface shall be entered for property-based NCIC file entries, and shall accurately reflect the information contained in the entering agency's investigative documentation.

(e) An agency must enter any additional information that becomes available later.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0202 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0202 TIMELINESS

(a) Law enforcement and criminal justice agencies shall enter records within three days when conditions for entry are met except when a federal law, state statute, or documentation exists to support a delayed entry. Any decision to delay entry under this exception shall be documented.

(b) Timeliness can be defined based on the type of record entry being made:

(1) Wanted Person - entry of a wanted person shall be made immediately after the decision to arrest or to authorize arrest has been made, and the decision to extradite has been made. "Immediately" is defined as within three days.

(2) Missing Person - entry of a missing person shall be made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) and the appropriate record documentation are available. For missing persons under age 21, a NCIC Missing Person File record shall be entered within two hours of receiving the minimum data required for entry.

(3) Article, Boat, Gun, License Plate, Securities, Vehicle Part, Boat Part, Vehicle, Protection Order, and Sex Offender Registry files - entry is made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) and the record documentation are available. Information about stolen license plates and vehicles shall be verified through the motor vehicle registration files prior to record entry if possible. However, if motor vehicle registration files are not accessible, the record shall be entered into NCIC and verification shall be completed when the registration files become available.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0203 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0203 VALIDATIONS

(a) Law enforcement and criminal justice agencies shall validate all record entries, with the exception of articles, made into the NCIC restricted and unrestricted files.

(b) Validation shall be accomplished by reviewing the original entry and current supporting documents. Stolen vehicle, stolen boat, wanted person, missing person, protection order, and sex offender file entries require consultation with any appropriate complainant, victim, prosecutor, court, motor vehicle registry files or other appropriate source or individual in addition to the review of the original file entry and supporting documents.

(c) Validations shall be conducted through the CIIS automated method.

(d) Any records containing inaccurate data shall be modified and records which are no longer current or cannot be substantiated by a source document shall be removed from the NCIC.

(e) Any agency which does not properly validate its records shall have their records purged for that month by NCIC. An agency shall be notified of the record purge through an NCIC-generated message sent to the agency's main DCIN device. An agency may re-enter the cancelled records once the records have been validated.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0204 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0204 HIT CONFIRMATION

(a) Any agency entering record information into the NCIC restricted and unrestricted files, or which has a servicing agency enter record information for its agency, shall provide hit confirmation 24 hours a day. Hit confirmation of NCIC records means that an agency receiving a positive NCIC response from an inquiry must communicate with the official record holder to confirm the following before taking a person or property into custody:

(1) the person or property inquired upon is the same as the person or property identified in the record;

(2) the warrant, missing person report, theft report, or protection order is still outstanding; or

(3) a decision regarding the extradition of a wanted person has been made; the return of a missing person to the appropriate authorities is still desired; the return of stolen property to its rightful owner is still desired; or the terms, conditions, or service of a protection order.

(b) The official record holder must respond after receiving a hit confirmation request with the desired information or a notice of the amount of time necessary to confirm or reject the record.

(c) An agency that is the official record holder shall have 10 minutes to respond to a hit confirmation request with a priority level of "urgent." If the agency fails to respond after the initial request, the requesting agency shall send a second hit confirmation request to the official record holder. Any subsequent hit confirmation requests shall also be at 10-minute intervals.

(d) An agency shall have one hour to respond to a hit confirmation request with a priority level of "routine." If the agency fails to respond after the initial request, the requesting agency shall send a second hit confirmation request to the official record holder. Any subsequent hit confirmation requests shall also be at one-hour intervals.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0301 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0300 – SUBMISSION OF DATA FOR CRIMINAL HISTORY RECORDS

12 NCAC 04I .0301 ARREST FINGERPRINT CARD

(a) Fingerprint cards submitted in accordance with G. S. 15A – 502 must contain the following information on the arrestee in order to be processed by the SBI and FBI:

(1) ORI number and address of arresting agency;
(2) complete name;
(3) date of birth;
(4) race;
(5) sex;
(6) date of arrest;
(7) criminal charges; and
(8) a set of fingerprint impressions and palm prints if the agency is capable of capturing palm prints.

Any fingerprint cards physically received by the SBI that do not meet these requirements shall be returned to the submitting agency to be corrected and resubmitted. Any fingerprint cards that have been submitted electronically to the SBI that do not meet these standards shall not be accepted. The submitting agency shall receive electronic notification that the prints did not meet minimum standards through the agency's LiveScan device.

(b) The arrest and fingerprint information contained on the arrest fingerprint card shall be added to the North Carolina's CCH files, and electronically forwarded to the FBI's Interstate Identification Index (III) for processing.

(c) Criminal fingerprint cards shall be submitted in the following ways:

(1) electronically through the agency's LiveScan device to North Carolina's Statewide Automated Fingerprint Identification System (SAFIS); or

(2) mail addressed to:

North Carolina State Bureau of Investigation
Criminal Information and Identification Section
3320 Garner Road
Raleigh, North Carolina 27626
Attention: AFIS & Technical Search Unit

History Note: *Authority G.S. 15A-502; 15A-1383.*
Eff. May 1, 2014.

12 NCAC 04I .0302 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0302 FINAL DISPOSITION INFORMATION

(a) Final disposition information shall be submitted electronically to DCI by the Administrative Office of the Courts (AOC).

(b) The final disposition information shall be added to North Carolina's CCH files, and shall be electronically transmitted to the FBI's Interstate Identification Index (III).

(c) Any final disposition rejected by DCI shall be returned to the Clerk of Court in the county of the arresting agency for correction and resubmission.

History Note: *Authority G.S. 15A-1381; 15A-1382; 15A-1383; 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0303 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0303 INCARCERATION INFORMATION

(a) Incarceration information shall be electronically submitted to DCI by the North Carolina Department of Public Safety (DPS) on all subjects admitted to prison.

(b) The incarceration information shall be added to the North Carolina CCH files, and shall be electronically transmitted to the FBI's Interstate Identification Index (III).

History Note: *Authority G.S. 15A-502; 15A-1383; 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0401 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0400 – USE AND ACCESS REQUIREMENTS FOR CRIMINAL HISTORY RECORD INFORMATION, NICS INFORMATION, AND N-DEX INFORMATION

12 NCAC 04I .0401 DISSEMINATION AND LOGGING OF CHRI AND NICS RECORDS

(a) Criminal history record information (CHRI) obtained from or through DCIN, NCIC, N-DEx, or Nlets shall not be disseminated to anyone outside of those agencies eligible under 12 NCAC 04H .0201(a) except as provided by Rules .0402, .0404, .0406, and .0409 of this Section. Any agency assigned a limited access ORI shall not obtain CHRI. Any agency requesting CHRI that has not received an ORI pursuant to 12 NCAC 04H .0201(a) shall be denied access and referred to the North Carolina CJIS System Officer (CSO).

(b) CHRI is available to eligible agency personnel only on a "need-to-know" basis as defined in 12 NCAC 04H .0104.

(c) The use or dissemination of CHRI obtained through DCIN or N-DEx for unauthorized purposes is a violation of this Rule and subject to the provisions of 12 NCAC 04J .0102(c) and (d).

(d) CIIS shall maintain an automated log of CCH/CHRI/National Instant Criminal Background Check System (NICS) inquiries for a period of not less than one year from the date of inquiry. The automated log shall contain the following information as supplied by the user on the inquiry screen and shall be made available on-line to the inquiring agency;

(1) date of inquiry;

(2) name of record subject;

(3) state identification number (SID) or FBI number of the record subject;

(4) message key used to obtain information;

(5) purpose code;

(6) user's initials;

(7) (Attention field) name of person and agency requesting information who is the initial user of the record;

(8) (Attention 2 field) name of person and agency requesting information who is outside of the initial user agency. If there is not a second individual receiving the information, information indicating why the information is requested may be placed in this field; and

(9) if applicable, NICS Transaction Number (NTN) for NICS logs only.

(e) Criminal justice agencies making secondary disseminations of CCH, CHRI, N-DEx, or NICS information obtained through DCIN shall maintain a log of the dissemination in a case. This log must identify the name of the recipient and their agency.

(f) Each criminal justice agency obtaining CHRI through a DCIN device shall conduct an audit of their automated CCH log as provided by DCIN once every month for the previous month. The audit shall take place within 15 business days of the end of the month being reviewed. This audit shall include a review for unauthorized inquiries and disseminations, improper use of agency ORI's, agency names, and purpose codes. These logs must be maintained on file for one year from the date of the inquiry, and may be maintained electronically by the criminal justice agency. Any violation of CIIS rules must be reported by an agency representative to CIIS within 20 business days of the end of the month being reviewed. On those months that do not contain 20 business days, any violations of CIIS rules must be reported by an agency representative to CIIS by the first business day of the following month, at the latest. If an agency does not have a device connected to DCIN that can receive CHRI, this audit is not required.

(g) Each criminal justice agency obtaining information from NICS or N-DEx shall conduct the same monthly audit as those for CHRI logs. The audit shall take place within 15 business days of the end of the month being reviewed. This audit shall include a review for unauthorized inquiries or disseminations and improper use of purpose codes. These logs must be maintained on file for one year from the date of inquiry, and may be maintained electronically by the criminal justice agency. Any violation of CIIS rules must be reported by an agency representative to CIIS within 20 business days of the end of the month being reviewed. On those months that do not contain 20 business days, any violations of CIIS rules must be reported by an agency representative to CIIS by the first business day of the following month, at the latest.

(h) DCIN automated CCH logs, automated NICS logs, and any secondary dissemination logs shall be available for audit or inspection by the CSO or his designee as provided in 12 NCAC 04I .0801.

(i) Out of state agencies requesting a statewide criminal record check shall utilize NCIC.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0402 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0402 ACCESSING OF CCH RECORDS

Any accessing of or inquiry into CCH records must be made with an applicable purpose code. An "applicable purpose code" is defined as a code that conveys the reason for which an inquiry is made.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0403 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0403 USE OF CHRI FOR CRIMINAL JUSTICE EMPLOYMENT

(a) Agencies must submit an applicant fingerprint card on each individual seeking criminal justice employment, and the card must contain the following information in order to be processed by DCI and FBI:

(1) complete name;
(2) date of birth;
(3) race;
(4) sex;
(5) position applied for;
(6) hiring agency; and
(7) a set of legible fingerprint impressions.

Any fingerprint cards that do not meet these requirements shall be returned by DCI to the submitting agency for correction and resubmitted.

(b) For sworn and telecommunicator positions the response and the fingerprint card will be forwarded to the appropriate training and standards agency. For non-sworn positions, the response shall be returned to the submitting agency. DCI shall not maintain the cards or responses.

(c) Agencies may submit the information in Paragraph (a) in an electronic method to CIIS for processing. Any fingerprints and associated information not meeting the requirements in Paragraph (a) shall not be accepted. An electronic notification shall be sent by DCI to the submitting agency indicating the submitted information did not meet minimum requirements.

History Note: *Authority G.S. 114-10; 114-10.1; 114-16; 114-19.*
Eff. May 1, 2014.

12 NCAC 04I .0404 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0404 RIGHT TO REVIEW

(a) An individual may obtain a copy of his or her own criminal history record by submitting a written request to the North Carolina State Bureau of Investigation Criminal Information and Identification Section, Attention: Applicant Unit – Right to Review, 3320 Garner Road, Raleigh, North Carolina 27626. The written request must be accompanied by a certified check or money order in the amount of fourteen dollars ($14.00) payable to the North Carolina State Bureau of Investigation, and must contain proof of identity to include:

(1) complete name and address;
(2) race;
(3) sex;
(4) date of birth;
(5) social security number; and
(6) a legible set of fingerprint impressions.

(b) The response will be submitted only to the individual. Copies of the response cannot be provided by DCI to a third party.

(c) The accuracy or completeness of an individual's record may be challenged by submitting the "Right to Review Request Criminal History Written Exception" form available from DCI.

(d) Upon receipt of the "Right to Review Request Criminal History Written Exception", the CIIS shall initiate an internal record audit of the challenger's record to determine its accuracy. If any potential inaccuracies or omissions are discovered, DCI shall coordinate with the arresting agency to review the charge information previously submitted by that agency. Appropriate action shall be taken based on, in part, information provide by the arresting agency. DCI shall inform the challenger in writing of the results of the audit.

(e) If the audit fails to disclose any inaccuracies, or if the challenger wishes to contest the results of the audit, he is entitled to an administrative hearing pursuant to G.S. 150B-23.

History Note: *Authority G.S. 114-10; 114-10.1; 114-19.1.*
Eff. May 1, 2014.

12 NCAC 04I .0405 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0405 CCH USE IN LICENSING AND NON-CRIMINAL JUSTICE EMPLOYMENT PURPOSES

(a) Criminal justice agencies authorized under 12 NCAC 04H .0201 which issue licenses or approve non-criminal justice employment and want to use computerized criminal history information maintained by DCI for licensing, permit, and non-criminal justice employment purposes shall submit to CIIS a written request listing the types of licenses, permits, and employment for which they desire to use computerized criminal history information. A copy of the local ordinance or a reference to the North Carolina General Statute giving authority to issue a particular permit or license must be included in the written request.

(b) Authorization to use computerized criminal history information for licensing, permit, or employment purposes may be given only after the DCI and the North Carolina Attorney General's Office have evaluated and granted authorization based upon the authority of the North Carolina General Statutes or local ordinance pertaining to the issuance of that particular license or permit for employment.

(c) Once authorization has been given, DCI shall provide the agency an access agreement, which outlines the guidelines for information usage. The access agreement shall also include information on billing mechanisms. DCI shall bill the agency fourteen dollars ($14.00) for a check of North Carolina computerized criminal history files, and thirty-eight dollars ($38.00) for a search of both the North Carolina computerized criminal history files and a search of the FBI's Interstate Identification Index (III) files. DCI shall send an invoice to the requesting agency to collect these fees.

(d) The access agreement shall be signed by the requesting agency's head, and returned to DCI.

(e) The agency's terminal, if applicable, shall receive the capability to use the purpose code "E" in the purpose field of the North Carolina CCH inquiry screens for employment or licensing once the agency head has signed the access agreement and returned it to DCI. Once an agency has received this capability, it shall use the purpose code "E", the proper two character code, and recipient of the record's name. A log of all primary and any secondary dissemination must also be kept for one year on all responses received from this type of inquiry.

(f) Criminal justice agencies may also gain access by submission of non-criminal justice applicant fingerprint cards. Approval must be obtained pursuant to the procedure in Paragraph (a) of this Rule. One applicant fingerprint card must be submitted on each individual. The fingerprint card must contain the following information on the applicant in order to be processed by DCI and the FBI:

(1) complete name;
(2) date of birth;
(3) race;
(4) sex;
(5) reason fingerprinted to include the N.C.G.S. or local ordinance number;
(6) position applied for;
(7) the licensing or employing agency; and
(8) a set of legible fingerprint impressions.

DCI shall return the letter of fulfillment to the submitting agency indicating the existence or absence of a criminal record.

(g) Requests from non-criminal justice agencies or individuals to use criminal history information maintained by DCI for licensing and employment purposes shall be treated as a fee for service request pursuant to G.S. 114-19.1 or any other applicable statute. The process for approval for non-criminal justice agencies or individuals shall be the same process as in Paragraph (a) of this Rule.

(h) Upon being approved, the requesting agency shall submit its requests to the North Carolina State Bureau of Investigation, Criminal Information and Identification Section, Special Processing Unit, 3320 Garner Road, Raleigh, North Carolina 27626. Each request shall include a fee of ten dollars ($10.00) for a name-only check, fourteen dollars ($14.00) for a state-only fingerprint based check, or thirty-eight dollars ($38.00) for a state and national fingerprint based check (if applicable) in the form of a certified cashier's check, money order, or direct billing.

(i) Criminal history record information accessible pursuant to this Rule shall be North Carolina criminal history record information, and FBI III information if permitted by statute.

History Note: *Authority G.S. 114-10; 114-10.1; 114-19.1.*
Eff. May 1, 2014.

12 NCAC 04I .0406 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0406 RESTRICTIVE USE OF CCH FOR EMPLOYMENT PURPOSES

(a) Use of computerized criminal history information maintained by the CIIS for licensing permits or non-criminal justice employment purposes shall be authorized only for those criminal justice and non-criminal justice agencies who have complied with Rule .0405 of this Section.

(b) The following requirements and restrictions are applicable to all agencies who have received approval to use computerized criminal history information for licensing, permits, or non-criminal justice employment purposes. Each such agency is responsible for their implementation:

(1) computerized criminal history information obtained shall not be used or disseminated for any other purpose;

(2) computerized criminal history information obtained shall not be released to or reviewed by anyone other than the agencies authorized by CIIS;

(3) the only data in the computerized criminal history files which may be used in an agency's determination of issuing or denying a license, permit or employment are those crimes stipulated in the referenced ordinance or statutory authority as grounds for disqualification. All criminal history arrest information held by CIIS shall be released regardless of disposition status. Each agency is responsible for reviewing each statutory authority and knowing what data may be used and what data shall not be used for grounds in denying or issuing a particular license or permit for employment;

(4) prior to denial of a license, permit, or employment due to data contained in a computerized criminal history record, a fingerprint card of the applicant shall be submitted to CIIS for verification that the record belongs to the applicant;

(5) if the information in the record is used to disqualify an applicant, the official making the determination of suitability for licensing or employment shall provide the applicant the opportunity to correct, complete, or challenge the accuracy of the information contained in the record. The applicant must be afforded a reasonable time to correct, complete or to decline to correct or complete the information. An applicant shall not be presumed to be guilty of any charge/arrest for which there is no final disposition stated on the record or otherwise determined. Applicants wishing to correct, complete or otherwise challenge a record must avail themselves of the procedure set forth in 12 NCAC 04I .0404 (c).

(c) A "no-record" response on a computerized criminal history inquiry does not necessarily mean that the individual does not have a record. If the requesting agency desires a more complete check on an applicant, a fingerprint card of the applicant shall be submitted to DCI.

History Note: *Authority G.S. 114-10; 114-10.1; 114-19.1.*
Eff. May 1, 2014.

12 NCAC 04I .0407 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0407 RESEARCH USE AND ACCESS OF CCH RECORDS

(a) Researchers who wish to use criminal justice information maintained by CIIS shall first submit to the North Carolina CJIS System Officer (CSO) a completed research design that guarantees protection of security and privacy. Authorization to use computerized criminal history records shall be given after the CSO has approved the research design.

(b) In making a determination to approve the submitted research design, the CSO must ensure that:

(1) an individual's right to privacy will not be violated by the research program;

(2) the program is calculated to prevent injury or embarrassment to any individual;

(3) the results outweigh any disadvantages that are created for the North Carolina criminal justice system if the research information is provided;

(4) the criminal justice community will benefit from the research and use; and

(5) the requestor is responsible for cost.

(c) For purposes of this Rule, a researcher is defined as a non-criminal justice or private agency or a criminal justice agency wishing to access criminal history data for a statistical purpose.

History Note: *Authority G.S. 114-10; 114-10.1; 114-19.1.*
Eff. May 1, 2014.

12 NCAC 04I .0408 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0408 LIMITATION REQUIREMENTS

Research designs must preserve the anonymity of all subjects. The following requirements are applicable to all such programs of research and each criminal justice agency or researcher is responsible for their implementation:

(1) Computerized criminal history records furnished for purposes of any program of research shall not be used to the detriment of the person(s) to whom such information relates.

(2) Criminal history records furnished for purposes of any program of research shall not be used for any other purpose; nor may such information be used for any program of research other than that authorized by the North Carolina CJIS System Officer (CSO).

(3) Each researcher or anyone having access to the computerized criminal history shall, prior to having such access, sign a Disclosure Agreement with the CSO incorporating the requirements of 12 NCAC 04H .0305.

(4) The authorization for access to computerized criminal history records shall assure that the criminal justice agency and CIIS have rights to monitor the program of research to assure compliance with this Rule. Such monitoring rights include the right of CIIS staff to audit and review such monitoring activities and also to pursue their own monitoring activities.

(5) CIIS and the criminal justice agency involved may examine and verify the data generated as a result of the program, and, if a material error or omission is found to have occurred, may order the data not be released for any purpose unless corrected to the satisfaction of the agency and CIIS.

History Note: *Authority G.S. 114-10; 114-10.1; 114-19.1.*
Eff. May 1, 2014.

12 NCAC 04I .0409 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0409 ACCESS TO CHRI BY ATTORNEYS

(a) An attorney must have entered in to a proceeding in accordance with G. S. 15A-141 in order to access CHRI. The attorney may have access to the CHRI of only the defendant he or she is representing.

(b) If, during a proceeding, an attorney desires CHRI of an individual involved in the proceeding other than the attorney's client, the attorney shall make a motion before the court indicating the desire for the CHRI.

(c) In order to maintain compliance with state and federal requirements an attorney shall disclose the purpose for any request of CHRI.

(d) CIIS shall provide a form to be utilized by any DCIN user when fulfilling a request for CHRI by an attorney. This form shall help ensure compliance with state and federal rules regarding access to and dissemination of CHRI.

(e) The attorney must fill out all applicable fields of the form and return it to the DCIN user to process the request. The attorney shall provide:

(1) the client's name;

(2) docket number for the matter;

(3) prosecutorial district in which the matter is being tried; and

(4) the next date on which the matter is being heard.

(f) The attorney may submit requests for CHRI only within the prosecutorial district of the District Attorney that is prosecuting the defendant(s). If a change of venue has been granted during a proceeding, this rule still applies, and the attorney must still seek the CHRI from the prosecutorial district within which the proceeding originated.

(g) Records of requests and dissemination to attorneys must be kept by the disseminating agency for a period of one year.

(h) Requests for North Carolina-only CHRI may be notarized in lieu of approval from the DA or ADA.

History Note: *Authority G.S. 114-10; 114-10.1; 15A-141.*
Eff. May 1, 2014.

12 NCAC 04I .0410 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0410 ACCESS TO CHRI IN CIVIL PROCEEDINGS

(a) Access to CHRI is permitted in civil domestic violence and civil stalking proceedings.

(b) Access to and dissemination of CHRI for civil proceedings in this Rule shall be done in accordance with Rules .0401 and .0402 of this Subchapter.

(c) Access to and dissemination of CHRI for any other type of civil proceeding is prohibited.

(d) Civil courts may be issued an Originating Agency Identifier (ORI) for the purposes of this Rule. The ORI issuance must be approved by the FBI and North Carolina's CJIS System Officer (CSO).

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0501 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0500 – REMOVAL OF CRIMINAL HISTORY RECORD INFORMATION

12 NCAC 04I .0501 EXPUNGEMENTS

Upon the receipt of a valid court ordered expungement, CIIS shall expunge the appropriate CHRI as directed by the court order. An electronic notification regarding the expungement shall be sent to the FBI for processing and all agencies that have inquired on the record within the past 90 days shall be advised of the court order.

History Note: *Authority G.S. 15A-145; 15A-146; 90-96; 90-113.14; 114.10; 114-10.1; 150B-19(5)b., e.*
Eff. May 1, 2014.

12 NCAC 04I .0601 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0600 – STATEWIDE AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

12 NCAC 04I .0601 STATEWIDE AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

(a) Agencies which meet the requirements of 12 NCAC 04H .0201(a) may access the North Carolina Statewide Automated Fingerprint Identification System for criminal justice purposes.

(b) The acronym used for the Statewide Automated Fingerprint Identification System shall be the SAFIS.

History Note: *Authority G.S. 15A-502; 114-10; 114-10.1; 114-16.*
Eff. May 1, 2014.

12 NCAC 04I .0602 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04I .0602 AVAILABLE DATA

(a) The following data is available through SAFIS and may be used to make comparisons and obtain CCH data:

(1) fingerprint images; and

(2) state identification number.

(b) When the state identification number is used to obtain CCH data, dissemination requirements outlined in Rule .0401(c) and (d) of this Subchapter must be followed.

History Note: *Authority G.S. 15A-502; 114-10; 114-10.1; 114-16.*
Eff. May 1, 2014.

12 NCAC 04I .0603 is adopted as published in 28:10 NC 1008 as follows:

12 NCAC 04I .0603 FINGERPRINTING OF CONVICTED SEX OFFENDERS

(a) Fingerprints submitted in accordance with G. S. 14 – 208.7 must contain the following information on the convicted sex offender in order to be processed by the SBI:

(1) ORI number;
(2) complete name;
(3) date of birth;
(4) race;
(5) sex;
(6) sex offender registration number (SRN); and
(8) a set of fingerprint impressions and palm prints if the agency is capable of capturing palm prints.

Submissions shall be made through the registering agency's LiveScan device.

(b) Fingerprints submitted to CIIS that do not contain all of the items in (a) shall not be accepted.

(c) The submitted fingerprint information shall be added to the North Carolina Sex Offender Registry and to SAFIS.

History Note: *Authority G.S. 114-10.*
Eff. May 1, 2014.

12 NCAC 04I .0701 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0700 – DIVISION OF MOTOR VEHICLE INFORMATION

12 NCAC 04I .0701 DISSEMINATION OF DIVISION OF MOTOR VEHCILES INFORMATION

(a) DMV information obtained from or through DCIN shall not be disseminated to anyone outside those agencies eligible under 12 NCAC 04H .0201(a) unless obtained for the following purposes:

(1) in the decision of issuing permits or licenses if statutory authority stipulates the non-issuance or denial of a permit or license to an individual who is a habitual violator of traffic laws or who has committed certain traffic offenses and those licensing purposes have been authorized by CIIS and the Attorney General's Office;

(2) by governmental agencies to evaluate prospective or current employees for positions involving the operation of publicly owned vehicles; or

(3) by a defendant's attorney of record in accordance with G.S. 15A-141.

(b) Each agency disseminating driver history information to a non-criminal justice agency for any of the purposes listed in Paragraph (a) shall maintain a log of dissemination for one year containing the following information:

(1) date of inquiry for obtaining driver's history;

(2) name of terminal operator;

(3) name of record subject;

(4) driver's license number;

(5) name of individual and agency requesting or receiving information; and

(6) purpose of inquiry.

(c) Driver history information obtained from or through DCIN shall not be released to the individual of the record.

(d) DMV information obtained for any purpose listed in Paragraph (a) of this Rule shall be used for only that official internal purpose and shall not be redisseminated or released for any other purpose.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04I .0801 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0800 - AUDITS

12 NCAC 04I .0801 AUDITS

(a) CIIS shall biennially audit criminal justice information entered, modified, cancelled, cleared and disseminated by DCIN users. Agencies subject to audit include all agencies that have direct or indirect access to information obtained through DCIN.

(b) CIIS shall send designated representatives to selected law enforcement and criminal justice agency sites to audit:

(1) criminal history usage and dissemination logs;

(2) NICS usage and dissemination logs;

(3) driver history dissemination logs;

(4) security safeguards and procedures adopted for the filing, storage, dissemination, or destruction of criminal history records;

(5) physical security of DCIN devices in accordance with the current FBI CJIS Security Policy;

(6) documentation establishing the accuracy, validity, and timeliness of the entry of records entered into NCIC wanted person, missing person, property, protection order, and DCIN and NCIC sex offender files;

(7) the technical security of devices and computer networks connected to DCIN in accordance with the current FBI CJIS Security Policy;

(8) user certification, status, and background screening;

(9) user agreements between the agency and North Carolina's CJIS System Agency (CSA);

(10) servicing agreements between agencies with DCIN devices and agencies without DCIN devices (when applicable);

(11) use of private contractors or governmental information technology professionals for information technology support along with the proper training and screening of those personnel; and

(12) control agreements between agencies and entities providing information technology support (when applicable).

(c) The audits shall be conducted to ensure that the agencies are complying with state and federal regulations, as well as federal and state statutes on security and privacy of criminal history record information.

(d) CIIS shall provide notice to the audited agency as to the findings of the audit. If discrepancies or deficiencies are discovered during the audit they shall be noted in the findings along with possible sanctions for any deficiencies or rule violations.

(e) If applicable, CIIS shall also biennially audit agencies' N-DEx access and usage. CIIS shall audit:

(1) network security;

(2) N-DEx transactions performed by agency personnel; and

(3) user certification and status

(f) Audits of N-DEx usage will occur concurrently with an agency's DCIN audit, and shall ensure compliance with state and federal regulations on security and privacy of criminal justice information contained within N-DEx.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04J .0101 is adopted as published in 28:10 NCR 1008 as follows:

SUBCHAPTER 4J - PENALTIES AND ADMINISTRATIVE HEARINGS

SECTION .0100 - DEFINITIONS AND PENALTY PROVISIONS

12 NCAC 04J .0101 DEFINITIONS

As used in this Subchapter:

(1) "Revocation of Certification" means a DCIN user's certification is canceled for a period not to exceed one year. At the end of the revocation period the user must attend the DCIN Module 1 certification class. Notification of the revocation shall be sent by DCI via certified mail to the DCIN user and the user's agency head.

(2) "Suspension of Certification" means a DCIN user is prohibited from operating a DCIN device for a period not to exceed 90 days. Notification of the suspension shall be sent by DCI via certified mail to the DCIN user's agency head and to the DCIN user. The agency shall be audited within 90 days of reinstatement of a user's certification.

(3) "Suspension of Services" means an agency's direct access to DCIN is suspended for a period not to exceed two weeks after the North Carolina CJIS System Officer's (CSO) finding of fault, and the agency head must then appear before the CSO to respond to the cited violation. This suspension may be limited to certain files or may include a complete suspension of services, depending on the administrative procedure violated. The agency is subject to a re-audit after 90 days of reinstatement. Further violations of the same regulation, within two years from the date of the suspension, or failure to appear before the CSO to respond to the cited violation is grounds to cancel the user agreement with the agency.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04J .0102 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04J .0102 SANCTIONS FOR VIOLATIONS BY INDIVIDUALS

When any certified DCIN user is found to have knowingly and willfully violated any provision of these Rules, DCI may take action to correct the violation and to ensure the violation does not re-occur, to include, but not limited to, the following:

(1) issuing an oral warning and a request for compliance;
(2) issuing a written warning and a request for compliance;
(3) suspending the DCIN user's certification; or
(4) revoking the DCIN user's certification.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04J .0103 is adopted as published in 28:10 NCR 1008 as follows:

12 NCAC 04J .0103 SANCTIONS FOR VIOLATIONS BY AGENCIES

When any agency who has entered in to an agreement in accordance with 12 NCAC 04H .0301 is found to have knowingly and willfully violated any provision of these Rules, DCI may take action to correct the violation and to ensure the violation does not re-occur, to include, but not limited to, the following:

(1) issuing an oral warning and a request for compliance;

(2) issuing a written warning and a request for compliance; or

(3) suspending services to the violating agency.

History Note: *Authority G.S. 114-10; 114-10.1.*
Eff. May 1, 2014.

12 NCAC 04J .0201 is adopted as published in 28:10 NCR 1008 as follows:

SECTION .0200 - APPEALS

12 NCAC 04J .0201 NOTICE OF VIOLATION

DCI shall send a written notice via certified mail to the offending agency or employee when DCI has determined that a violation of a DCI rule has occurred. The notice shall inform the party of appeal rights and shall also contain the citation of the rule alleged to have been violated.

History Note: *Authority G.S. 114-10; 114-10.1; 150B-3(b); 150B-23(f).*
Eff. May 1, 2014.