

SUBCHAPTER 18B – SECURITY AND PRIVACY

SECTION .0100 – SECURITY AT DCIN DEVICE SITES

14B NCAC 18B .0101 SECURITY OF DCIN DEVICES

Agencies 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0101 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .0102 OFFICIAL USE OF DCIN

- (a) DCIN shall be used for 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0102 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 14B NCAC 18A .0401(c).

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

*Transferred and Recodified from 14B NCAC 04I .0103 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 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.
- (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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0104 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

SECTION .0200 – RESTRICTED AND RESTRICTED FILES

14B NCAC 18B .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 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0201 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 - 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0202 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0203 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0204 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

SECTION .0300 – SUBMISSION OF DATA FOR CRIMINAL HISTORY RECORDS

14B NCAC 18B .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 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.

(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.

(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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0301 Eff. November 1, 2015;*

Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.

14B NCAC 18B .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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0302 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0303 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

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

14B NCAC 18B .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 14B NCAC 18A .0201(a) except as provided by Rules .0403, .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 14B NCAC 18A .0201(a) shall be denied access and referred to the North Carolina 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.
- (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 14B NCAC 18B .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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0401 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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" means a code that conveys the reason for which an inquiry is made.

*History Note: Authority G.S. 114-10; 114-10.1;
Eff. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0402 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 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) of this Rule in an electronic method to CIIS for processing. Any fingerprints and associated information not meeting the requirements in Paragraph (a) of this Rule 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0403 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 shall be submitted only to the individual. Copies of the response 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0404 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 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).

(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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0405 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 Rule .0404(c) of this Section.

(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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0406 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0407 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

14B NCAC 18B .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 Rule 18A .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. August 1, 2014;
 Transferred and Recodified from 12 NCAC 04I .0408 Eff. November 1, 2015;
 Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.

14B NCAC 18B .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 District Attorney.

History Note: Authority G.S. 114-10; 114-10.1; 15A-141;
 Eff. August 1, 2014;
 Transferred and Recodified from 12 NCAC 04I .0409 Eff. November 1, 2015;
 Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.

14B NCAC 18B .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 Section.
- (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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0410 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.

SECTION .0500 – REMOVAL OF CRIMINAL HISTORY RECORD INFORMATION

14B NCAC 18B .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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0501 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.

SECTION .0600 – STATEWIDE AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

14B NCAC 18B .0601 STATEWIDE AUTOMATED FINGERPRINT IDENTIFICATION SYSTEM

(a) Agencies which meet the requirements of 14B NCAC 18A .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 SAFIS.

History Note: Authority G.S. 15A-502; 114-10; 114-10.1; 114-16;
Eff. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0601 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.

14B NCAC 18B .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 of this Subchapter must be followed.

History Note: Authority G.S. 15A-502; 114-10; 114-10.1; 114-16;
Eff. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0602 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.

14B NCAC 18B .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 Paragraph (a) of this Rule 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0603 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

SECTION .0700 – DIVISION OF MOTOR VEHICLE INFORMATION

14B NCAC 18B .0701 DISSEMINATION OF DIVISION OF MOTOR VEHICLES INFORMATION

(a) DMV information obtained from or through DCIN shall not be disseminated to anyone outside those agencies eligible under 14B NCAC 18A .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 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 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0701 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*

SECTION .0800 - AUDITS

14B NCAC 18B .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 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 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. August 1, 2014;
Transferred and Recodified from 12 NCAC 04I .0801 Eff. November 1, 2015;
Pursuant to G.S. 150B-21.3A, rule is necessary without substantive public interest Eff. October 4, 2016.*