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.