



Compliance Unit

Criminal Information & Identification Section
North Carolina State Bureau of Investigation

2025-2027 Agency Audit Guide

Audit Questions

For any audit related questions please contact the auditor assigned to your agency. Their contact information will be listed on your audit worksheet or you may email

ARAHelp@ncsbi.gov.

Concealed Handgun Permit Questions

CHPHelp@ncsbi.gov

Validation or EVOLVE Questions

EVOLVEHelp@ncsbi.gov

E Purpose Code Questions

AIUHelp@ncsbi.gov

ORI Questions

ORI@ncsbi.gov

Security Awareness Training Questions

SATHelp@ncsbi.gov

Available in Omnixx under Links->Compliance->Security Awareness->Security Awareness Training

DCIN Error Reporting Instructions

Available in Omnixx under Links->Compliance->Error Reporting Notice Requirement

Audit Process

Pre-Audit

During the Pre-Audit phase the auditor will contact the agency to verify all contact information. This information is used to ensure that the agency will receive the audit packet and to validate the NCIC and NLETS ORI files. They will also prepare the forms needed by the agency and will send the prepared audit packet to the agency head and TAC by email.

Audit

During the month that the agency is assigned the audit they will be responsible for completing the worksheet and submitting all requested documents. All agencies will have until the **last calendar day of the month of their audit** to submit all documents or the agency may be found Non-Compliant for the missing information. (For Example: An agency whose audit is scheduled for January of 2022 will have until 11:59pm on January 31, 2022 to submit all requested documents)

The worksheet and all requested documents are to be completed electronically or scanned and submitted by email. This will allow for backups of all files to be stored and to ensure that all deadlines are met.

Post-Audit

Once the Compliance Unit has received the worksheet and all requested documents they will begin evaluating the agency. Once the audit has been processed it will be reviewed for completeness and the results will be sent by email to the agency head and TAC.

Compliant Agencies

If the agency is Compliant the audit file will be closed once the results are received by the agency.

Non-Compliant Agencies

If the agency is Non-Compliant they will need to respond to all sections marked Non-Compliant. The response should be typed on agency letterhead and signed by the agency head. It will need to address each of the four questions below for each section marked Non-Compliant.

1. What violation was found?
2. Who committed the violation? (include the DCIN User ID if applicable)
3. What has been done to address these specific issues?
4. What corrections has your agency implemented to ensure that this issue will not reoccur?

Mail your response to:

North Carolina State Bureau of Investigation
Criminal Information and Identification Section
Attn: Compliance Unit Supervisor
3320 Garner Road
Raleigh, NC 27610

****Please see following page for information on sanctions****

Penalties – Definitions and Provisions

14B NCAC 18C .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 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.

14B NCAC 18C .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.

14B NCAC 18C .0103 Sanctions for Violations by Agencies

When any agency who has entered into an agreement in accordance with 14B NCAC 18A .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.

Agency Audit Worksheet

Each agency receiving an audit will receive an Audit Worksheet (CIIS Form 79). This worksheet must be completed electronically and submitted by email to ARAHelp@ncsbi.gov. On the worksheet are five sections of yes/no questions, a list for active servicing agreements, lists for non-sworn DCIN Users, and a section listing the documents that need to be submitted.

Requested Documents

Technical Security Audit

1. If your agency has any devices that connect to the DCIN you will be required to complete a Technical Security Audit (TSA). This document is required by the NC State Bureau of Investigation Information Technology Division (ITD) to ensure that all technical security requirements are met by the agency.
2. Answer all questions on the TSA and ensure that you include a diagram meeting the requirements listed in the document.
3. The SBI Compliance Unit only collects the TSA documents and forwards them to ITD for further review. All questions on how to complete the TSA should be directed to the ITD helpdesk using the contact information listed on the TSA.
4. Certain state and federal agencies are not required to submit separate TSAs for their different locations so one may not be included in your audit packet. If the box is checked on your worksheet you will need to complete and submit the TSA.

Security Awareness Training

1. If anyone at your agency has access to DCIN devices/printouts or criminal history information, those individuals are required to complete Security Awareness Training.
2. The North Carolina State Bureau of Investigation has implemented **two** online programs for Security Awareness Training. The “Getting Started” guide for TACs has been placed in Omnixx > Force > Links > Compliance > Security Awareness > Security Awareness Training. It is also in Omnixx Trainer.

There are two programs, **CJIS Online** and **nexTEST**. All DCI certified users will use nexTEST. Non-users/personnel/vendors with possible access to criminal history information will use CJIS Online. The compliance unit will be maintaining both programs as well as the help mailbox. Tutorials for each have been placed on the Launch Pad under CJIS Training. All questions should be forwarded to SATHelp@ncsbi.gov. **You do NOT need to submit anything for training. This is completed through the online Security Awareness Training programs.**

3. **Note:** Your agency **nexTEST** report is audited against your DCI User Summary. These lists should mirror each other. Any current employees no longer actively DCI certified should be disabled and removed from your DCI User Summary. If those individuals are still employed, they must complete the Security Awareness Training in CJIS Online.

Active Non-Sworn DCIN Users (Page 2 of Audit Worksheet)

1. List **ONLY** active non-sworn employees that are USERS of the DCI Network hired on or since the date listed. This list will be used to verify that fingerprints have been submitted to the SBI in the time frame required.
 - a. Fingerprints should be submitted, and results received by your agency **PRIOR** to the employee attending DCI class.
 - b. New employees that come to your agency and are already DCI certified should be fingerprinted and results received by your agency within 30 days of hire.
 - c. Results must be agency specific (meaning that the fingerprint card should be submitted under agency name & ORI number).
 - d. Correctional Facilities must submit a transaction viewer for each user listed. See Audit Guide page 7 for example transaction viewer.

Hot File Documentation

1. For **all** categories, submit information that supports the NCIC entry, including incident reports, summaries, file documentation explaining late entries, criminal history/DMV inquiries, documentation showing it was cleared and when, etc. For **protection order files** also include the full current order, the ex parte, and any renewals. For **wanted person files** also include a copy of the warrant.
 - a. This does not include screen shots of your DCI screens.
 - b. Submit even if the record is cleared.
 - c. No documents for Sex Offenders should be submitted as the records are reviewed in house.
 - d. Submit each requested hot file as a separate PDF labeled by Name or NIC.

NICS Documentation (SO Only)

1. Submit concealed handgun permit application requested.
2. Submit each requested file as a separate PDF by Applicant Name.

Audit Worksheet Questions

The following sections will address some questions that may need further explanation or examples. If you have any questions about how you should answer for your specific agency, please contact the auditor assigned to your audit.

Section A – Use and Access of Criminal History Record Information

1. Does your agency disseminate criminal history record information to anyone not employed by your agency?

If your agency gives CHRI to **anyone** that is not directly employed by your agency then answer **Yes** to this question and then answer questions 1A-1E.

Note – Does not include defense attorney request. Refer to question #6 on the Audit Worksheet.

1D. Does your agency maintain a log consisting of the name and agency of the recipient for CHRI secondary dissemination?

This log is separate from the automated CCH log.

2. Does your agency's TAC or designee conduct a review of the automated CCH/NICS logs?

If you answer **Yes** to this question then answer questions 2A-2C.

2C. Does your agency maintain the documentation necessary to verify that CHRI is obtained for authorized purposes for at least one year?

For example: applications for employment, signed request forms for investigations, incident reports, etc.

3. Does your agency issue Concealed Handgun Permits (Sheriff's Offices ONLY)?

This question does not apply to Correctional Facilities.

3B. Does your agency perform QNP (and QNR when necessary) transactions for each applicant?

A QNP must be run on all gun permit applicants. If there is a hit that needs further information, the QNR screen must be used.

Section B – Division of Motor Vehicles Information

5. Does your agency use DMV information for authorized non-criminal justice purposes?

If your agency uses DMV Driver History information for the reasons below answer **Yes** to this question and answer questions 5A and 5B:

- License and/or permits related to a local ordinance or state statute
- Operation of publicly owned vehicles
- Does **not** include Defense Attorney requests

5B. Does your agency maintain a log of driver history information that is disseminated for at least one year?

Driver History dissemination information must be maintained for a minimum of one (1) year for approved non-criminal justice purposes. This could be in the form of an agency created spreadsheet but must contain the following information:

- Date of inquiry
- Name of Terminal Operator
- Name of record subject
- Driver's license number
- Name of individual and agency requesting or receiving information
- Purpose of inquiry

Example:

[illegible]

Section C – Security – This Now includes Automated License Plate Reader Vendors.

10. Do all employees and IT personnel that have access to DCIN information complete Security Awareness Training prior to CJIS access and every year thereafter?

The Security Awareness Training information is available in Omnixx > Force > Links > Compliance > Security Awareness > Security Awareness Training and under Omnixx Trainer. There are two programs, CJIS Online and nexTEST. All DCI users will use nexTEST. Non-users and vendors will use CJIS Online.

The Security Awareness Training is available at <https://evolve.ncdci.gov/>.

11. Has your agency submitted fingerprints on all certified DCIN Users and/or IT staff/vendors that have access to DCIN devices to the SBI for a state and national background check?

This includes employees of the agency, other governmental employees that do not directly report to the agency (city/county IT departments), or a private vendor (ALEN, Southern Software, OSSl, VC3, etc.).

The IT Vendor only needs to be fingerprinted if they service/access the equipment; not if they only provide software.

Access to DCI devices includes any work done directly or remotely on DCI terminals, DCI mobiles, or your message switch. The work does not have to specifically relate to DCI. If the device contains DCI, it is included.

Agency/City/County IT personnel must complete a fingerprint-based background check within 30 days of DCI access. Vendor IT personnel must complete a fingerprint-based background check PRIOR to access to any device that houses/contains DCI. Results must be agency specific (meaning that the fingerprint card should be submitted under agency name & ORI number).

This question should be “not applicable” for federal agencies or those agencies with only sworn personnel and no IT support.

11A. Does your agency have a copy of a “Letter of Fulfillment” on file for all certified DCIN Users, and/or IT staff/vendors showing the result of the state and national fingerprint-based background checks?

Letters of Fulfillment have been sent out for fingerprint background check responses since 2008. Anyone that was fingerprinted after 2008 should have a letter of fulfillment on file at your agency. The letter of fulfillment must be addressed to your agency (agency specific). A letter of fulfillment from a previous employer will not be accepted. If they were fingerprinted before 2008 you should have a copy of the fingerprint card stamped with “AFIS No Record” on file. If either of these circumstances apply, answer **Yes** to this question.

Correctional facilities should have “transaction viewers” instead of the fulfillment letter. If you have the transaction viewers, answer **Yes** to this question.

Examples:

Letter of Fulfillment



NORTH CAROLINA
STATE BUREAU OF INVESTIGATION
DEPARTMENT OF JUSTICE

3320 GARNER ROAD
RALEIGH, NC 27626
(919) 866-4500
FAX: (919) 866-4623

SEPTEMBER 25, 2012



TO: RICH COOPER, ARMYCORP GENERAL

FROM: GREGORY S. MCLEOD, DIRECTOR

REFERENCE: Fingerprint check of DOE, JOHN JOE, 01/01/2012

A search of the North Carolina fingerprint database was conducted for your agency pursuant to the submission of the fingerprint card bearing the name DOE, JOHN JOE. If allowed by your governing law and requested in your submission, a search of the national fingerprint database was also conducted. Based on the fingerprint search, NO CRIMINAL HISTORY RECORD was located in the files of the State Bureau of Investigation or the Federal Bureau of Investigation, if applicable.

Your requested fingerprint-based search includes a search of the criminal history records maintained by the SBI and the FBI (if requested). It is important to know that it is possible that a fingerprint card associated with an inmate may not be in file with the SBI or the FBI. This may occur if the arresting agency fails to submit the fingerprints or the fingerprints may have been rejected due to poor quality. Consequently, a portion of criminal records maintained by the local courts of justice may not be available at the state or national level. Also, this criminal record search does not include a search of fingerprint-based records maintained by other states which have not been submitted to the FBI.

Under no circumstances shall the criminal record information obtained from the FBI or SBI be released to or reviewed by anyone other than the designated officials of your agency. Please direct any questions to (919) 862-4509, extension 4266.

Criminal Information and Identification Section

Transaction Viewer

Field	Value
Type Of Transaction	SRE
Date	10/10/2010
Priority	4
Destination Agency	NO RECORD
Originating Agency	
Transaction Control Number	
Transaction Control Reference	
Name Scanning Resolution	00.00
Nominal Transmitting Resolution	00.00
Field	
Logical Record Length	0000
Image Designation Character	00
Attention Indicator	
Send Copy To Record	
Originating Agency Case Number	
FBI Number	
State Identification Number	
Name	
Employer And Address	DOC WESTERN REG. EMP. OFFICE, 214 WEST JONES ST., RALEIGH, NC 27628
Occupation	
Residence Of Person Fingerprinted	
Search Results Finding	1
Action To Be Taken	
Controlling Agency Identifier Record	
Controlling Agency Identifier	
Electronic Rap Sheet	
SwiftRecordNumber	
Treat As Adult	

Cancel Complete Next

Section D – Agreements

12. Does your agency have a copy of a User Agreement signed by your current agency head?

If you have a copy signed by both your current agency head and by the current SBI representative, then answer **Yes** to this question.

Criminal Information and Identification Section
Compliance Unit
PO Box 29000
Raleigh, NC 27609
(919) 852-4500

Date: 1/14/2013

USER AGREEMENT CERTIFICATION

AGENCY: Test Agency 1
ORI: NC0000001
COUNTY: Wake
DISTRICT: 4
AGENCY HEAD: John Doe
AGENCY TAC: Jane Smith

INSTRUCTIONS:

1. Read, review and understand the requirements outlined in the attached User Agreement.
2. Sign this Certification.
3. Return this Certification to:
NC State Bureau of Investigation
Criminal Information and Identification Section
Compliance Unit
PO Box 29000
Raleigh, NC 27609
4. After review by the SBI, a completed agreement will be returned to your agency by email.

If you have any questions contact: Mike Vess Email: mvess@ncdoj.gov

Test Agency 1
I certify that I have read and understand the requirements for this agreement, and I will uphold this agreement. I further certify that I am the duly authorized head of this agency.
John Doe
Signature of agency head Date

North Carolina State Bureau of Investigation
I certify that I am the duly authorized representative of the North Carolina State Bureau of Investigation (SBI), Criminal Information and Identification Section and I will uphold this agreement.
Wendy L. Brinkley
Special Agent in Charge, FBI CAS Systems Officer (CSO)
Signature Date

CIS-6 Rev. 01/03/2013

14. Are your agency's devices serviced by IT staff employed by a municipality or county government who do not report directly to the agency?

If IT personnel do not report directly to the agency, and the agency head does not have the ability to hire/fire or discipline them then answer **Yes** to this question and answer question 15A.

This typically includes city and county IT personnel.

14A. Does your agency have a copy of a Management Control Agreement on file signed by your current agency head and a representative of the municipal or county government IT department?

This agreement is between the agency head and the department head of the municipal or county government IT department. An example is provided in the CJIS Security Policy available in Omnixx under Links->IT Assistance->CJIS Security Policy. This was previously referred to as a Memorandum of Agreement (MOA), but in order to match the CJIS Security Policy it is now referred to as a Management Control Agreement (MCA).

15. Are your agency's devices serviced by IT staff employed by a private contractor?

If your IT services are provided by a contracted private vendor, such as ALEN, OSSI, Southern Software, VC3, etc, then you will need to answer Yes to this question and answer questions 16A-16B.

The IT Vendor needs to be fingerprinted if they service the equipment, not if they only provide software.

15A. Does your agency have a copy of a Private Contractor User Agreement on file signed by your current agency head and a representative of the private contractor?

A Private Contractor User Agreement should be similar in format to the Management Control Agreement shown above. This was previously referred to as a Memorandum of Agreement (MOA), but in order to match the CJIS Security Policy it is now referred to as a Private Contractor User Agreement (PCUA).

15B. Does your agency have a copy of a signed CJIS Security Addendum for each employee of the private contractor that has access to your agency's DCIN devices?

The CJIS Security Addendum can be found in Omnixx under Links > IT Assistance > CJIS Security Policy.

Section E – NCIC Record Policies (Hot Files)

16. Does your agency have a procedure established for performing second party checks?

If your agency has the capability of issuing warrants or entering other records in NCIC you are required to have a policy for performing second party checks. A second party check is when someone performs a check on a NCIC entry that was made by your agency or by a servicing agency to ensure it is entered accurately. This second party check should be documented by signing or initialing a printout of a query performed on the completed NCIC entry. For serviced agencies the second party check can be performed by either the agency that requested the entry, or by the agency that entered it. Second party checks should be covered in your Servicing Agreement with the agency that enters your records.

17. Does your agency have a procedure for ensuring that hit confirmations of NCIC Record Entries (Hot Files) occur within the deadline established by the FBI?

NCIC Policy requires that all requests for a Hit Confirmation of an active record be responded to within the specified time of the request. Agencies that do not have DCIN terminals should have a policy established with their servicing agency in their Servicing Agreement to ensure they meet this requirement.

Communications Centers answer N/A to questions 16 and 17. Only the holder of the record should answer YES or NO.

Acknowledgement

Once all the questions on the worksheet have been answered by your agency representative, please type the name of the representative in the space provided on the acknowledgement page. This will serve as an electronic signature and acknowledges that all information provided is complete and accurate.

Submitting Audit Packet

Please submit the completed worksheet and requested documents electronically. Send an email to ARAHelp@ncsbi.gov with the following documents as an attachment (a list of acceptable file formats are in []):

1. Worksheet [.pdf]
2. (If Requested) Technical Security Audit [.pdf]
3. (If Requested) Hot Files [.pdf] **Please submit each hot file as a separate PDF doc labeled by Name or NIC.**
4. NICS Files (SO Only). **Please submit each NICS file as a separate PDF doc labeled by Name.**

If you are unable to add all attachments in a single email due to file size, you may send multiple emails.