

Terminal Agency Coordinator Manual



Criminal Information and Identification Section

TABLE OF CONTENTS	
Outline	
Introduction	
Purpose	3
What is a Terminal Agency Coordinator (TAC)?	3
Minimum Requirements for TAC Appointment	3
Function of the SBI/DCIN	
Legislative Authority	4
NCSBI – Criminal Information & Identification Section (CIIS)	4
Standards and Agreements	
Eligibility for Agency DCIN Access	4
Legal Agreements for Access	4-6
TAC Responsibilities	
TAC Administrative Duties	6-10
NCIC and DCIN Records Compliance	10
CCH Files Compliance	10
Dissemination of Information	10-11
System Security – Access, Use, and Dissemination	12
Training Coordinator	13-16
Audit Coordinator	16-17
Information and Assistance	
SEND and Functional Message Integrity	17
SBI Service Desk	17
Contact Us	18

Title:	Terminal Agency Coordinator Training
Purpose:	To present TAC's an overview of: - Legislative Authority - DCIN System Security - TAC Responsibilities - TAC Resources for Information and Assistance
Training Objectives:	At the end of this instruction, TAC's will be able to achieve the following objectives: 1. Define TAC & ATAC Responsibilities 2. Identify documents to assist with TAC duties 3. Explain the procedures that must be followed when there is a change in an agency head 4. Explain DCIN's policy on System Security 5. Explain the procedures that must be followed when performing a background check on a new user 6. Explain the audit process and the role as a TAC 7. Perform authorized functions in Omnixx Console to add and maintain users for your agency 8. Enroll students in DCIN certification classes
Hours:	Two (2)
Instructional Method:	Lecture/Discussion Hands On (if available)
Training Aids:	Computer Student Outline/Manual Omnixx Console and Trainer Manual Security Awareness Training Manuals North Carolina Administrative Code Title 14B Chapter 18 FBI CJIS Security Policy
Revised By:	Jessica Ward Criminal Information Training Specialist – Training Unit – SBI CIIS April 21, 2025; November 1, 2023
Revised By:	Patricia Viverette Criminal Information Training Specialist – Training Unit – SBI CIIS July 28, 2020
Revised By:	Patricia Viverette/Jeannie McBride Criminal Information Training Specialist – Training Unit – SBI CIIS February 2020; September 2019; June 2019; April 2016
Revised By:	Jeannie McBride/Patricia Viverette Criminal Information Training Specialist – Training Unit – SBI CIIS March 2015
Revised By:	Patricia Viverette Criminal Information Training Specialist – Training Unit – SBI CIIS April 2013

I. Introduction

A. Purpose

The purpose of this manual is to assist the individual within an agency who has been assigned as a Terminal Agency Coordinator (TAC). This manual contains an overview of the responsibilities of this individual but is not to be considered a comprehensive guide to fulfilling those duties. References have been made to the North Carolina Administrative Code (NCAC), the FBI's CJIS Security Policy, the Omnixx Console and Trainer Manual, and the Security Awareness Training Manuals. All of these resources contain current and complete information to support the TAC's duties and responsibilities.

B. What is a Terminal Agency Coordinator (TAC)?

Terminal Agency Coordinator is an individual designated by the agency head to act as a liaison between the agency and NCSBI staff regarding DCIN information as required by the FBI. The person assigned to this position is to ensure compliance with state and national regulations pertaining to the use of the criminal justice computer system (DCIN) and the other systems it accesses (NCIC, NLETS, etc.). Each agency having direct access to DCIN must appoint a Primary TAC and may appoint Assistant TACs (ATACs). There is no limit to the number of ATACs that can be appointed. The ATAC(s) are held to the same standards and requirements as the TAC and have the same technical rights.

1. The TAC should be an individual in the management structure of the agency who has sufficient authority to implement procedures and policies and who is authorized to cross agency section/unit boundaries.
2. The TAC should be knowledgeable of state, NCIC, and Nlets policies and procedures.
3. The TAC should be someone who can attribute adequate time and attention to performing the functions of the position and who is authorized to enforce regulatory compliance within the agency.
4. TAC responsibilities include:
 - a) Administrative Duties
 - b) NCIC and DCIN Records Compliance
 - c) CCH Files Compliance
 - d) Dissemination of Information
 - e) System Security
 - f) Training Coordinator
 - g) Audit Coordinator
 - h) Participate in the TAC Orientation training provided by the SBI.

NOTE: These areas will be discussed later in this manual.

C. Minimum Requirements for TAC Appointment

The TAC and ATAC must be certified in a minimum of DCIN Module 1 – General Inquiries but should be familiar with ALL DCIN modules utilized by their agency. The TAC must complete a TAC Orientation training provided by their SBI DCIN Training Specialist.

NOTE: For agencies with terminal access, a DCIN Module 2 – Criminal Record Inquiries certification is required. For NCIC record validations, a DCIN Module 3 – File Transactions certification is required.

II. Function of the SBI/DCIN

A. Legislative Authority

By the authority of North Carolina General Statutes 143B-902 through 143B-905, the Division of Criminal Information Network (DCIN) was established to provide for the collection, storage, and dissemination of information that will assist criminal justice and law enforcement agencies in the performance of their duties. These statutes gave the Attorney General the authority to adopt rules and regulations governing the types of information relating to the administration of criminal justice to be entered into the system, and who shall have access to such information. These rules are located in the North Carolina Administrative Code (NCAC), Title 14B, Subchapter 18. A copy of the NC Administrative Code can be found at <https://www.ncsbi.gov/omnixlinks> under Compliance.

B. NC State Bureau of Investigation – Criminal Information and Identification Section (CIIS)

1. The Criminal Information and Identification Section (CIIS) of the North Carolina State Bureau of Investigation falls under the Professional Standards Division and is North Carolina's central repository for Criminal History Record Information (CHRI). Specialized functions/units within this section provide critical analysis and coordination of this information.
<https://www.ncsbi.gov/Divisions/Criminal-Information-and-Identification>
2. See the last page of this manual for contact information for the various CIIS units.

III. Standards and Agreements

Due to the vast amount of information available through the DCIN System, the integrity, confidentiality, and proper use of the system is essential. To achieve these desired goals, the FBI and State have drafted and implemented standards and agreements to be conformed to by all users and the DCIN.

A. Eligibility for Agency DCIN Access

ACCESS - Eligibility for DCIN access is restricted to agencies authorized by the North Carolina State Bureau of Investigation, the National Crime Information Center and/or the International Justice and Public Safety Information Sharing Network. Authorized agencies are those that have obtained a valid ORI.

- a) Direct Access – DCIN accessible devices and the personnel who operate them must be under the direct management control of a criminal justice agency/board or an FBI-approved non-criminal justice agency. Management control criteria is specified in 14B NCAC 18A.0202. A User Agreement is required (discussed in next section).
- b) Non-Terminal Access – An agency with no DCIN accessible devices may gain access to DCIN through a criminal justice agency that has direct access. The agencies must enter into a Servicing Agreement (discussed in next section). Criteria for this is specified in 14B NCAC 18A.0203 and 18A.0302.

B. Legal Agreements for Access

1. USER AGREEMENT (UA)

- a) The current head of each agency with direct access to DCIN shall sign a User Agreement certifying that he/she has read and understood the agreement and requirements for security of the DCIN system.
- b) The User Agreement outlines managerial control, physical security, system discipline, data collection and storage, and the system access requirements.

- c) The User Agreement is e-mailed to the agency head and TAC. Once signed by the agency head, the original signature page must be returned by US mail to:
North Carolina State Bureau of Investigation
Criminal Information & Identification Section
ATTN: Compliance Unit
3320 Garner Road
P.O. Box 29500
Raleigh, NC 27626
- d) After the signature page is reviewed and signed by the SBI, it will be scanned into an electronic file by the Compliance Unit and then e-mailed back to the agency head and TAC.
- e) Agencies must maintain a copy of the signed User Agreement on file and make available for review during an audit.
- f) If the agency head changes, email ARAHelp@ncsbi.gov with the new agency head's name, email address, and phone number. They will create and send an updated copy.

2. SERVICING AGREEMENT (SA)

- a) Any agency providing indirect access to the DCIN to another agency shall enter into a Servicing Agreement with the recipient agency head.
- b) The Servicing Agreement shall cover all services your agency is to provide to the recipient agency. Servicing Agreements may be needed or requested for device and/or non-device agencies to provide continuous access to DCIN.
- c) Servicing agreements should be specific to the needs of the two agencies entering into the agreement; therefore, fillable, or blank copies are not available. Criteria is specified in 14B NCAC 18A.0302.
- d) The SA must be signed by both current agency heads and both agencies should maintain a copy of the Servicing Agreement. Send a copy to the Compliance Unit at ARAHelp@ncsbi.gov.
- e) Service Agreements will be reviewed during the audit process.

3. MANAGEMENT CONTROL AGREEMENT (MCA)

- a) A **city or county IT department**, sometimes referred to as a government non-criminal justice agency (NCJA), designated to perform criminal justice functions for the criminal justice agency shall be eligible for access to CJIS (Criminal Justice Information). See the current version of the CJIS Security Policy at <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>.
- b) The city or county IT department shall sign and execute a MCA with the criminal justice agency, which stipulates management control of the criminal justice function remains solely with the criminal justice agency.
- c) The MCA may be a separate document or included with the language of an inter-agency agreement. A sample MCA may be found in the CJIS Security Policy.
- d) This document must contain the signatures of the heads of both the criminal justice agency and the IT department, and clearly state the scope of service(s) being provided.
- e) If either of the signatories change, a new agreement must be completed with the new signatory(ies).
- f) These must be kept on file at both the criminal justice agency and the IT department and are subject to audit by the FBI and state.

4. PRIVATE CONTRACTOR USER AGREEMENT (PCUA)
- a) **Private contractors** who perform criminal justice functions shall meet the same training and certification criteria required by governmental agencies performing a similar function and shall be subject to the same extent of audit review as are local user agencies.
 - b) The PCUA should specifically identify the agency's purpose and scope of providing services for the administration of criminal justice.
 - c) Examples of a private contractor or vendor would be those companies that install and maintain: RMS software, CAD software, MDTs, LPRs, etc.
 - d) Each contractor employee who has access to and/or performs maintenance on any CJIS system (desktop or mobile DCIN) shall acknowledge and abide by all aspects of the CJIS Security Addendum via signing the certification page.
 - (1) CJIS SECURITY ADDENDUM CERTIFICATION
 - (a) Available in the Appendix section of the CJIS Security Policy. <https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center>
 - (b) NO changes can be made to the addendum.
 - (c) If a private company is contracted to provide services to more than one criminal justice agency, then a new certification form must be signed for each additional criminal justice agency.
 - (d) These signed forms must be kept on file at both the criminal justice agency and the private contractor company and are subject to audit by the FBI and state.
 - (e) City or County IT personnel are not required to sign the CJIS Security Addendum Certification.

IV. TAC Responsibilities

A. TAC Administrative Duties

1. ON-SITE EXPERT IN POLICY AND PROCEDURES
- Being assigned as the TAC for an agency, you must be familiar with all policies and procedures enforced by NCIC, Nlets, DCIN and your agency.
- a) The NCIC Operations Manual and the Technical and Operational Updates (TOUs) are available through Law Enforcement Enterprise Portal (LEEP) online. This manual and the TOUs are the policies and procedures enforced by NCIC. A link to LEEP registration can be found at <https://www.ncsbi.gov/omnixxlinks>.
 - b) The CJIS Security Policy is available in Omnixx Links under IT Assistance. This policy manual created and maintained by the FBI CJIS Division is a fluid manual with revisions as needed. The policies in this manual must be adhered to by each and every law enforcement and criminal justice agency nationwide for compliance.
 - c) The NC Administrative Code Title 14B Chapter 18 Sections A, B and C are the Codes that authorize the SBI and are used as a foundation for policies and procedures enforced in NC for the operation of the DCIN. It can be found in Omnixx Links under Compliance.
 - d) The Omnixx Console & Trainer Manual provides valuable information you will need to make use of the Omnixx Console and Trainer as efficiently as possible. This manual will also guide you through the steps necessary to maintain database records for users assigned to your agency. It can be found in Omnixx Links under Terminal Agency Coordinator.

- e) Security Awareness Training (SAT) is mandatory to ensure the confidentiality, integrity, and availability of CJIS data and systems throughout the user community.
 - (1) The CJIS Launch Pad houses the SAT programs and manuals.
<https://evolve.ncdci.gov/launchpad/index.pl>
 - (a) CJIS Training = Manuals
 - (b) NexTEST = SAT for DCI certified employees
 - (c) CJIS Online = SAT for all others with access to CJI (examples: administration, city/county IT personnel, private contractor IT personnel, maintenance/cleaning crews with unescorted access, etc.)
- f) Your agency must adopt written Standard Operating Procedures concerning the operation of DCIN as well as access to the information received through the DCIN.

2. SECURITY OF DCIN DEVICES

Agencies that have management control of a DCIN device shall institute controls for maintaining the sensitivity and confidentiality of all CJI as described in 14B NCAC 18B.0101.

3. DCIN ACCOUNT MANAGEMENT

- a) Agency TAC must ensure that DCIN users meet the following qualifications prior to access and/or registering for DCIN classes:
 - (1) United States citizen
 - (2) At least 18 years of age
 - (3) Completed a fingerprint-based background check under the management control agency AND
 - (a) Has NO felony convictions (ineligible)
 - (b) Has NO Class B misdemeanor convictions within the last 10 years of date of access request
 - (c) Does NOT have 2 or more Class B misdemeanor convictions at any time (ineligible)
 - (d) Has NO pending/outstanding criminal charges that would disqualify the applicant if convicted
- b) Changes in Users - In the event there is a change in your agency's user list, the TAC will make the following updates:
 - (1) For new users that have never been DCIN certified in North Carolina, the TAC must add the user in Omnixx Console. Instructions for this can be found in the Omnixx Console and Trainer Manual located in Omnixx Links under Terminal Agency Coordinator. [Omnixx Console and TrainerManual Link](#)
 - (2) For users transferring certification from another NC agency to your agency, the TAC must email his/her District Training Specialist to have the user moved in Console and copy SATHelp@ncsbi.gov to have the user moved in NexTEST.
 - (3) For users leaving an agency the TAC will DISABLE the user's current status and email their District Training Specialist so that the user can be moved to the inactive file. Copy SATHelp@ncsbi.gov to the email to have them removed from the agency's NexTEST list.

NOTE: You only disable their current status, and not the status of OFB and OT.

- (4) If a user has a legal name change, they may opt (not required) to update their DCIN user ID. The TAC must first run a “User Test History” report in Console on the current user ID. This report must be printed and retained by the TAC/agency. The TAC will then use the following form to request the change: [User ID Change Request Form Link](#)
 - c) Passwords – The TAC/ATAC is responsible for resetting DCIN passwords. See section IV.F.b.
 - d) Operator Sign-In/Sign-Out - Only one operator per device is allowed to log into the system at one time. Operator access is based on the User ID of the individual signing into the system. The certified operator must not leave an unattended terminal signed on. If the certified operator leaves the terminal area or ends a shift, he or she must sign out.
 - (1) The CJIS Security Policy, Section 5 states: Users shall directly initiate a session lock mechanism to prevent inadvertent viewing when a device is unattended. A session lock is not a substitute for logging out of the information system. An example of a session lock is a screen saver with a password.
 - (2) In the interest of officer safety, devices that are (1) part of a police vehicle, or (2) used to perform dispatch functions and located within a physically secure location, are exempt from this requirement.
 - (3) Unauthorized use of Operator Sign-In – Any agency personnel using a certified operator’s identifier other than their own to gain access to DCIN and violating any rule for the purpose of concealing their identity will be in violation of Administrative Procedures Subchapter 18B section .0402 of the NC Administrative Code Title 14B and will be subject to provisions of Subchapter 18C section .0102.
 - e) The agency shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures.
4. REPORT DCIN NON-COMPLIANCE ISSUES WITHIN THE AGENCY AND NON-DEVICE AGENCIES YOU MAY PROVIDE SERVICE
- a) To gather information, several options are available:
 - (1) DCIN Off Line Search - NC only, goes back 1 year, located in Omnixx Links under IT Assistance
 - (2) NCIC Off Line Search – National, goes back further than 1 year, brochure located in Omnixx Links under IT Assistance
 - (3) DMV Off Line Search (CJLEADS)
 - (4) Nlets Off Line Search (using NLQ and NFQ transactions)
 - b) Once your investigation is complete, mail a letter on agency letterhead within 30 calendar days of the date the agency initially received the complaint. The letter should detail the findings and corrective measures if applicable. The following four questions should be addressed if areas of non-compliance are found:
 - (5) What violation was found?
 - (6) Who committed the violation – include position/title if applicable?
 - (7) What has been done to address the issue?
 - (8) What steps or policies has your agency implemented to ensure this situation will not reoccur?
 - c) Send agency response letter to:
*North Carolina State Bureau of Investigation
Criminal Information & Identification Section
ATTN: Compliance Unit
PO Box 29500*

5. PRINT, REVIEW AND MAINTAIN ALL CCH/NICS LOGS (QCHL Logs)
 - a) Logs are created automatically in DCIN and used to comply with NCIC/DCIN rules regarding access and dissemination. QCHL log information is also covered in the DCIN Module 2 Criminal Record Inquiries Training Manual.
 - b) Logs must be obtained monthly for each DCIN terminal (in-house) device.
 - (1) A monthly summary log is available on the first day of the following month. A NICS log will only be returned if NICS transactions were performed.
 - (2) Logs must be printed, reviewed, and signed within 15 business days of the end of the month being reviewed. (Logs can also be stored electronically instead of printed.)
 - (3) Review includes: Checking transactions used, purpose codes, valid requestor, secondary dissemination, etc.
 - (4) Any discrepancies found during the review should be reported to the Compliance Unit via the online Error Reporting Form. It can be found in Omnixx Links under Compliance. [Error Reporting Form Link](#)
 - (5) If no CCH inquiries are run on a specific device, a log must still be printed or stored electronically.
 - c) Logs are available only for the previous eighteen months.
 - d) Maintain logs on file for one year.
 - e) QCHL Logs are addressed in the the DCIN Module 2 Training Manual.
6. NOTIFY SBI/CIIS OF UPDATES AND CHANGES TO AGENCY STAFF AND AGENCY INFORMATION
 - a) Agency Head Change – Email the Compliance Unit at ARAHelp@ncsbi.gov with the new agency head's information. They will update the User Agreement and send it to you. Update any Service Agreements you may have with other criminal justice agencies and email them also.
 - b) Changes in TAC Appointment – In the event the TAC or ATAC of an agency leaves the position, the online TAC Notification Form must be immediately completed. It can be found in Omnixx Links under Terminal Agency Coordinator. [TAC Notification Form Link](#)
 - (1) This form will allow the Training Specialist to assign appropriate authorizations and schedule TAC Orientation training if needed and prompt CIIS to make appropriate changes to the mailing list.
 - c) Change of Address, Phone/Fax Number, Agency Name, County – Email your District Training Specialist and the Compliance Unit at ARAHelp@ncsbi.gov.
 - (1) Update NCIC/NLETS ORI Information - The ORI files give users nationwide the capability to inquire upon any Originating Routing Identifier (ORI) to receive its translation and other information. Each agency nationwide is required to maintain accurate information in their ORI files.
 - (a) NCIC ORI file can be modified at any time to make corrections by using the Modify NCIC ORI Record (MO) transaction.
 - (b) To make corrections to your NLETS ORI file, email the Compliance Unit at ARAHelp@ncsbi.gov.
7. ATTEND TAC MEETINGS

To keep up with changes and updates, TACs and ATACs are encouraged to attend scheduled TAC Meetings in their district. Each District Training Specialist is responsible

for scheduling any needed TAC Meetings throughout the year. These meetings are important and necessary to provide users with information about system changes, enhancements, and problems. Training material will be provided for each meeting. The material will be posted to Omnixx Links under Terminal Agency Coordinator.

B. NCIC and DCIN Records Compliance

NCIC/DCIN Records are those entered into the system for the purposes of investigation and crime solving (i.e. Wanted Persons, Missing Persons, Stolen Vehicles, Stolen Guns, Protection Orders, etc.). This information is covered in the Module 3 – File Transactions training manual.

1. All records entered must have documentation to support the information included in the entry, including anything used to pack the record. This documentation may be kept in paper or electronic form but must be accessible 24/7/365 for hit confirmation purposes.
2. Copies of all transactions, entries, modifications, and hit confirmations should be maintained in the case files.
3. Second-party checks are required and must be documented in the case files.
4. Validations – Each month, the TAC (or their designee) will receive an email when there are records ready to be validated. The EVOLVE software is used to complete validations and is located on the CJIS Launch Pad under CJIS Validations.
<https://evolve.ncdci.gov/launchpad/index.pl>
 - a) An EVOLVE tutorial is available on the CJIS Launch Pad under CJIS Training. Detailed instructions can also be found in the DCIN Module 3 – File Transactions training manual.
 - b) For each record on the list, personnel must review all documentation included in the case file for completeness and accuracy. Attempts should be made to obtain new/additional information for each record, including performing new NCIC/DCIN transactions, contacting reporting parties, contacting the clerk of court, etc. All of this should be thoroughly documented in the case file.
 - c) Agencies must complete the validations prior to the due date to prevent a purge (deletion) of the records in NCIC/DCIN.

C. CCH Files Compliance

Access to criminal history record information obtained through DCIN, NCIC, or Nlets sources is restricted by federal and state regulations to authorized criminal justice agencies for criminal justice purposes on a “need to know” basis. Agencies with an ORI ending in the letter “P” are NOT authorized to receive criminal history information. TACs and ATACs should be knowledgeable about criminal history inquiries, including the proper transactions and purpose codes. Details on the rules and regulations can be found in the Module 2 – Criminal History Record Inquiries training manual. See section IV.A.5. for details on TAC responsibilities for the monthly QCHL logs.

D. Dissemination of Information

1. INFORMATION LIAISON – In this quickly paced technological age it becomes increasingly important to relay information in a timely and systematic manner. As the TAC for an agency, you will be made aware of various updates and changes and must make sure to forward that information to appropriate sections of your agency.
2. USER AGREEMENT – Disseminate as discussed in Section III.B.1 of this manual.

3. SERVICING AGREEMENTS – Disseminate as discussed in Section III.B.2 of this manual.
4. E-MAILS from District Training Specialists should be disseminated to those personnel within your agency that are affected by the information.
5. NEWSLETTERS – District Training Specialists will publish and forward Newsletters to TACs providing information regarding the DCIN computer system, other systems, and files to which it provides access. Many times, the newsletters contain information on DCIN/NCIC file changes, training available, changes in training material, or to simply reiterate important information for agencies concerning DCIN access, use, and dissemination.
 - a) Newsletters are classified law enforcement sensitive material.
 - b) It is the TAC's responsibility to disseminate to ALL appropriate agency and/or IT personnel. Newsletters can be disseminated by agency e-mail, secure bulletin boards, at roll calls, or other secure means of communication used by your agency.
 - c) All newsletters are posted in Omnixx Links.
6. MODULE TRAINING MANUALS – Each agency is responsible for providing an updated copy of the appropriate module training manual to each student attending class or preparing for re-certification testing.
 - a) Module Training Manuals are found in Omnixx Links under Training.
 - b) The Module Training Manual contains the material and exercises that will be covered during the appropriate classroom instruction.
7. SEND TRANSACTION – A SEND transaction is used to disseminate information to law enforcement and criminal justice agencies statewide using the DCIN. These messages should be disseminated to all appropriate personnel, in the form of a radio transmission if applicable, posted to a secure bulletin board, provided to a shift commander to disseminate at roll call, etc., i.e. Amber Alert/Missing Endangered Alert, Wanted/Missing person.

E. System Security – Access, Use and Dissemination

1. TERMINAL SECURITY – Agency heads that are responsible for management control shall institute controls for maintaining the sensitivity and confidentiality of DCIN information and for safeguarding the devices that access DCIN and CJIS information. Information may be found in the NC Administrative Code and the CJIS Security Policy that outlines the requirements for secure locations of terminals and devices.
 - a) The TAC is responsible for ensuring that all state and federal regulations are adhered to and the agency is in compliance with these rules and regulations.
 - b) Ensure all criminal history record information is kept in secure locations and is disseminated only for criminal justice purposes.
 - c) It is the responsibility of the TAC to notify the CIIS/Compliance Unit of any violations of these rules and regulations at any time they may occur.
2. REQUEST FOR DCIN INTERFACE – Requests for a DCIN interface or to request additional devices must be submitted in writing to the SBI ITD using the Terminal

Request form. This can be found in Omnixx Links under IT Assistance. VPN requests are made via the VPN Request link under IT Assistance in Omnixx Links.

3. EMPLOYEE SCREENING – A background investigation must be conducted on all employees assigned as DCIN operators, anyone with direct or indirect access to information obtained through the DCIN, or anyone with access to record storage areas, which shall include a state and national fingerprint search for a criminal record.
 - a) As of 2008, a copy of the SBI “Letter of Fulfillment” (fingerprint results) should be on file for any operator who was placed in the position of a certified operator and all personnel with direct access to records or record storage. Prior to 2008, a copy of the operator’s fingerprint card with a red “no record” stamp should be on file.
 - b) Sworn officers who are certified as DCIN operators should already have fingerprint results on file with your agency due to employment checks required for certified law enforcement officers.
 - c) All IT staff, regardless of sworn status or date of hire, must have fingerprint results on file. These results are agency specific and must be addressed to the agency using their service.
 - d) All private contractors and vendors that have access to CJIS data must also be fingerprinted for each agency they service. The results of the background check (“Letter of Fulfillment” from SBI) must be maintained at each agency they service and with the private company.
4. DCIN OPERATOR ACCESS – See requirements listed in section IV.A.3 of this manual.
5. SECURITY AWARENESS TRAINING – Security Awareness Training is required by the CJIS Security Policy and must be provided prior to appointment or assignment, and every year thereafter, to all personnel who have direct or indirect access to CJIS data.
 - a) For questions or help with the Security Awareness Training, email SATHelp@ncsbi.gov.
 - b) There are two (2) separate programs for Security Awareness Training. NexTEST is for DCIN certified employees only (direct access). CJIS Online is for employees with indirect access.
 - c) Training Manuals for both programs are located on the CJIS Launch Pad under CJIS Training. <https://evolve.ncdci.gov/launchpad/index.pl>
 - d) Documentation pertaining to the materials used and those employees which receive the training must be maintained in a current status.
 - e) Security Awareness Training documentation (log) is created in nexTEST and CJIS Online accounts once the user has completed the training and taken the test, so there is no need for a written log. The automated logs are subject to audit by the SBI and FBI.
6. LOCAL AGENCY SECURITY OFFICER (LASO) – Each agency with access to criminal justice information must designate someone as the LASO. This can be any member of the agency or IT provider that is able to effectively communicate regarding IT hardware, equipment, software, network connections, and IT policies/procedures. The TAC will coordinate with the agency LASO on technical security issues related to DCIN. Both the TAC and LASO may interact with the SBI’s Information Technology (IT) department. The following newsletter addresses the LASO requirement:
<https://www.ncsbi.gov/DCIN/Omnixx-Links/Newsletters/2021/2021-00003LASO2.aspx>.

F. Training Coordinator

1. MAINTAIN USERS IN OMNIXX CONSOLE

- a) User Identifier – The User ID is a unique identifier assigned to each certified operator. The User ID consists of the user's first name initial; last name up to 15 characters, and 4 digits which are assigned by user's agency. Do not use Social Security Number. ***The User ID cannot be modified once it has been created.*** If you enter an incorrect User ID, contact your Training Specialist to have it deleted from the system ***before*** you enroll the user in class. Then you may re-enter a correct User ID.
- b) Password – A password is a security code created and maintained by each certified operator, used to complete operator sign-in.
 - (1) The password must be 8-12 characters containing letters, numbers and at least one special character (! @ # \$ *). [Password Requirements Link](#)
 - (2) Passwords expire every 90 days and must be changed prior to that to maintain access.
 - (3) Passwords cannot be re-used within fifteen (15) password changes.
 - (4) The operator may change the password when logging into Omnixx by using both the current and new password fields.
 - (5) If an operator forgets his/her password they will be unable to sign onto the DCI Network. In order to re-establish the password, the operator must notify their TAC/ATAC, who can change the password in Console. Passwords being reset by TACs/ATACs must be done in ALL CAPS. Directions are located in the Omnixx Console and Trainer Manual.
- c) Operator Leaves Employment – Within 24 hours, the TAC will DISABLE the user's current status and email their District Training Specialist so that the user can be moved to the inactive file. Copy SATHelp@ncsbi.gov to the email to have them removed from the agency's NexTEST list.
NOTE: You only disable their current status; not the status of OFB and OT.
- d) Employee Screening – See section IV.A.3. of this manual.
- e) Certification of Operators - An operator who is attempting to achieve certification in Modules 1-7 for the first time, or whose certification has expired for more than 365 days, must attend the instruction classes.
 - (1) Within 120 days of being hired or assigned responsibilities as a DCIN operator, the employee must attend an SBI approved certification class. Certification is valid for and must be renewed every two years. An operator may re-certify 30 days prior to expiration and up to 365 days after his/her certification expiration date.
 - (2) Determine which module certification each user will need. CIIS supports a modular certification program. The intent of this program is to allow operators to be certified only in those modules the agency deems to be appropriate for that operator.
 - (3) Some certified operators may be employed by more than one agency. For example, an operator is employed by a Communications Center and also works part-time for a Sheriff's Office, the level of certification required may differ for each agency. The primary (full-time) employer will maintain the individual's certification records and is responsible for class enrollment and testing.
 - (a) An operator's certifications may only be maintained under one agency's ORI. This is normally the full-time agency, if applicable.

- (b) While DCIN certified, the operator may use their certification at any agency where they work either part-time or full time.

2. CLASS ENROLLMENT

DCIN classes are held each month at various locations throughout the state and virtually. Each District Training Specialist is responsible for scheduling these classes within his/her district based on certification needs.

- a) Instruction enrollment – Before a TAC can enroll a student into a certification class, the student must be listed under the agency ORI in Console. Also see employee screening requirements in section IV.A.3.
- b) Class Offerings – In-person classes are available for registration in Console. Virtual, or online, classes are available for registration in Omnixx Links under Training.

3. NEW DCIN OPERATOR ORIENTATION

It is the responsibility of the agency TAC to ensure new operators receive appropriate DCIN experience prior to attending module certification instruction. A new operator has up to 120 days to operate the device under the direct supervision of a certified operator prior to attending DCIN certification class.

- a) For students attending Module 1, the *Introduction & Overview – Local Agency Instruction* section of the Module 1 manual must be reviewed and completed prior to class attendance.
- b) Have them take the mandatory Security Awareness Training and test in NextTEST.
- c) Provide an overview of DCIN, including instruction on the various keyboard functions used to operate the system.
- d) Provide a full exploration of the Force environment. This should include investigating the menu Bar, other components of the Force environment, Form Help, Field Help, Quick Keys, and Saved Workspace used by your agency.
- e) Provide a full exploration of the MDT (Mobile Data Terminal) environment (if applicable). This should include investigation of the menu, folders and other components of the MDT system as they vary depending on the software and version that is being used.
- f) New users should be allowed to practice **(under direct supervision)** making inquiries, based on the level of access this operator will receive.

NOTE: CCH inquiries and File entries should be limited to actual inquiries/entries, if available. Never use yourself, the new employee, or any other person for CCH/File Transaction training purposes.

- g) Provide an explanation of your departmental policies and procedures dealing with how hit confirmations and validations are performed, CCH & NICS logs are printed, reviewed, and stored at your agency, and any other internal logs or procedures used by your agency. Review your departmental policy for performing driver's or criminal histories for non-criminal justice purposes as supported by CIIS regulations (i.e. Defense Attorney access).
- h) If applicable, allow the student to perform hot file transactions such as entering, modifying, supplementing, and clearing actual records for your agency. The student does not have the authorization to perform these transactions, therefore, the student must work under the direct supervision of the certified operator whose sign-on they are using. If no records are available for entry, the student may enter a practice record, ensuring the notation **'TEST RECORD'** is entered in both the OCA and MIS fields. Any practice entry on a fictitious record should be cancelled rather than cleared.

4. CLASS WITHDRAWALS

If a student has been enrolled to attend a DCIN certification class, but is unable to attend, it is important you as the TAC/ATAC for your agency withdraws the student from class. Classes are in high demand, and a student who is enrolled but does not attend may prevent another student who needs the instruction from enrolling.

- a) For in-person classes, withdraw them in Console. See the Omnixx Console and Trainer Manual for instructions.
- b) For virtual classes, the registered student can use the “cancel” link provided in the WebEx confirmation email to withdraw. If the student cannot access this, the TAC/ATAC should send an email the District Training Specialist for that class.

5. TRAINING MANUALS

Provide the student with the current module Training Manual(s) for each certification class the student is enrolled in. The module training manuals are available in Omnixx Links under Training.

6. CERTIFICATION TESTING

The TAC must schedule and conduct all certification and re-certification testing.

- a) Initial Certification – Users must coordinate the testing with their agency’s TAC. The TAC will schedule a date/time for the testing and may specify a particular location where the testing is to occur.
 - (1) Testing must be completed prior to fifteen (15) days from the last day of classroom instruction. If the student fails to pass the test within the fifteen (15) days, he/she will lose access to Trainer and must attend class again.
 - (2) *Status will change to ‘Expired’ at 12:01 AM on the date of expiration.*
 - (3) If a user takes a certification test without properly contacting his agency TAC, the score will be deleted and the student must retake that test. The user may be sanctioned by the SBI. A subsequent violation may result in revocation of the user’s DCIN certification.
- b) Recertification – Operators who are within 30 days of their DCIN certification expiring should contact their TAC and schedule an online recertification test. This test can be taken 30 days prior to the expiration date or up to 365 days after the expiration date.
- c) Expired Certification – If an operator’s certification has expired, he/she will not be permitted to operate the device until he/she has successfully passed the online recertification test. When a student’s certification has been expired for more than 365 days, the student will be required to attend the DCIN certification class.
- d) Test Results - When the test has been submitted for grading, the user will immediately receive a Test Results page displaying the test score and all questions and answers from the test. This will now allow users the ability to review missed test questions.
 - (1) The user is required to confirm they have reviewed the test results by clicking on the “*I acknowledge reviewing my test results*” located at the bottom of the page. *The certification status will then be updated to reflect the new 2-year certification.* This step must be completed before the Test Results page can be printed. *If this acknowledgement is not checked the current test status will not be saved and the user’s certification status will show expired.*
 - (2) The Test Results page must be printed, signed and dated by both the TAC/ATAC and user, then placed in the appropriate training file

maintained by the agency for the 2-year certification timeframe. A copy of the results page and a certificate may also be printed. If it is the TAC taking the certification/recertification test, the TAC will print the results page, sign and date it. The TAC should then have his/her supervisor countersign the results page(s).

7. SUSPENSION/REVOCATION OF DCIN CERTIFICATIONS

The SBI may suspend or revoke an operator's certification for willfully or repeatedly violating SBI rules and regulations. An agency head requesting revocation of an operator's certification should notify the SBI. The SBI may revoke an operator's certification when sufficient evidence is given as grounds for revocation and proven factual. For additional information on revocation for certification refer to 14B NCAC 18C.0100.

E. Audit Coordinator

1. CONTACT PERSON - The TAC will be the contact person for triennial audits conducted by the state and the FBI.

- a) The TAC should be available to work with SBI staff during the audit cycle. If the TAC is unavailable during the audit cycle, arrangements should be made for appropriate personnel to be on hand to assist SBI staff with questions or requests.
- b) As part of the audit process, an Auditor or Training Specialist will make contact with the TAC to set up a date and time for an on-site security check of your terminals.
- c) Coordinate agency's response to any non-compliance issues noted in the audit and monitor adherence to resulting policy changes.

2. OFF-CYCLE AUDITS

- a) Unscheduled Audits – Off-cycle audits were previously called “Special Audits” or “Administrative Investigations” and are not on a regular cycle such as the triennial audits.
- b) Reason - These audits may occur due to complaints from individuals outside of the agency, requests from within the department or by an agency head, or due to information obtained from other sources.

3. PRE-AUDIT - During the Pre-Audit phase, the auditor assigned to your audit will make contact with your agency to verify the contact information for the TAC and agency head and also to verify information in the NCIC and Nlets ORI files.

4. AUDIT NOTIFICATION - The auditor assigned to your audit will send an email to the TAC and agency head with the audit packet attached. It is the responsibility of the TAC to ensure the appropriate documentation is available for inspection and all paperwork is submitted before the end of the audit cycle.

5. AUDIT RESULTS

- a) Evaluation – Once the requested documents are received by the Compliance Unit, they will begin evaluating the agency.
- b) Results – Once the audit file has been processed and reviewed, the results will be emailed to the agency head and TAC. This document is password protected. You must contact your auditor for the password.
 - (1) Compliant – If your agency is found compliant, the audit file will be closed.

- (2) Non-Compliant – If your agency is found non-compliant, the results will indicate what issues were found and provide instructions for how to proceed.
- b) Response - Coordinate agency's response to any non-compliance issues noted in the audit results and monitor adherence to resulting policy changes.

IX. Information and Assistance

Refer to your DCIN module training manuals. Other information may be found at <https://www.ncsbi.gov/omnixlinks>.

A. SEND and Functional Message Integrity

1. AUTHORIZATION - The DCI Network is for appropriate criminal justice and law enforcement uses only. All traffic generated over the system shall be made in the performance of the employee or agency's official duties as they relate to the administration of criminal justice.
2. INAPPROPRIATE MESSAGES - An inappropriate message is one which requests information which is available through other system files or is of a personal nature. The below list is not all inclusive:
 - a) Requesting the location of an agency when such information may be found by inquiring into the ORI files, or requesting a check on warrants when such information should be in NCIC Wanted Persons file and/or eWarrants if a warrant exists.
 - b) Transmitting long lists of property stolen which should be entered into the NCIC hot files.
 - c) Messages which give inadequate information for processing.
 - d) Any messages recruiting personnel.
 - e) Any messages which advertise the selling of equipment or property by the agency or other outside source.
 - f) Non-criminal justice information would include any message of a personal nature or subject matter totally unrelated to the administration of criminal justice.
3. POLICY AND REGULATIONS - For further information, refer to 14B NCAC 18B.0102.

B. SBI Service Desk

1. CUSTOMER SUPPORT – IT ASSISTANCE - The North Carolina State Bureau of Investigation, Information Technology Division, Service Desk is operational 24 hours a day, 7 days a week. You should always refer to the online help information (Form or Field Help) about DCIN files and transactions when experiencing problems. However, if you are unable to find the answer to these questions after normal business hours, you should contact the SBI Service Desk at terminal PIB, by phone at 919-773-7900, or email at ServiceDesk@ncsbi.gov. Outside the Raleigh area may use the toll-free number: 1-866-867-7106.
2. VPN PASSWORD - The SBI Service Desk personnel are the only ones that may reset your VPN account if needed or create a new account for newly certified DCIN operators. The training specialists cannot reset your VPN password. Make sure you advise Service Desk personnel it is your VPN password that needs to be reset, and not your DCIN password.

C. Contact Us

Division of Criminal Information Network

HELP during the DAY — Monday–Friday 8 am–5 pm

1) Email / Call : **Your District Trainer**
ONLY IF Trainer's AutoReply Directs You, Contact 2 or 3

2) Email : TACHelp@ncsbi.gov

3) Call : **(919) 773 - 7900**
Leave Voice Message on DCIN Help Line

>> New VPN Requests must be made online <<
[Click here](#) for VPN Account Request Instructions
Excel Spreadsheet still Required

After-Hours DCIN Assistance

HELP after 5:00 pm — Evenings, Holidays, Weekends

Contact SBI Service Desk

for assistance with a VPN connection, a DCIN password change,
TID reset, or other technical assistance

Within Raleigh Area: **(919) 773 - 7900**

Toll Free : **(866) 867 - 7106**
Email : ServiceDesk@ncsbi.gov
Send Message : **PIB** >Terminal Address

If you need emergency advanced help on a DCIN transaction,
SBI Service Desk will connect you to the DCI HelpLine.
Please leave a **CLEAR voice message** with **Agency+Phone** after recording

Only YOUR Voice Message Notifies the On Call Trainer to Call You Back.

**** Non-Emergency After-Hours Requests**
May Receive Responses on NEXT Business Day
Monday– Friday 8 am – 5 pm

During Business Hours — Monday – Friday, 8 am – 5 pm

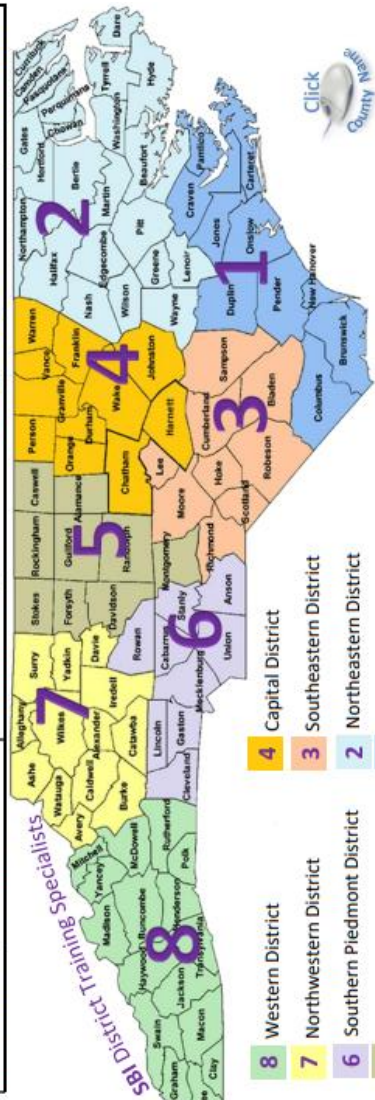
CONTACT US

Email Unit for Most Efficient Response * [click link](#) * — then if needed, phone



TOPIC	SBI Unit	Email	Phone
Access Agreements	Access Integrity Unit	AIUHelp@ncsbi.gov	(919) 582 - 8639
Audits	Compliance Unit	ARAHelp@ncsbi.gov	(919) 582 - 8640
Criminal History Corrections	CCH / NICS Unit	CCHmodification@ncsbi.gov	(919) 582 - 8690
Crime Reporting, UCR, NIBRS	Crime Reporting Unit	SBCrimeReport@ncsbi.gov	(919) 582 - 8680
DCIN–NCIC–NLETS Usage/Records	Training Unit	TACHelp@ncsbi.gov	(919) 773 - 7900
DCIN Notification ListServ	IT Customer Support Center	ServiceDesk@ncsbi.gov	(919) 773 - 7900
E Purpose Codes	Access Integrity Unit	EcodeHelp@ncsbi.gov	(919) 582 - 8639
EVOLVE – Validations	Compliance Unit	EVOLVEHelp@ncsbi.gov	(919) 582 - 8640
FBI – NICS Dispositions	CCH / NICS Unit	FBI-NICS@ncsbi.gov	(919) 582 - 8690
Fingerprint Results	CIIS Customer Service Unit	CIISHelp@ncsbi.gov	(919) 582 - 8660
LASO - Local Agency Security	Compliance Unit	ARAHelp@ncsbi.gov	(919) 582 - 8640
ORI – Request Additional ORI	Compliance Unit	ORI@ncsbi.gov	(919) 582 - 8640
Permits Concealed Gun	Compliance Unit	CHPHelp@ncsbi.gov	(919) 582 - 8640
Sex Offender Registration	Sex Offender Coordination Unit	SORHelp@ncsbi.gov	(919) 582 - 8670
Security Awareness Training	Compliance Unit	SATHelp@ncsbi.gov	(919) 582 - 8640
TAC Support	Training Unit	TACHelp@ncsbi.gov	(919) 773 - 7900
Technical + VPN Issues	IT Customer Support Center	ServiceDesk@ncsbi.gov	(919) 773 - 7900
Terminals—Request Additional Devices	IT Customer Support Center	BISL@ncsbi.gov	(919) 773 - 7900

SBI District Training Specialists



Regional Instructors

[Click](#) 

8 Western District

7 Northwestern District

6 Southern Piedmont District

5 Northern Piedmont District

4 Capital District

3 Southeastern District

2 Northeastern District

1 Coastal District