COLCHESTER POLICE DEPARTMENT

	SUBJECT: NCIC Policy
EFFECTIVE DATE: November 20, 2024	**NUMBER: GENERAL ORDER #34**
REFERENCE: Supersedes GO #34 dated April 4, 2018	
REEVALUATION DATE: Annual **APPROVED:** RAST VM (181)	**NO. PAGES: 11**

I. PURPOSE

The National Crime Information Center (NCIC) is a nationwide, computerized information system of accurate and timely criminal justice information managed by the FBI for the benefit of law enforcement. NCIC includes information for wanted persons, missing persons, stolen property, criminal history, and other information compiled during investigations of crimes that are known or believed on reasonable grounds to have occurred. Additionally, evidence on identifiable individuals collected to anticipate, prevent, or monitor possible criminal activity, as well as information pertaining to unidentified persons is available through the NCIC system.

II. POLICY:

It shall be the policy of the Colchester Police Department (CPD) to ensure the proper operation of NCIC.

The standards, procedures, formats, and criteria as contained in the FBI CJIS Security Policy and NCIC Operating Manual will be followed by all Department members accessing the same through the Vermont State Message Switch (VLETS) and the International Public Safety Network (NLETS).

III. AGENCY COMMITMENTS

The primary responsibility for the entry and maintenance of accurate, timely, and complete records lies with the agency whose ORI is on the record. However, each agency is monitored by the CJIS Systems Agency (CSA). This Agency has direct telecommunication lines to NCIC, and is held responsible for records entered through those lines. There is no more than one CSA per state.

In Vermont, the CSA is the Vermont Crime Information Center (VCIC), Department of Public Safety in Waterbury, Vermont.

VCIC is responsible for monitoring system use, enforcing system discipline, and assuring that all users under their jurisdiction follow NCIC operating procedures. As CSA, VCIC's goal is to assist agencies in their use and compliance with the NCIC System. However, VCIC's obligation is to ultimately ensure the integrity of the system, therefore, robust administrative procedures and controls are in place to ensure accurate data entry and compliance with documented policies and procedures. These procedures and controls can prevent lost court cases, civil liability suits, and criminal charges against the law enforcement officer, dispatcher, administrative personnel and/or their agency.

The data stored in the NCIC System and separately in the Interstate Identification Index (III) File is documented criminal justice information and must be protected to ensure correct, legal, and efficient dissemination and use. It is incumbent upon the agency operating an NCIC terminal to implement the necessary procedures to make that terminal secure from any unauthorized access and/or use. Any departure from this responsibility warrants the removal of the offending terminal from further NCIC participation.

Additionally, to protect the integrity of the state-wide system access to federal records systems, failure to comply with NCIC Operating Policy, CJIS Security Policy to include access and dissemination of III records and/or VCIC's NCIC and CJIS Security policies may result in sanctions up to and including the agency's removal from the VT Law Enforcement Telecommunications State Message Switch (VLETS).

Furthermore, the failure of the CSA to hold any noncompliant agency accountable, up to and including removal from the State Message Switch, could result in the FBI disallowing further connection to and removing the entire State of Vermont from NCIC access.

The following definitions illustrate CPD's agreements with NCIC and VCIC, and are to be referenced and followed.

Any device (whether in its entirety or one limited to logins and/or specific users), as defined by the FBI's CJIS Security Policy, that accesses NCIC information will only be used by trained and NCIC certified personnel.

When a new record is entered into NCIC, or an existing NCIC record is modified, the resulting printout (or appropriate cover sheet) must be initialed and dated by the person who made the entry or modification, and by the person who performed the NCIC-required second-party check. This printout/coversheet, along with the entry request and entry confirmation will remain in CPD's Hot File. If CPD becomes a non-terminal or non-24 hour, a duplicate copy of this information will be maintained by its Holder of Records.

As required by the FBI, CPD will have at least one FSTO-certified user designated as "TAC" (Terminal Agency Coordinator), which is the Point-Of-Contact between the agency and VCIC for NCIC purposes.

A. Timeliness – To ensure maximum system effectiveness, NCIC records must be entered immediately when the conditions for entry are met, not to exceed 3 days upon receipt (electronic or hard copy format) by the CPD. The only exceptions to immediate entry are when otherwise prescribed by federal law or when documentation exists to support delayed entry.

1. WANTED PERSON FILE
   a. A timely entry in the Wanted Person File is one made immediately once: The decision to arrest, or authorization to arrest, has been made, regardless of extradition parameters.
   b. An active Vermont State Warrant must exist prior to entry.
   c. Timely removal from the file means an immediate removal once the responsible agency has documentation that the subject has been arrested, or is otherwise no longer wanted.
2. FEDERAL FUGITIVE FILE
   a. Entry is made immediately (i.e., within 24 hours) upon receipt of information by CPD, after the decision to arrest, or authorization to arrest has been made. Exceptions to this rule occur if imminent arrest is expected or other clear, identifiable, operational reasons would preclude immediate entry (e.g., insufficient descriptive data resulting in a "John Doe" warrant).
   b. Any exceptions to delayed entry in NCIC must be minimized and documented.
3. MISSING PERSON FILE
   a. Timeliness of entry and modification in the Missing Person File is made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) and the appropriate record documentation are available.
   b. For missing persons not emancipated in VT or otherwise under age 21, NCIC Missing Person File records must be entered within two (2) hours of receiving the minimum data required for entry, in accordance with the Adam Walsh Child Protection and Safety Act 34 U.S.C. § 41308 et seq.
4. ARTICLE, BOAT, GUN, LICENSE PLATE, SECURITIES, VEHICLE/BOAT PART, and VEHICLE FILES

a. Entry is made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) is available.
b. Information about stolen license plates and vehicles should be verified through the appropriate motor vehicle registration files prior to entry, if possible. However, if motor vehicle registration files are not accessible, the record should be entered into NCIC, and verification should be completed when the registration files become available.

5. ALL OTHER FILES
   a. Entry is made as soon as possible once the minimum data required for entry (i.e., all mandatory fields) is available.
   b. See the NCIC Operating Manual Introduction for additional guidelines pertaining to timeliness.

B. Validation – Validation obligates the ORI of record to confirm that the record is complete, accurate, and still outstanding or active.

Validation is accomplished by reviewing the entry and current supporting documents, and by recent consultation with any appropriate complainant, victim, prosecutor, court, nonterminal agency, or other appropriate source or individual.

Every effort will be made to ensure that all available information has been entered into NCIC, and that the information contained in each NCIC record is accurate.

In the event the ORI is unsuccessful in its attempts to validate the record, the entering authority must decide, based on the best information and knowledge available, whether or not to retain the entry in the file (NCIC Operating Manual Introduction).

The local agency is to have a written validation procedure in place, to include validation documentation (how the record was validated), and make it available for review upon reasonable notice by authorized VCIC or FBI representatives:

1. CPD will find the records selected by VCIC each month to be validated using the using the CJIS Validations platform found at https://ncicvalidations.dps.state.vt.us/validations/index.pl and do so by the listed deadline.
2. One of CPD's TACs will review the entry and current supporting documents and attempt to consult with any appropriate complainant, victim, prosecutor, court, nonterminal agency, or other appropriate source or individual

to ensure that the record is accurate and should still be active.

   a. Contact attempts shall be documented on the Hot File cover sheet along with the disposition of file retention if contact is made.
   b. If no contact is established after repeated attempts, that shall be documented on the Hot File cover sheet, and the TAC and Chief of Police will decide whether to retain the record in NCIC or to clear it. A documenting memo signed by the Chief of Police will be included in the Hot File explaining the decision to retain or clear.

3. The TAC shall select the appropriate action in the CJIS Validation platform: to keep "As Is," to "Modify," or to "Clear" for each record.
4. The TAC shall update the record in NCIC using OpenFox Messenger's modify form for the appropriate record type and entering their OpenFox username in the "Name of Validator" field, along with any other fields that need updating.
5. Printouts of the modification confirmation will be kept with the month's checklist report printed from the CJIS Validation platform and be available for review upon request.

C. Completeness

1. Complete records of any kind include all information that was available on the person or property at the time of entry ("packing the record"). When additional information becomes available after original record entry into NCIC, that information should be added to the record as quickly as reasonably possible.
2. Complete person records include numbers that could be indexed in the record, i.e., FBI#, Social Security, Passport, VIN, License Plates, Driver's License, etc. Inquiries should be made on all names and aliases used by the suspect. Complete vehicle inquiries include VIN and license plate numbers.

D. Accuracy

1. The accuracy of NCIC entries and modifications must be verified by a second party. Verification should include confirmation that the available crosschecks (i.e., VIN/license numbers) were made and that the data in the NCIC record matches the data in the investigative report.

IV. DATA QUALITY

Stolen property, wanted or missing persons, and files for information on dangerous person or groups are considered "Hot Files."

A. Entry Procedures

1. A paper or electronic NCIC entry form will be completed and stored in the Hot Files folder. The NCIC printout should be filed or scanned with the appropriate Hot File entry form. The NCIC Operating Manual is available on the CJIS Launch Pad for consultation for questions regarding required fields criteria.

B. Error Checking

1. Any NCIC entry or record modification will result in a response from NCIC acknowledging the request and verifying entry, providing the ORI (Originating agency) with a NCIC number. The NCIC number is the unique number assigned to each entry.
2. Z-NCIC Confirmation is the Entry/Modification Confirmation and should be used by the originating agency to confirm that the information entered or modified is correct.
3. The initials of the person making the entry or record modification in NCIC, as well as of the person providing the secondary accuracy check, are required to be included on the record documentation.

C. NCIC Record Clear and Cancellation Procedures

1. It is the responsibility of the ORI of record to clear (or cancel, only when appropriate) the record in NCIC when property has been recovered, or the person record is no longer valid (i.e. – missing person located, wanted person arrested, etc.).
2. After clearing (or cancelling when appropriate) a record, the resulting "Clear NCIC" message will be placed with the appropriate Hot File paperwork, removed from the Hot File, and filed with the case.
3. The same will be followed for cancellations. The TAC should be advised of the record clear or cancellation.
4. Cancel vs Clear – NCIC records should be cleared and not cancelled, unless and except those records prove erroneous (should not have been entered into NCIC in the first place), or are in such error that they cannot be modified to correction.

D. Inquiry Transaction

1. A query on a name will result in the automatic checking of all of the NCIC Person Files and may also result in a Vehicle File record check if a vehicle has been linked to a name.
2. Some of the NCIC Person Files are for officer safety only, and to facilitate the exchange of information between agencies, and others may result in taking the subject into custody once the "hit" is confirmed.
3. All positive responses must be read carefully, and data compared to determine if the person and/or property in the NCIC response and the person and/or property encountered/discovered/recovered by the officer are the same.

E. Hit Confirmation Procedures

1. Any agency that receives a positive response to an NCIC inquiry must confirm the "hit" before taking any action such as arresting the wanted person, detaining a missing person, or seizing the stolen property.
2. Confirming a hit means to contact the entering agency to ensure that the person or property encountered is identical to the person or property identified in the record, ensure that the warrant, missing person or theft report is still outstanding, and to obtain a decision regarding the extradition of the wanted person, information regarding the return of the missing person, and/or information regarding the return of stolen property to the rightful owner.
3. NLETS (The International Justice and Public Safety Network) will be used for any hit confirmation outside of VT: Open Fox Messenger Hit Confirmation Request forms can be found in the NLETS or NCIC folders: YQ (hit confirmation request) or YR (hit confirmation response).
4. If the initial confirmation is made by a telephone call to the agency, it is to be followed up with the use of either an Administrative Message (AM) or by the appropriate form (i.e. – Notification of Arrest Status (NAS)) so that there will be an audit trail of the contact. This paperwork will be attached to the original case.
5. Hit Confirmation responses should be provided within ten (10) minutes of receiving the request.

F. Locate Procedure

1. After confirming the hit, and upon taking a person into detention or custody, or recovering property, a Locate should be placed on the NCIC record. The only exception to this is a

wanted person where the extradition limits clearly exclude extraditing from Vermont, including NOEX status.

2. Placing a locate on a Missing Person File record will automatically clear the record.

V. CRIMINAL HISTORY RECORDS (INTERSTATE IDENTIFICATION INDEX ((III)) ((TRIPLE I)))

NCIC provides the capability to search the Interstate Identification Index (III) using an individual's personal identifiers, assigned SID (state ID#), and/or assigned FBI number to determine if an index to a person's criminal history exists.

Criminal History Inquiry provides an index of subjects matching inquiry, and includes information regarding where the record is maintained. A positive response contains additional identifying data to associate the record with the person of the inquiry (height, weight, race, fingerprint classification, tattoos, etc.). With this information, an agency can decide whether to request the record.

Criminal Record Request is used for specific criminal history records via III. Only the SID or FBI number can be used to identify the record being requested.

All subjects on whom III queries are conducted must be included in the Incident Case involvements, as substantiation for the Criminal Justice Administrative purpose for accessing III.

A. Confidentiality

1. The Privacy Act of 1974 decrees the confidentiality of criminal history records, as well as requiring the FBI to maintain an audit trail of the purpose for each disclosure. In order to provide justification for accessing criminal history records, there are multiple purpose codes from which to choose, and the correct purpose code must be utilized during the III inquiry, as defined in the III Manual. Additionally, an audit trail is maintained by VCIC.
2. The name of the officer requesting the record, the case number that generated the need to have the record, as well as any other agency/person that will receive this record (secondary dissemination) must be included in the attention field of the request.
3. The ORI of the agency requesting access to criminal history records must be used on the request.
4. In addition to these safeguards, the disposal of criminal history records produced by Soundex, which have no connection to the case, will be shredded immediately to

prevent access by unauthorized persons. At no time are these erroneous criminal history records to be included in case files to which they do not belong.

5. Criminal History records will not be released to anyone other than those listed in the dissemination request, including the subject of the record.
6. Criminal History records will not be faxed, except to authorized recipient ORIs, and only when an authorized user of the recipient ORI is at the receiving fax machine at the time of transmission, and confirms receipt of the same. Prior to fax machine disposal, the fax machine's hard drive must be destroyed or completely overwritten multiple times.
7. Criminal History records are to be hand delivered or sent via encrypted email. Email encryption must be to the FBI encryption standards. Office 365 (@vermont.gov) email is not encrypted to FBI standards and not to be utilized in the exchange of Criminal History Information without additional CJIS Security-compliant encryption, to include separately provided CJIS compliant passwords.
8. To establish and maintain an audit trail, Criminal History information may also be sent via certified return receipt United States Postal Service mail to a uniquely identified person (point of contact) at the receiving agency.
9. Generally, all of the above Criminal Justice Administrative requirements also apply to accessing Vermont Criminal Histories through the Vermont Criminal History Database.

VI. TRAINING & CERTIFICATION

Training and recertification testing are completed using the resources located on the CJIS Launch Pad and the nexTEST websites.

A. Personnel NOT Accessing NCIC/NCIC Data – CJIS Online

1. Agency personnel who will not have access to NCIC, but will have exposure to the same and/or other CJIS data and CJIS systems in the course of their duties, must complete CJIS Security and Privacy Training through the CJIS Online website. This process is managed by the Agency TAC (account creation & certification level assignment).
2. CJIS Online is also used to manage the special Security and Privacy Training requirements for persons fulfilling the Local Agency Security Officer (LASO) and Tech Liaison roles, irrespective of said person's access to NCIC data.
3. CJIS Online is also used to manage the special Security and Privacy Training requirements for Vendors and their affiliated Vendor Users.

B. Personnel Accessing NCIC/NCIC Data – nexTEST

1. TACs must submit a New VLETS Account Request form (via OpenFox Messenger) for every new or returning hire who will have access to NCIC (includes all sworn personnel regardless of role within the agency), and ensure said new/returning hire promptly completes Security and Privacy Training prior to accessing CJIS data, through the nexTEST system.
2. Non-terminal agencies should submit a hardcopy New VLETS Account Request form directly to VCIC for processing.
3. If an agency has new sworn personnel (full or part-time) who will be working prior to attending the VT Police Academy, then said personnel MUST complete Security and Privacy Training without delay. A VLETS account and certification is required the same as for non-sworn personnel.
4. Part-time sworn personnel, who will not be working until after graduating from the Part-Time VT Police Academy, must have a VLETS account ready for certification immediately upon graduation.
5. VCIC partners with the VT Police Academy, on behalf of the agency, providing NCIC and Security and Privacy Training/certifications as part of the curriculum for fulltime sworn personnel who will NOT be working until after Academy graduation.

C. Annual NCIC/CJIS Recertification

1. Annual recertification is required for all personnel with CJIS Online accounts.
2. Annual recertification is required for all personnel with nexTEST accounts.

D. Terminal Agency Coordinators (TACs)

1. TACs must maintain Full Service Terminal Operator Certification and complete annual TAC training.

E. Training/Testing Records

1. The agency will maintain records of all NCIC and CJIS Security Awareness training and testing.
2. The nexTEST and CJIS Online programs provide reporting capabilities, including user training, testing, and certification status.
3. The TAC will ensure that these records are maintained on behalf of the agency.

VII. VERMONT STATE MESSAGE SWITCH (VLETS)

Access to the Vermont State Message Switch, which allows data exchange between NLETS, VLETS, VCIC, NCIC, III and DMV, is a privilege allotted to all Vermont CJIS Security and NCIC-compliant criminal justice agencies, for the sole purpose of criminal justice administration.

The FBI's CJIS Security Policy identifies responsibility to the CSA for establishing and administering an information technology security program throughout the CSA's user community, to include the local levels.

For system integrity to be established and maintained, VCIC must monitor system use, enforce system discipline, and assure all Vermont users are following NCIC operating procedures and adhering to CJIS Security Policy requirements.

VCIC assumes a large degree of administrative responsibility, and possible legal liability, for the maintenance of a criminal justice information system. Accordingly, VCIC has instituted appropriate and reasonable quality assurance procedures for all federal and state users which access the Vermont State Message Switch.

Removal from the Vermont State Message Switch will preclude all users certified under the removed agency's ORI from data exchange derived from connection with the Vermont State Message Switch. This includes the removal of both direct access (via fixed terminal or mobile device), and indirect access (via dispatch and/or administrative services).

Generally, VCIC's Information Security Officer (ISO) determines whether an agency is allowed continued access to the Vermont State Message Switch after a facts-based investigation is completed.

Should the infraction or noncompliance be of such a nature that immediate termination of access is deemed prudent to ensure the integrity of the Vermont State Message Switch, a formal investigation will ensue after said termination rather than preceding it.

Any decision issued by the ISO may be appealed, in writing, within ten (10) business days of said decision, to the Director of VCIC, who is the State of Vermont's CJIS Systems Officer (CSO).

A final appeal of the CSO's determination may be made, in writing, within ten (10) business days of said decision, to the Department of Public Safety Commissioner's Office.