

# WATERTOWN POLICE DEPARTMENT GENERAL ORDER



JOANNA W. VITEK  
CHIEF OF POLICE

Effective Date: May 1, 2010	Rescinds: Amends: A-188 (January 2004)	Number: A-188
Subject: Triple I - Interstate Identification Index (III)		Re-evaluationDate: May 2013
Distribution: ALL PERSONNEL	Related CALEA Standards:	

This order consists of the following numbered sections:

1. Policy
2. Definitions
3. Procedures

## 1. POLICY:

It is the policy of the Watertown Police Department to provide guidelines and rules that are consistent with federal laws and state statutes governing Interstate Identification Index (III) and henceforth referred to as the "III" or "Triple I" file. The III file usage and the applicability of those laws that the United States Department of Justice, Federal Bureau of Investigations and the National Crime Information Center have created are to ensure that only authorized purposes and security are to be strictly adhered to as it relates to the III file. It is the express intent that personnel adhere strictly to those III guidelines when accessing and obtaining III information from terminal devices. Security must be guarded to prevent any unauthorized access to or use of the data received from the NCIC 2000 System/NLETS (National Law Enforcement Telecommunications System). Any knowledge or receipt of information that is in violation of the Watertown Police Department Policy, Federal Law and/or State Statute must be immediately reported to a Communications Center Supervisor and/or shift supervisor. Training and knowledge of the applicable policy, laws and statutes can be obtained from the NCIC 2000 (National Crime Information Center) Operating Manual, Federal and state statutes.

## 2. DEFINITIONS:

- a. Interstate Identification Index (III): The Interstate Identification Index (III) file is a repository for criminal history information for states. It houses and responds with criminal history information from states that submit criminal history and fingerprint card information to the FBI.

## 3. PROCEDURES: Procedure Guidelines For Security and Confidentiality of Interstate Identification Index (III) Criminal History Queries and Information Obtainment:

- a. Receipt of Requests for III information by Law Enforcement personnel and agencies
  - i. Access or use of the data obtained from terminal devices.
    1. Operators shall access FBI/CJS system only for those purposes for which they are authorized.
    2. Operators shall ensure only proper use of the system for which only authorized purposes have been determined.
    3. Operators must be certified and continue to maintain certification by passing the 2 year Terminal Operator Re-Certification Test for operating the NLETS System.
    4. Operators shall enforce and maintain security to terminal devices and data to prevent any unauthorized access or use of the III data obtained from files.
    5. Operators shall ensure proper documentation and management of the hand written log, which is maintained by Operators in the dispatch center for a minimum of one year.
      - a. The hand written log shall be made available upon request to the state authorities such as the CTO (Control Terminal Officer), the FBI (Federal Bureau of Investigations), NCIC (National Crime Information Center (NCIC 2000) and/or their designee(s) for validation purposes.
      - b. The hand written logs shall be stored in a secure environment as to ensure the integrity of the department and its record keeping of III logs.
    6. The supervisor shall enforce rules, guidelines, policies, laws and statutes that are relevant to terminal access and data.

7. New employees will not be granted access to the NLETS/NCIC systems until such time as it is appropriate to access the system.
  - a. The new employee must submit within 10 days two fingerprint cards and an application to Law Enforcement Training for submission to FBI CJS for identification purposes.
  - b. If there is no match of fingerprints with an III record, the new employee will be granted access to NLETS/NCIC systems.
- ii. The hand written III log shall identify a minimum of requirements when a III record is requested:
  1. Identifies the Operator, by a unique personalized identifier, who initiates, pursues and concludes the transaction.
  2. Identifies the requestor of the record by a unique identifier such as a name, rank, unique identifier, etc. (not badge numbers as personnel change within badge numbers).
  3. Identifies the authorizing agency of the requestor of the record.
  4. Identifies the authorization, purpose code and recipient of the III transaction.
- iii. Validity of III records.
  1. Records should be properly destroyed when no longer current.
  2. Future and subsequent information requires the requestor to request a new copy of the III data information as additions and deletions may be made at any time.
  3. Records stored for extended periods of time, shall be maintained in a secure environment and filed with the case files/criminal record files to prevent any unauthorized access to those records and preserve the integrity of those records.
  4. Final destruction of records shall be accomplished in a secure manner so as to preclude any unauthorized access or use of those records by unauthorized persons.
    - a. Destruction of media such as hard disk, RAM disk, tape drives, removable media backup devices, etc. must be in a manner to sufficiently destroy the data without possible reconstruction or use of that information.
    - b. Documentation is necessary to verify the destruction of III data on these media type of devices.
- iv. Law Enforcement officers/personnel, law enforcement agencies and obligee agencies associated with law enforcement must request III information by filing out the Law Enforcement III form from the Communications Operations Center.
  1. All known information will be documented on the form.
  2. The request form for III access authorization will be signed by the requestor of the III information.
  3. Once the III information is queried and a hard copy is received, the requestor is obligated to date, time and sign the form that the requestor is in receipt of the criminal history information from the III file.
  4. Once the requestor has dated, timed and signed the III request form, the Communications Officer who relayed the criminal history hard copy information to the requestor will sign and file the form.
  5. The III request forms will be filed for or a period of one year.
  6. A request for a III record that an officer/agency chooses not to receive at a later date, will be shredded by the Communications Officer who will date and sign the request form and if possible engage the officer in signing the documentation also.
  7. Any III record removed from the immediate area of the dispatch center, will not be taken back by the dispatch center for destruction – once the III record leaves the center, it is the responsibility of the officer or agency to destroy and document the destruction of the record.
- v. The accuracy of III record hard copy information shall be verified by the receiving officer/agency for accurate information.
  1. An incorrect III record request shall be corrected by querying the information again with the correct information.
  2. The III form will note the date, time and signature on the form again at the second time of the query.
- vi. Validation of III records.
  1. Approximately every two years the state will perform validations, which involves a review for compliance by Operators who have authorization to access the III records through the NLETS system.
  2. Deficiencies within the III record access process must be immediately corrected.

- b. Standards for Discipline – “Operators shall access FBI CJS systems only for those purposes for which they are authorized” (CJIS Security Policy Manual September 2002)
- i. Violations may include but are not inclusive for actions of misconduct such as:
    1. Querying of the III files without authorization for the query.
    2. Disclosing to non-authorized agents/individuals sensitive and classified information.
    3. Any modification or destruction of data on the hard copy or computer screen.
  - ii. Discipline for policy violators.
    1. It is the responsibility of every Operator to self-police and police the activity associated with III files.
    2. Any violation of III file access or sharing of sensitive information with unauthorized persons, etc. shall be immediately reported to the Communications Center and/or Shift Supervisor(s).
  - iii. Violation(s) include the following progressive discipline actions:
    1. First, a verbal warning will be given to the violator.
    2. Second, a written letter of reprimand will be given to the violator.
    3. Third, a suspension will be issued.
    4. Fourth, termination will be the result for a fourth and final violation of III records.
    5. Any criminal activity brought about through the system shall be grounds for immediate dismissal of the Operator.

---

JOANNA W. VITEK  
Chief of Police  
Watertown Police Department  
Watertown, South Dakota