



Attorney General Guidelines on the Collection, Handling, Storage and Dissemination of Intelligence in New Jersey

I. Attorney General's Intelligence Concepts

The law enforcement community in New Jersey must utilize intelligence to fulfill its mission in protecting the public from crime. At the same time, law enforcement agencies must protect the privacy rights of their citizenry and adopt standards and policies for the collection, evaluation, collation, analysis, and dissemination of intelligence.

Intelligence is key to effective law enforcement. As noted in the *U.S. Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*, "Members of groups or organizations acting in concert to violate the law present a grave threat to society...guidelines establish safeguards for group investigations...including tighter management controls and higher levels of review."¹

Within New Jersey, the Division of State Police has long been a leader in the intelligence field. Today's environment requires that all law enforcement agencies understand and use generally-accepted policies relating to intelligence. The most common standard in state and local law enforcement is 28 *CFR* Part 23, the *Criminal Intelligence System Operating Policies*. In the past, these policies have only been mandatory for multi-jurisdictional intelligence systems that were established or operated with the assistance of federal funding through the U.S. Department of Justice, Bureau of Justice Assistance. Today, these policies are the accepted standard for many intelligence systems, involving thousands of agencies across the country.

As the result of many factors, agencies large and small are either establishing or re-dedicating their intelligence efforts. It is therefore appropriate that, at this time, the Attorney General, as Chief Law Enforcement Officer in the State of New Jersey, promulgate guidelines that apply to all agencies in or supervised by the Department of Law and Public Safety, including county and municipal agencies with law enforcement powers.

¹ U.S. Attorney General, May 30, 2002, pp. 12 and 13; at www.usdoj.gov/olp/generalcrimes2.pdf.

It is also understood that “criminal investigatory records” which are the primary information entered into intelligence systems, are exempted from public access in the Open Public Records Act, P.O. 2001, Chapter 404 *N.J.S.* 47:1A-3, Executive Order #26, Executive Order #9 (Hughes 1963), and as affirmed by the Government Records Council final decision #2002-30 dated February 13, 2003.

II. Duties of Criminal Justice Agencies

A. A criminal justice agency may place information in an intelligence system and disseminate intelligence only if:

1. The agency has adopted written policies and procedures consistent with these guidelines.
2. The head of the agency has designated and trained an intelligence professional (officer or analyst) to act for the agency as set forth in these guidelines.
3. The agency agrees to abide by 28 *CFR* Part 23 (*Criminal Intelligence System Operating Policies*) and subsequent revisions of that policy.

B. Collection of information in intelligence systems

1. A criminal justice agency may collect information for placement in an intelligence system only if the following conditions are met:
 - a. the information concerns an individual, group, or entity that trained personnel in the agency reasonably suspect of criminal activity, and
 - b. the information does not reference the subject’s participation in or association to a political, religious, or social organization unless there is reasonable suspicion to believe that the participation is tied to criminal activity, and
 - c. the information is collected lawfully.
2. Law enforcement collection under these policies does not permit maintaining files on individuals solely for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States.

C. Storage of information in intelligence systems

1. A criminal justice agency may store information in a criminal intelligence system only if the following conditions are met:
 - a. the information has been evaluated for the reliability of the source and the validity of the data, and
 - b. the information has been classified as to its level of sensitivity, and
 - c. the information is dated as to its timeliness, and
 - d. the information is marked as to its suspense date for review or purge, and

e. information that has not been updated during a five year retention must be updated or purged.

D. Analysis of information

1. A criminal justice agency should be able to analyze information held in criminal intelligence systems, as well as other data to support intelligence and investigations.
2. Agencies may use either sworn or civilian personnel to analyze criminal information.
3. Agencies should provide appropriate personnel with training on standard methods of collection, analysis and reporting of data.

E. Dissemination of Intelligence

1. A criminal justice agency shall disseminate criminal intelligence information only to law enforcement or criminal investigative authorities with a right to know and a need to know the information in the performance of law enforcement duties.
2. A criminal justice agency shall disseminate criminal intelligence information only to those agencies who have adopted these guidelines or are in another state and have adopted 28 *CFR* Part 23 policies or are consistent with 28 *CFR* Part 23.
3. An audit trail or dissemination record is required when information is disseminated. The audit trail must include, at a minimum:
 - a. the date of the request,
 - b. the name of the individual requesting the information,
 - c. the name of the agency requesting the information,
 - d. the reason (need to know) for the requested dissemination,
 - e. the information inquired upon,
 - f. the information provided to the requester,
 - g. the name of the individual disseminating the information, and
 - h. the date of the dissemination (if different from the date of the request).
4. Information should not be disseminated if it was received from another agency (i.e., third party information) unless the agency from which it was received agrees to its dissemination.
5. Dissemination records must be made available, upon request, to individuals from the Division of State Police, Division of Criminal Justice or the County Prosecutor's Office conducting guideline compliance audits.
6. Nothing in these guidelines prohibits the dissemination of intelligence information

6. Nothing in these guidelines prohibits the dissemination of intelligence information to federal agencies which may not be covered by 28 *CFR* Part 23 but are covered by their departmental information policies, such as the Department of Justice *Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations*.

7. Nothing in these guidelines or other policies prohibits the release of intelligence information to a non-criminal justice individual in the case of imminent danger to life or property.

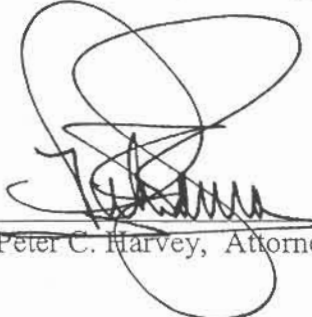
F. Security

1. Intelligence information must be kept in a physically secure area that is restricted to designated authorized personnel.
2. Visitors to this restricted area will be logged into a visitor log book and will be escorted during their visit.
3. Employment policies and procedures for screening/rejecting, transferring, or removing personnel must be in place.
4. If the intelligence system used is electronic, both programmatic and physical precautions must be in place to prohibit unauthorized access.

III. Duties of the Division of State Police, Division of Criminal Justice and County Prosecutors

As part of their roles in overseeing the operations of criminal justice agencies they supervise, the Division of State Police, the Division of Criminal Justice and the County Prosecutors, on behalf of the Attorney General, will be responsible for training, monitoring and auditing compliance with these intelligence guidelines.

These Guidelines are effective on this 9 day of March, 2004.


Peter C. Harvey, Attorney General

3/9/04
(Date)