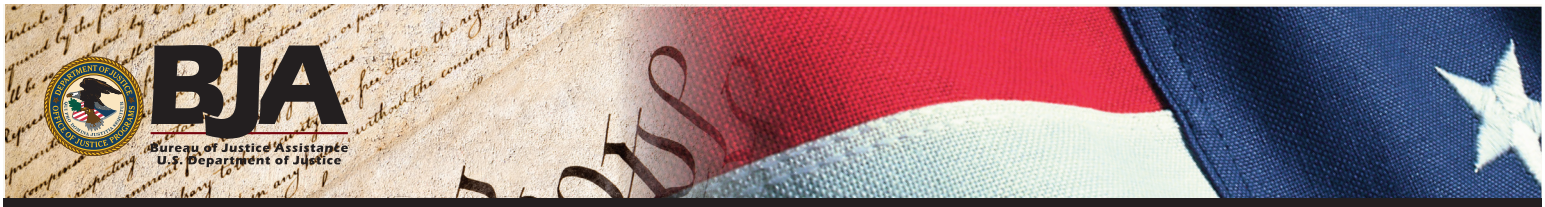


28 CFR Part 23

A Guide to Criminal Intelligence Policies

Criminal Intelligence Systems Operating Policies (28 CFR Part 23)

28 CFR Part 23 is a federal regulation that provides guidance to law enforcement agencies on the implementation standards for operating multijurisdictional criminal intelligence systems funded under the Omnibus Crime Control and Safe Streets Act of 1968, as amended (Crime Control Act). The purpose of the regulation is to ensure the protection of constitutional (civil rights and civil liberties) rights and further an individual's reasonable expectation of privacy. It provides guidelines to govern criminal intelligence systems regarding:

- Submission/entry (collection) of criminal intelligence information
- Inquiry
- Dissemination
- Review and purge or validation
- Audit and inspection
- Security

The *National Criminal Intelligence Sharing Plan* (NCISP) (http://it.ojp.gov/gist/150/) recommends the use of the regulation in order to ensure that the submission or collection, storage, and dissemination of criminal intelligence information by law enforcement agencies protect the privacy and constitutional rights of individuals and organizations. The NCISP recommends that this occur regardless of whether or not an intelligence system is supported with Crime Control Act funds.

The regulation has been in place since 1980, with only a minor revision (1993) and clarification (1998) to address emerging technology, providing clear and succinct guidance for criminal intelligence systems. In addition, the regulation has been identified as the minimum standard for sharing criminal intelligence information for state, local, tribal, and territorial (SLTT) law enforcement agencies across the country.

Authority

The Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), is the issuing authority for the regulation. The Bureau of Justice Assistance (BJA) provides policy guidance and regulatory interpretations, incorporated throughout this brochure, that govern the operation of criminal intelligence systems funded under the Omnibus Crime Control and Safe Streets Act of 1968, as amended.

Complying With the Regulation

Each agency operating a criminal intelligence system needs to develop its own operating policies and procedures, which should include:

- Access to criminal intelligence (participation standards)
- Participation agreements and other forms, as required
- Submission/entry requirements
- Types of criminal activity eligible to be maintained in the system
- Inquiry, dissemination, review and purge or validation procedures
- Audit and inspection, security requirements
- Definitions of key terms, including "need to know" and "right to know"

28 CFR Part 23 lays out a framework and identifies certain principles that need to be incorporated into an agency's policies and procedures regarding these aforementioned categories. The regulation offers a foundation for collecting, maintaining, and sharing criminal intelligence information while ensuring the privacy, civil rights, and civil liberties afforded to all Americans.

Agencies maintain a variety of reports, files, and databases that contain investigative or management information, public record information, commercial databases, and other fact-based information that is not subject to the regulation. If information from these sources is analyzed as part of an investigation and the result of that analysis meets the submission criteria outlined in 28 CFR Part 23, it could be entered as a submission to a criminal intelligence system.

Several national networks of agencies provide a coordinated process for the gathering of information and the evaluation and analysis of the information, turning it into actionable criminal intelligence information that an intelligence project can collect.

Criminal Intelligence Systems

Submission to the Database

Individuals and Organizations (Criminal Subjects)

- The trained law enforcement or criminal investigative agency officer, investigator, or analyst submitting the criminal intelligence information must have analyzed enough information from sources, observations, or other investigative or information-gathering efforts to believe there is a reasonable possibility that the named subject (individual or organization) is currently involved in a definable criminal activity or enterprise (the definition of reasonable suspicion).
- The trained employee who makes the determination of reasonable suspicion should be able to articulate why the criminal subject meets this threshold criterion.
- The criminal subject does not have to be the target of an active or ongoing investigation.
- The criminal subject does not have to have been arrested.
- The submission criteria apply to all names for which a record is created in the database, including:
  - Individuals (including criminal associates)
  - Organizations (may be formal, such as a business, or informal, such as a gang)
- The name of an organization that operates as a criminal enterprise or is a front for criminal activity can be entered into the criminal intelligence database. Once entered, its members may be considered to be reasonably suspected of involvement in the specified criminal activity of the organization and their names may be entered into the database as criminal associates and as criminal subjects.
- The suspected identifiable criminal activity of the subject (individual or organization) must meet the project's criminal activity criteria for a record to be entered into the criminal intelligence database.
- Backup documentation supporting the submission, including the suspected criminal activity of the subject, must be kept in the submitting agency's files.

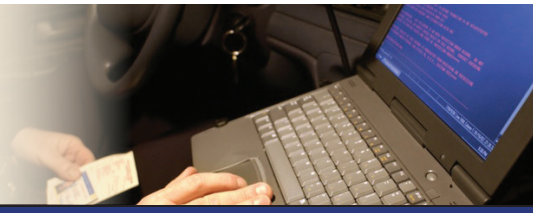
What NOT to Do

- Do not automatically enter the names of individual members of organizations without first making a determination that the organization is a criminal enterprise or front.
- Do not create and maintain a record on an individual or organization unless there is reasonable suspicion of involvement in a current criminal activity or enterprise.
- Do not include as part of a criminal intelligence record the name of any individual or organization that is not reasonably suspected of criminal activity unless such name is clearly labeled as "noncriminal identifying information."
- **Noncriminal Expressive Information**—Do not enter information about a subject's political, religious, or social views, associations, or activities unless the information directly relates to the subject's criminal activity or enterprise.

Noncriminal Identifying Information (NCII)

- Under the following circumstances, names and relevant data about individuals or organizations who are not suspected of criminal involvement that provide descriptive, identifying information regarding the criminal subject or the criminal activity in which the subject is engaged may be included in a subject's record in the criminal intelligence database as "noncriminal identifying information" (NCII):
  - The information must be labeled or contain a disclaimer indicating that it is NCII.
  - The criminal subject identified by this information must meet all requirements of 28 CFR Part 23.
  - NCII may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system.
  - The NCII may be searched as part of an inquiry, provided that any "hit" is clearly labeled as NCII.
    - The reason for this label is to ensure that the user understands the context in which the noncriminal identifying name is included in a criminal intelligence record—that it is included for identification purposes and not because the individual or the organization that the noncriminal identifying name pertains to is reasonably suspected of criminal involvement.

Operating Policies (28 CFR Part 23)



Scenarios

If	Then
An individual is observed taking pictures of a power plant in a surreptitious manner. This information is provided to law enforcement as an anonymous tip.	The information cannot meet reasonable suspicion because there is neither involvement in definable criminal activity or conduct nor an identified subject. It could not be entered into a criminal intelligence system, but it could be entered into a tip file.
A member of a criminal gang is arrested for narcotics violations. The gang is a documented criminal gang involved in interstate narcotics trafficking. The gang member is arrested while driving a vehicle registered to his father. The father is not reasonably suspected of involvement in the gang activity or narcotics trafficking.	The name of the gang member and the name of the gang may be entered into the database and linked as criminal associates in their respective records. The name of the father can be entered only as "noncriminal identifying information" relevant to the individual gang member and must clearly be labeled as such.
Surveillance on a criminal subject shows the individual frequently entering a particular place of business. The business is not suspected of involvement in the criminal activity of the subject.	The name of the business can be included in the criminal subject's record as "noncriminal identifying information" only if it is determined to be relevant to the identification and investigation of the subject and must clearly be labeled as such.
An individual is arrested for narcotics violations and is believed to be a member of an antigovernment group. The antigovernment group is not suspected of being involved in the subject's narcotics activities.	The name of the individual may be entered into the database. The name of the antigovernment group (political views or associations) cannot be entered into the criminal intelligence database as "noncriminal identifying information" because it is not directly related to the criminal activity of the subject.
A participating agency determines that a gang exists for the principal purpose of illegally manufacturing methamphetamine, and the agency submits the gang name as a subject in the criminal intelligence database based on the documentation of the criminal activity and purpose of the gang.	Any individual identified as a member of the gang can be entered as reasonably suspected of involvement in the criminal activity (manufacturing methamphetamine) of the gang. Project policy (or state law) must establish standards to determine when an individual will be considered a "member" of an identified criminal gang.

Setting Up a Database

A criminal intelligence database is an investigative tool that houses intelligence information related to criminal activity. In addition to other submission criteria, such as reasonable suspicion, the record should be labeled for the confidence level to be provided for each criminal subject (individual or organization) entered into the database. The confidence level has two aspects:

- Source reliability—for example: Reliable, Usually Reliable, Unreliable, Unknown
- Content validity—for example: Confirmed, Probable, Doubtful, Cannot Be Judged

Note: Entering the combination of "Unreliable" or "Unknown" for source reliability and "Cannot Be Judged" for content validity would not meet the 28 CFR Part 23 "reasonable suspicion" standard, and therefore the subject should not be entered into the criminal intelligence database.

In addition, the database should provide:

- The name of the submitting agency and the individual submitter's name.
- All names (individuals or organizations) entered into the database as criminal subjects to be linked to an identifiable criminal activity. These should be required fields.
- Sufficient data to identify the subject (name [mandatory], date of birth, race, sex, address, etc.).
- The capability to label or add appropriate disclaimers for NCII. While NCII may be a searchable field in the criminal intelligence database, it must be clear to the user that the information is NCII and therefore relevant to the identification of the criminal subject.
- Entry of the submission date or the purge date (or both) so that a determination can be made of how long the information has been in the system and when it is due for purge or validation.
- Capturing an audit trail of information disseminated from the database. A record must be kept of who viewed or downloaded (received) the information, the date disseminated, and the reason for release of the information.

Database Operations

Purging or Validating Data

Purging and validation of criminal intelligence information helps to ensure that the information in the system remains current and relevant. Purge requirements should be set forth in the project's operational policy, including, but not limited to, the retention period, who can perform purge activities, and whether there is a validation process.

A criminal intelligence record must be purged from the database by the expiration of its retention period (no longer than five years), unless the record has been reviewed and validated for an additional retention period by the submitting agency.

Validation means the submitter has determined that the subject continues to be reasonably suspected of current involvement in a definable criminal activity or enterprise.

Administrative and Security Issues

There are several security and administrative requirements a criminal intelligence project should ensure are implemented to protect the confidentiality of sensitive information and achieve compliance with the regulation. The project should provide:

- Physical, technical, and administrative security of the system, including user identification, passwords, audit trails, and hardware and software designed to prevent unauthorized access to the information.
- A written agreement signed by each participating agency to certify its commitment to compliance with 28 CFR Part 23 standards and system requirements with regard to criminal intelligence submitted to or received from the criminal intelligence system.
- A process for audit and inspection of backup documentation supporting participating agency submissions to the criminal intelligence database.

In addition, the project must make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation and that its users do not violate the Electronic Communications Privacy Act (Title III) or any applicable federal or state statute related to wiretapping and surveillance during the gathering of information.

Training

Online Training

To facilitate greater understanding of 28 CFR Part 23, BJA has developed online training designed to help SLTT law enforcement agency personnel understand and follow the guidelines that govern the development and implementation of policies and systems that facilitate criminal intelligence sharing. Online training topics include:

- 28 CFR Part 23—An Overview of the Regulation
- Complying With the Regulation
- Submission/Collection, Processing, and Storage of Criminal Intelligence Information
- Inquiry and Dissemination
- Review and Purge or Validate

28 CFR Part 23 online training is available on the National Criminal Intelligence Resource Center Web site (http://www.ncirc.gov) and can be accessed from your secure system or by using the following secure portals:

- RISSNET™: For access to RISSNET, contact the Regional Information Sharing Systems® Center that serves your geographic area. http://www.riss.net/Centers.aspx
- The FBI's Law Enforcement Enterprise Portal (LEEP): Users may also access RISSNET through LEEP. https://www.cjis.gov/CJISEAI/EAIController

Training and Technical Assistance

Training and technical assistance focus on an understanding of the value of intelligence gathering and analysis while complying with 28 CFR Part 23 and the importance and need for law enforcement to protect the privacy and constitutional rights of individuals. The Criminal Intelligence Sharing: Protecting Privacy, Civil Rights, and Civil Liberties Training course expands the discussion of 28 CFR Part 23 to include:

- Intelligence and information sharing trends
- The legal perspective regarding key concepts found in 28 CFR Part 23, such as privacy and reasonableness
- 28 CFR Part 23 and how to apply its principles to everyday situations
- How to limit the potential for violating an individual's privacy, civil rights, and civil liberties while limiting your agency's liability

Training or technical assistance may be requested via e-mail at 28cfr23info@ncirc.gov.

BJA Bureau of Justice Assistance U.S. Department of Justice

This project was supported by Grant Numbers 2010-DG-BX-K044 and 2014-DP-BX-K017, awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the SMART Office. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.