# 28 CFR Part 23

## A Guide to Criminal Intelligence Policies

## Criminal Intelligence Systems Operating Policies (28 CFR Part 23)

28 Code of Federal Regulations (CFR) Part 23 (28 CFR Part 23) is a federal regulation that provides guidance to law enforcement agencies on the implementation standards for operating interjurisdictional and 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*[1] (NCISP) recommends the use of the regulation to ensure that the submission or collection, access or 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 law enforcement agencies adopt the operating principles of 28 CFR Part 23 regardless of whether 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, sharing, and purging criminal intelligence information while ensuring the privacy, civil rights, and civil liberties afforded to all individuals in the United States.

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 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 drug trafficking organization [DTO])
- 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.
  - A criminal gang may qualify as an "organization" for purposes of 28 CFR § 23.20(c). Under state law, criminal gangs are often defined by certain organizational attributes and specified criminal activities. If this is the case, agencies in such states must follow that law in identifying a criminal gang. In the absence of a state law, the project[2] may adopt and use policy criteria for identifying criminal gangs. In both situations, the organization must, at a minimum, be primarily or significantly involved in a "definable criminal activity or enterprise" that meets the submission criteria in 28 CFR § 23.20(a)-(d).
- Once the name of the organization has been 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. To enter an individual's name into the system's database based on gang membership:
  - Step One: The criminal gang must have already been identified and entered into a criminal intelligence database in accordance with state law or in the absence of state law, project policy criteria.
  - Step Two: If the individual is identified as member of that criminal gang (based upon state law criteria, or in its absence, project-established policy criteria for identifying gang members) the individual may then be entered as a criminal subject in a criminal intelligence information record.
  - This line of reasoning applies to any type of criminal organization and its members, employees, etc.
- 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. This responsibility ends when the criminal intelligence information record is purged from the system.

### 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 information 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 and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.
- Do not assume that all individuals who associate with the gang participate in its illegal activities. Non-gang members may be in the company of gang members (e.g., older brother is a member of a known gang, but the younger brother is not).

## Noncriminal Identifying Information (NCII)

- At times, the names and relevant data about individuals or organizations who are not suspected of criminal involvement may provide descriptive, identifying information regarding the criminal subject or the criminal activity in which the subject is engaged. This information may be included in a subject's record in the criminal intelligence database as "noncriminal identifying information" (NCII) under the following circumstances:
  - 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 information 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 DTO is arrested for narcotics violations. The organization is a documented DTO involved in interstate narcotics trafficking. The member is arrested while driving a vehicle registered to his father. The father is not reasonably suspected of involvement in the narcotics trafficking or other criminal activity of the DTO. | The name of the member and the name of the DTO 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 NCII relevant to the individual member of the DTO and must clearly be labeled as such. This rationale applies beyond DTOs to any type of criminal organization and its members, employees, etc. |
| 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 NCII because it is not directly related to the criminal activity of the subject. |
| A participating agency[3] determines that a criminal organization exists for the principal purpose of illegally manufacturing methamphetamine and illegally selling weapons. The agency submits the organization's name as a subject in the criminal intelligence database based on the documentation of the criminal activity and purpose of the organization. | If the individual is identified as member of the criminal organization based upon state law criteria, or in its absence, project-established policy criteria, the individual may be entered as a criminal subject (i.e., reasonably suspected of involvement in the criminal activity of the organization). This rationale applies to any type of criminal organization and its members, employees, etc. |

# 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

28 CFR Part 23 requires that criminal intelligence information be reviewed and validated or purged. The department/agency can set its retention policy but the term for retention cannot exceed five years. This requirement 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 information 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. The submitter can do so by providing additional information about the subject, such as a new criminal associate or involvement in a different criminal activity or updating information about the criminal activity.

## Administrative and Security Issues

There are several security and administrative requirements that 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 information 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. The 28 CFR Part 23 online training is located on the National Criminal Intelligence Resource Center (NCIRC) website at 28cfr.ncirc.gov and is limited to sworn law enforcement, support staff, and approved criminal justice and public safety users.

This training includes an introductory-level overview of the regulation's core principles and provides an understanding of privacy and civil liberties concerns related to criminal intelligence information sharing. The training includes five modules:

1. 28 CFR Part 23—Introduction and Overview
2. How to Comply With the Regulation
3. Submission and Collection Criteria
4. Inquiry and Dissemination Guidelines
5. Retention Issues—Review and Validation or Purge

Users may access the training by logging into an existing registered NCIRC account or may use one of the following three access options:

1. Regional Information Sharing Systems (RISS) Access: RISS members may access the training through the secure RISS portal. Instructions may be found here: https://28cfr.ncirc.gov/documents/Accessing_28CFRPart23_training_RISS.pdf. The 28 CFR Part 23 training program does not manage the RISS website.
2. The FBI's Law Enforcement Enterprise Portal (LEEP) Access: Members with a secure account through the FBI's LEEP may log in to LEEP to access the training. Instructions may be found here: https://28cfr.ncirc.gov/documents/Accessing_28CFRPart23_training_LEEP.pdf. Note: LEEP accounts will need to be marked with the standard "law enforcement designation" which will allow users to see the 28 CFR Part 23 training once signed in to LEEP.
3. Users With an Agency Preauthorization Code: A preauthorization code is provided by a representative within your agency or organization who has been designated to serve as a preauthorization code agent. Users who have been provided a preauthorization code from their agency may register the code here. Note: An agency's assigned preauthorization code cannot be requested through this website or by email. However, users may submit a request to learn if their agency or organization has been assigned a preauthorization code by using the Contact Us form. New preauthorization codes are no longer being issued at this time.

# End Notes

[1] National Criminal Intelligence Sharing Plan, Version 2.0, October 2013, Criminal Intelligence Coordinating Council, Global Justice Information Sharing Initiative, Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, https://bja.ojp.gov/library/publications/national-criminal-intelligence-sharing-plan-building-national-capability.

[2] Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies. 28 CFR § 23.3(b)(5).

[3] Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority, and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system. 28 CFR § 23.3(b)(5).

Revised 10/25/2022

This project was supported by Grant No. 2018-DP-BX-K016 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.