

System Data Fields to Assist in Complying With 28 CFR Part 23

Criminal Activity

- A project must determine what types of offenses will be eligible for inclusion into their criminal intelligence system (§23.30(b)).
 - For a 28 CFR Part 23 compliant criminal intelligence system, the criminal offenses must represent a "significant and recognized threat to the population." This determination, according to the 1993 Revision and Commentary on the regulation, is up to each individual project to determine (in concert with its policy boards and member agencies, if any), provided the additional regulatory requirements set forth in §23.30(b) are met.
 - The additional requirements are that the criminal activities: (1) are either undertaken for the purpose of seeking illegal power or profit or pose a threat to the life and property of citizens; and (2) involve a significant degree of permanent criminal organization; or (3) are not limited to one jurisdiction. If the project determines certain offenses represent a significant and recognized threat to the population, then it must look for compliance with the requirement stated in (1) and then in either (2) or (3).
- National Crime Information Center (NCIC) offenses are recommended as a standard but may not be all inclusive for agency needs.
 - The Office of General Council, Office of Justice Programs, has approved use of the following criminal-activity descriptions; however, each requires the identification of a specific underlying criminal activity.
 - ♦ Terrorism
 - ♦ Security Threat Group
 - ♦ Narcotics
 - ♦ Racketeer Influenced and Corrupt Organization (RICO)
 - ♦ Labor racketeering
 - ♦ Organized crime
 - ♦ Criminal Gang
 - Street Gang
 - Prison Gang

Submission Format

- It is recommended that a project use a standard form or format for the submission of a criminal intelligence record. A project may offer a hardcopy submission form as well as an electronic submission environment.
- It is recommended that the project establish key data fields such as name of subject, type of criminal activity, and levels of sensitivity and confidence as required fields on each submission. This will help ensure that only information which meets all 28 CFR Part 23 operating policy requirements is included as criminal intelligence information.

- It is also recommended that a project request affirmation on each submitted record indicating the information contained in the record meets all 28 CFR Part 23 submission requirements. The regulation requires that a project must either receive sufficient information to make a determination that the reasonable suspicion requirement has been met and that the information was not obtained in violation of applicable federal, state, or local law, or this responsibility may be delegated to the submitting agency (§23.20(c) and (d)). The affirmation could be a statement on a hardcopy submission form that is signed by the submitting officer or a data field in an electronic submission, such as 28 CFR Part 23 COMPLIANCE (yes/no) or both.

Submission Criteria

- Generally, a criminal intelligence record on individuals and organizations may be maintained only if an individual or organization is reasonably suspected of current involvement in criminal activity and the information is relevant to that criminal activity (§23.20(a) and (b)).
 - This provision applies to all names maintained in a criminal intelligence database—primary subjects, associations, gangs, groups, organizations, businesses, employers, employees, relatives, victims, witnesses, attorneys, and so forth.
 - Provisions should be made in the database to link all names entered to a criminal activity or enterprise.
 - Entering information related to political, religious, or social views, associations, or activities of an individual or organization depends on a determination of whether the information *directly* relates to the criminal conduct or activity the subject is reasonably suspected of being involved in (§23.20(b)).
 - ♦ In considering where the line is on whether the identity of a group or individual is the kind of association protected under the regulation, note that it is political, religious, or social associations, but not an association that is generally a business or family relationship (which are fundamentally legal relationships with a social aspect).
 - ♦ When an organization functions as a criminal front or is an organization that exists primarily for the conduct of criminal activity (a criminal enterprise), then individuals who are members of that organization may be presumed to be involved in the organization’s criminal activity and can be included in a criminal intelligence database as criminal associates and/or as criminal subjects in their own right.
 - Information that does not meet the reasonable suspicion requirement but is relevant to the identification of the criminal subject or the criminal activity the subject is engaged in, called “noncriminal identifying information” (NCI), may be entered in a criminal intelligence database under the following circumstances (Policy Clarification issued by BJA, December 1998):

- ♦ The information must be labeled or contain a disclaimer that it is “noncriminal identifying information” carrying no criminal connotation.
- ♦ The criminal subject identified by this information must meet all requirements of 28 CFR Part 23.
- ♦ The identifying information cannot be used independently to meet the reasonable suspicion requirement needed to create a record or file in the database.
- The prohibition on including information on political, religious, and social views, activities, and associations also applies to the inclusion of this type of information as NCI. The 1998 Policy Clarification to the regulation specifies that the waiver on the restriction on entering names of individuals or organizations into a criminal intelligence database is limited to the reasonable suspicion requirement and does not apply to any of the other operating principles or submission criteria outlined in §23.20.

Labeling for Levels of Sensitivity and Confidence

- Information maintained must be labeled to indicate level of sensitivity and level of confidence (§23.20 (g)).
 - The submitting officer/agency or the project determines these levels at the time of submission. These indications help the user assess the value or weight that should be given to the information and protect sensitive investigative information.
- The level of sensitivity indicates the data classification for purposes of dissemination and may restrict who can receive the information or what information, if any, is to be disseminated.
 - This determination allows the submitter to retain control over how the information will be disseminated.
 - Placing a higher level of sensitivity on certain types of information such as civil rights violation, corruption, or political cases allows the information to be included in a criminal intelligence database for use by a specific audience while protecting the sensitivity of the case.
- The level of confidence has two aspects: source reliability and content validity.
 - Source reliability refers to how reliable the source of the information is. Many criminal intelligence databases have established a pick list that the submitter can choose from, such as: reliable, usually reliable, unreliable, or unknown.
 - Content validity refers to the accuracy and/or truthfulness of the information. Many criminal intelligence databases have established a pick list that the submitter can choose from, such as: confirmed, probable, doubtful, or cannot be judged.

- The combination of the lowest descriptors of confidence level (source reliability and content validity) does not meet system submission criteria and cannot be entered into a criminal intelligence database.

Dissemination Record

- An audit trail is required when information is disseminated from a criminal intelligence database. A record must be kept indicating who has been given information, the date the information was disseminated, and reason for release of the information (§23.20 (a) and (b)).
 - This record does not have to be created automatically by the database; policies and procedures could be implemented to handle the audit trail manually.

Retention Period

- All information retained in a criminal intelligence database must be reviewed and validated for continuing compliance with submission criteria before the expiration of its retention period, which in no event shall be longer than five years (§23.20(h)).
 - The project should establish a specific date that it will use to begin the retention period (submission to project, project review, and approval, entry into database, etc.).
 - The project may automatically purge records at the end of the retention period and/or set up a review and validation process.
 - ♦ Certain types of updates may occur prior to the end of the five-year retention period which may automatically extend the retention period. Updates must be substantive updates about the criminal activity of the individual or organization or indicate that the entire submission has been reviewed for currency in order to extend the retention period. Updates to data such as physical description, address, or like data do not qualify for extending the retention period. All information in a record, including any noncriminal identifying information, must be reviewed and validated or purged from the database at the end of the retention period.
 - The review, validation, and purge process may be a manual process, an automated process, or a combination of both.
 - The purge date could be calculated (either manually or automatically) based on the project established start date, or the purge date could be manually entered.
 - ♦ It is recommended that the system be set up to automatically calculate the purge date and purge the record, if not validated before the purge date, in order to avoid human error.