(Agency) Intelligence Database
Procedures and Protocols
(date)

Table of Contents

Part I. Criminal Intelligence Database Description

A. Purpose

The (Agency Name) Criminal Intelligence Database (CID) was created to meet the mandate of (cite laws or policies that cause you to have an intelligence database).

This database provides the (agency) with the ability to determine linkages among criminal individuals and activities in (jurisdiction) and outside of (jurisdiction) if the activity or individual has linkages to (jurisdiction). It also provides the (agency) with the necessary data to coordinate law enforcement efforts across the (jurisdiction). The central collection of information allows the immediate analysis of this data, providing alerts and cautions to State, local and federal law enforcement. It further allows (jurisdiction) to participate in information-sharing networks.

The (Agency name) system's policies are based on 28 C.F.R. 23, which provides standards for multi-jurisdictional information sharing within law enforcement.

B. Definitions

1. "User" is a law enforcement agency participation in the CID system.
2. "Access Officer" is an individual who has met the criteria for being an access officer in the CID system.
3. "Agency" is the (agency name).

Part II. Access to the Criminal Intelligence Database

A. Criteria for Access

Law enforcement agencies designated by the (Agency) will be able to access the CID.

Their access will be contingent on:

1. The signing of a Memorandum of Understanding between the User and the (Agency).
2. Successful completion of training in intelligence and the system guidelines by at least one User staff member.
3. The assignment of at least one person as intelligence coordinator for the User.
4. Ongoing compliance with the approved Information and Intelligence Guidelines and these procedures.

Part III. Protocols for Access

A. User Access Process

1. Potential Users qualified for access will be notified by the (Agency).
2. These potential Users will be sent a packet including:

a. a Memorandum of Understanding,
b. a copy of the Information and Intelligence Guidelines, and
c. a copy of the Criminal Intelligence Database protocols.

3. Potential Users wishing to be granted access will return the Memorandum of Understanding along with a memo stating who their primary contact person will be.

B. Access Termination Provisions

1. Criteria for User Termination
   a. Any breach of security in the CID system caused by an employee of the User, or
   b. Any breach of security in the CID system caused by inadequate security of the User, or
   c. Any violation by the User of federal, state, or local laws or regulations governing the conduct of criminal investigations or the handling of criminal information.

2. Process of Termination
   a. The (Agency head), or a designee, is informed of infraction by CID system supervisor
   b. If necessary, the (Agency head), or a designee, may order the system supervisor to temporarily suspend any access to the system pending the determination of more final action. This is done when continued access could harm the integrity of the system.
   c. System supervisor causes all pertinent information on the infraction to be gathered.
   d. (Agency head), or a designee, reviews information and invites User alleged to have committed the infraction to a meeting to present the User's response to the charges.
   e. Once the User's side is heard, the (Agency head), or a designee, determines if access should be permanently terminated.
   f. The User must return all manuals, logs, updates, and data received through or for the CID system to the system supervisor.

C. Access Officers

1. Criteria for Access Officers
   a. Only those individuals employed by law enforcement agencies are qualified for appointment as Access Officers.
   b. Only those individuals with a need to know the information and a right to know the data in the performance of their law enforcement duties may have access.
   c. Only those individuals who have completed the required CID training may have access.

2. Training for Access
   a. Upon notifying the User of its acceptance into the system, the User will identify access officer (s).

b. The access officers will be contacted by the CID system supervisor to schedule their training.
c. The Access Officers then participate in CID training.
d. The system supervisor gives a password, user manuals and other necessary material to each Access Officer at the training.

3. Access Termination Provisions
   a. Incidents requiring personal termination of access
      i. Termination of an Access Officer's employment with agency
      ii. Transfer of an Access Officer to another function within the user agency
      iii. Personal breach of security of the system
      iv. Violation of User agreement

   b. Process for termination
      i. Voluntary
         (a.) User agency notifies CID system supervisor of the transfer or termination of the Access Officer.
         (b.) CID supervisor deletes the password which allowed that officer to have access
         (c.) Officer returns all CID related material to (agency name).

      ii. Involuntary
         (a.) A personal breach of security is uncovered by the User or CID which involves an Access Officer.
         (b.) The Access Officer's access is immediately terminated by the system supervisor.
         (c.) Charges may be brought against the Officer.
         (d) An investigation into termination procedures for the User agency may ensue.
         (e.) The Access Officer returns all CID materials to (Agency name).

D. Access by (Agency name) Staff

1. CID Analysts – CID analysts will access all programs, equipment and data necessary to fulfill their duties as system employees. This access is for the purpose of assisting inquirers, and analyzing trends, patterns and commonalities for specifically assigned analytical products or projects.

2. (Agency Name) Investigators – (Agency name) Investigators may become Access Officers in a manner similar to the employees of user agencies. As such, they will have entry and inquiry access to the main index and inquiry files.

3. All (Agency name) staff members are required to keep information received from the system in strictest confidence and are not to use their access to obtain data for persons who would otherwise not have access to that data.

4. Any breach in the security of the system caused by an employee may be cause for immediate dismissal.

E. Access Restrictions

1. Entries and Inquiries - Access Officers may make entries to and inquiries of the database.

2. Sensitivity Levels:

A. Sensitive information. This information is the most sensitive data in the CID and will not be disseminated except under very restricted circumstances.

B. Confidential information. This data is less restricted than sensitive data. It will not be provided to inquirers, nor will they be told that a User submitted the data. The submitting User will, instead, be contacted and told who has inquired on the subject. The submitting User may then, at its discretion, contact the inquiring User and share the data.

C. Restricted sensitivity information will be given to inquirers along with submitting User's name for follow-up if additional information is needed.

D. Unclassified information which has been taken from public records or the media will be disseminated to inquirers without restriction.

D. Access Notifications and Verifications

1. The CID system supervisor will cause monthly logs of entries and inquiries to be generated.

2. All inquiries upon a subject in a file will result in the original submitting User to be notified of the inquiry.

3. Multiple entries on a single subject of a non-restricted classification will cause all entering users to be notified of the other entries.

4. Multiple entries on a single subject which include a restricted classification entry will only cause notification to appropriate users of general (not restricted) entries.

5. The CID system supervisor will cause a computerized log to be kept showing all incidence of matches between inquiries and entries. This log, when compared to the log of all records inquired upon, will show the 'hit rate' of the system.

Part IV. Physical Security

A. At the (Agency Name)

1. Location of CID - The CID computer will be located in a secure environment within the Intelligence Center at the (Agency Name). This is part of a secure, patrolled building.

2. The Intelligence Center is a secure section within the building to which access is limited to authorized CID staff and others with a demonstrable need to be on site.

B. At User Locations

1. Access to CID files are restricted only to Access Officers.

2. Users must have the terminal which accesses CID in a secure location which is not in a public area.

Part V. Main Index

A. Entry Criteria

1. An entry on a subject may be made only if the subject is reasonably suspected of being involved in terrorist or criminal activity within the past three (3) years).

    a. Terrorist activity is defined as the financing, support, participation, transportation, or furtherance of any activity deemed by federal or state law to be terroristic. Such acts may include:
        i. Threats to public officials and private citizens
        ii. Arson
        iii. Manufacture, use, or possession of explosive devices for purposes of intimidation or political motivation
        iv. Destruction of public or private property
        v. Releasing harmful biological substances to the public
        vi. Unauthorized detonation of nuclear weapons
        vii. Inciting or encouraging others to participate in terroristic activities
        viii. Soliciting or receiving funds to be used in support of terroristic activities
        ix. Assaults on operators or assistants on public conveyances
        x. Theft of conveyances or materials to be used as terroristic weapons
        xi. Any criminal acts perpetrated by individuals or groups related to terrorism

    b. Criminal activity is defined as any act which is enumerated in federal or state law as being criminal.

c. Reasonable Suspicion is present when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or analyst a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable terrorist or criminal activity or enterprise.

2. Entries are made on individuals, organizations, businesses or groups who are reasonably suspected of having been involved in the actual or attempted planning, organizing, financing, or commission of terrorist acts or are suspected of being or having been involved in criminal activities relating to terrorist acts.

3. No information shall be entered about the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to terrorist or criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in terrorist or criminal conduct.

4. No information will be included which has been obtained in violation of any applicable federal, State, or local law or ordinance.

B. Permanent Status Criteria

1. A subject/entity to be given permanent status must be identifiable—distinguished by a name and unique identifying characteristic (e.g., date of birth, criminal identification number, social security number, alien registration number, driver's license number, address).

2. Modus operandi files which describe a unique method of operation for a specific type of criminal scenario may be included in permanent status regardless of the lack of immediate link to an identifiable suspect.

3. All entries to the index must be reviewed for compliance with policies and criteria prior to being entered into the CID; this review will be completed by an (Agency name) analyst or investigator.

4. All entries will be held in an interim file until such a review is completed; at which time they will be entered into the CID.

C. Inquiries

1. An inquiry may be made only if the subject is reasonably suspected of being involved in terrorist or criminal activity.

2. An inquiry on a subject may only be made if the inquirer is involved in an investigation, prosecution or analysis involving the subject. A case or project number should be provided to substantiate this claim.

D. Temporary Status Criteria

5. A subject/entity upon which an inquiry has been made may be given temporary file status.

6. When a subject/entity is unidentifiable in the immediate future, having no known physical descriptors, identification numbers, or distinguishing characteristics available it may be given temporary file status.

7. When the link to terrorist or criminal activities is questionable the subject/entity may be given temporary file status. This may occur through:

    1. Possible terrorist associations – individual, organization, business or group (not currently reported to be active) associates with a known terrorist and appears to be jointly involved in illegal activities.
    2. Historic associations – individual, organization, business, or group (not currently reported to be active) that has a history of association with persons later known to be involved in terrorist activity and the circumstances currently being reported indicates they may become actively involved in terrorism.

Part VI. Dissemination

A. The (Agency name) shall disseminate intelligence information only to law enforcement authorities which agree to accepted procedures regarding information receipt, maintenance, security, and dissemination.

B. Dissemination shall only occur where there is a need to know and a right to know the information in the performance of a law enforcement activity.

C. Notwithstanding paragraph A of this part, the (agency name) may disseminate an assessment of intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

Part VII. Update or Purge of Materials

A. Any information that has been retained in the system but has not been reviewed for a period of time (shown below) must be reviewed and validated before it can be used or disseminated.

B. Entries

1. All entries will be reviewed on specific schedules to allow for update and possible purging of data due to obsolescence or inaccurateness. The following schedules will be used:

   a. Subjects entered which are currently under investigation will be updated or purged every two years.
   b. Subjects entered which are recently named for participation in terrorist or criminal activity will be updated or purged every five years.
   c. Entries scheduled for update or purge will be flagged by the CID databank. The submitting User will then be required to review the entry, update it or purge it from the files.

C. Inquiries

3. All inquiries will be automatically reviewed by the (Agency name) staff 180 days after their submission.

   a. If no further inquiries or other information has surfaced on the subject; the system will automatically purge the inquiry and notify the inquirer of the action.
   b. If further inquiries have come in on the subject, the information will be retained for 180 beyond the last inquiry.
   c. If the inquiry is on a subject in the CID database, the inquiry remains in the files until that subject is purged.

Part VIII. Sanctions

Particular sanctions are available in law and regulations covering the operations of a law enforcement information system. Following is a listing of some:

A. (Applicable laws governing files).

Part IX. Monitoring and Auditing

A. To ensure system participation and integrity, the (Agency name) will monitor an/or audit all User's participation in the system.

B. Automatic Monitoring

1. The CID has an automatic audit trail built into each access of the database.

2. Each action of an access officer will be recorded in a log including what data was accessed, who accessed the data, the date and time of the access.

C. User Location Site Visits

1. At least once bi-annually, each remote site will be visited to assure that there is adequate security for CID access and information received through the system.

2. Such visits will be completed by (Agency name) staff members.

Part IX. Disaster Preparedness

A. The system supervisor shall ensure the establishment of a documented disaster plan containing, at a minimum, the following elements:

1. Designation of an alternate computer site with sufficient capacity to process the CID workload to be used in the event of system failure.

2. Weekly backup of database content with off-site storage of backup.

3. Procedures to be followed to initiate and maintain operations at the alternate site when needed.

B. Disaster Response Testing

1. The system supervisor shall ensure that testing of all disaster response elements will be undertaken annually to ensure the viability of disaster recovery.

2. A report of this test will be provided to the (Agency head), or a designee.

B. Notification – The (Agency head), or a designee, will be immediately notified of any actual computer disaster.

Part XI. Changes to Protocols

A. All protocols in this manual are agreed to and established by the (Agency head).

B. Any modification of these protocols must be approved by the (Agency head), or a designee. Any routines established based on these protocols may be modified under the responsibility of the CID system supervisor.