Statewide Intelligence System

Sample Operating Policies and Procedures

Mission Statement

To provide a Statewide Intelligence System (SIS) for the timely sharing of criminal intelligence information among law enforcement and criminal justice agency personnel in an effort to prevent and control crime and in conformance with the privacy and constitutional rights of individuals.

Goals

Provide liaison, coordination, and resource assistance in the collection, storage, exchange or dissemination, and analysis of criminal intelligence information in ongoing multijurisdictional investigations or prosecution activities relating to specific areas of criminal activity (see Definitions).

Provide criminal intelligence information to law enforcement and criminal justice agency personnel on individuals and organizations involved in identified criminal organizations and enterprises.

Provide analysis of organized crime and criminal enterprises in [STATE]. This includes identification and/or projection of major changes in crime trends that may require adjustments in resource allocation.

General Operating Policies

Applicability

Federally funded criminal intelligence systems operating funding under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, *et seq*., as amended, are required to comply with the U.S. Department of Justice (DOJ) Criminal Intelligence Systems Operating Policies, 28 CFR Part 23 (hereinafter referred to as 28 CFR Part 23) and the 1998 Policy Clarification (see copy attached as Appendix A). These Sample Operating Policies and Procedures incorporate the 28 CFR Part 23 requirements.

Coordination and Control

By authority of [STATE LAW], the [HEAD] of the [NAME OF LEAD AGENCY] (hereinafter referred to as Lead Agency) or an individual with general policymaking authority who has been expressly delegated by the [HEAD] of the Lead Agency shall be responsible for coordinating the SIS and ensuring that information in the SIS is maintained and transmitted in accordance with the standards set forth in these operating policies and procedures.

SIS Control Group

A SIS Control Group (or Oversight Board) shall be formed to assist the [NAME OF LEAD AGENCY] in establishing policies and developing guidelines for the implementation and operation of the SIS. The SIS Control Group shall also assist the Lead Agency with planning, organizing, managing, and promoting the SIS project. The SIS Control Group members shall be selected from or appointed by a Participating Agency and shall be required to enter into an agreement (see Statewide Intelligence System Control Group Sample Memorandum of Understanding attached as Appendix B) with the [HEAD] of the Lead Agency.

Participation

Participation in the SIS is open to federal, state, county, and local agencies with law enforcement or criminal investigative authority in [STATE].

Agencies participating in the SIS are required to sign a Participation Agreement (see sample copy attached as Appendix C) agreeing to follow the SIS operating policies and comply with 28 CFR Part 23.

The chief executive of each Participating Agency shall designate in writing one or more persons from among the bona fide employees of the Participating Agency to represent the Participating Agency in the SIS. These representatives will be referred to as "Access Officers." The chief executive shall designate one Access Officer as the "Primary Representative." The chief executive may also designate an "Alternate Representative" from among the Access Officers. Both the Primary and Alternate Representatives may remain Access Officers.

The chief executive of the Participating Agency may from time to time change or make new designations and may designate himself/herself as Primary Representative, Alternate Representative, or Access Officer.

Any change in the designation of the Primary Representative shall be in writing from the chief executive of the Participating Agency to the [HEAD] of the Lead Agency. Changes in the Alternate Representative or the Access Officer may be made by written notice from

the Primary Representative unless the chief executive of the Participating Agency chooses to reserve that right.

The Primary Representative of the Participating Agency shall be the primary point of contact between the SIS Lead Agency central staff on administrative matters, and shall monitor agency compliance with the operating principles set forth in these operating policies and procedures.

Participating Agency Access Officers shall attend periodic SIS training and coordination sessions.

Criminal Activity Focus

Criminal intelligence information on individuals and organizations submitted to the SIS shall refer to significant multijurisdictional criminal activities. Some examples of criminal activity categories are:

- Narcotics manufacturing and/or trafficking
- Unlawful gambling
- Loan sharking
- Extortion
- Smuggling
- Vice and pornography
- Infiltration of legitimate businesses for illegitimate purposes
- Stolen securities
- Bribery
- Major crime including homicide, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, forgery, fencing stolen property, and arson
- Manufacture, use, or possession of explosive devices for fraud, intimidation, or political reasons
- Organized crime (see Definitions)
- Corruption of public officials
- Threats to public officials and private citizens

- Traveling criminals (see Definitions)
- Other designated multijurisdictional criminal activities

Operating Procedures

Information Storage and Retrieval System

The [STATE] SIS resides on a host computer system in the [NAME OF LEAD AGENCY] located at [ADDRESS OF THE LEAD AGENCY]. All information contained in the SIS shall be considered the property of the submitting agency and shall not be accessed or disseminated except as provided in these operating policies and procedures.

Submission of Information

All submissions of criminal intelligence information on individuals and organizations to the SIS are the property of the submitting agency.

Information may be submitted in either of two ways:

1. **Direct Entry:** Information may be entered directly from personal computer terminals that are linked by dedicated lines to the [NAME OF LEAD AGENCY] host computer. Screen-handling software and security measures will reside on the personal computer; however, data files and additional security measures will reside on the host computer system.

2. **Indirect Entry:** If an agency does not have an access terminal, information may be submitted on approved forms or in format for entry by SIS-designated personnel. Information can be submitted in person, via telephone, mail, e-mail, or facsimile. Information submission shall be validated by an Access Officer or other designated agency personnel at the time of entry or submission to determine that the submitted information meets the criteria necessary for inclusion in the SIS.

Information Submission Criteria

The Lead Agency shall only collect and maintain criminal intelligence information concerning an individual if there is "reasonable suspicion" that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

The Lead Agency shall not collect or maintain criminal intelligence information 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 criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

Reasonable suspicion or "criminal predicate" is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. The Lead Agency is responsible for establishing the existence of reasonable suspicion of criminal activity, either through examination of supporting information submitted by a Participating Agency or by delegation of this responsibility to properly trained Participating Agency personnel which is subject to routine inspection and audit procedures established by the Lead Agency.

The Lead Agency shall not include in the SIS any information that has been obtained in violation of any applicable federal, state, or local law or ordinance. The Lead Agency is responsible for establishing that no information is entered in the SIS in violation of federal, state, or local laws, either through examination of supporting information submitted by a Participating Agency or by delegation of this responsibility to properly trained Participating Agency personnel, which is subject to routine inspection and audit procedures established by the Lead Agency. Additionally, the subject should be identified by unique identifying characteristics, including but not limited to:

- Full Name
- Address
- Aliases
- Monikers
- Date of Birth
- Place of Birth
- Citizenship (if Alien, Identification Number)
- Social Security Number
- Driver’s License Number
- Physical Description: Height, Weight, Eye and Hair Color
- Violence Potential
- Distinguishing Scars, Marks, or Tattoos
- Criminal Identification Number

- Criminal Activity and/or Offenses
- Modus Operandi (see Definitions)
- Criminal Associates

Information submission criteria should also include the following:

- Date of Submittal of Information
- Name of Submitting Agency
- Submitting Officer's Name

Labeling of Information

Information to be retained in the SIS shall be labeled for source reliability and content validity prior to entry or submission.

Source Reliability

The reliability of the source is an index of the consistency of the information the source provides.

The source shall be evaluated according to the following:

- RELIABLE—The reliability of the source is unquestioned or has been well tested in the past.
- USUALLY RELIABLE—The reliability of the source can usually be relied upon. The majority of the information provided in the past has proved to be reliable.
- UNRELIABLE—The reliability of the source has been sporadic in the past.
- UNKNOWN—The reliability of the source cannot be judged; authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity

The validity of information is an index of the accuracy or truth of the information. The validity of the information shall be assessed as follows:

- CONFIRMED—The information has been corroborated by an investigator or another reliable independent source.
- PROBABLE—The information is consistent with past accounts.
- DOUBTFUL—The information is inconsistent with past accounts.
- CANNOT BE JUDGED—The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

Information maintained in the SIS may be labeled using any combination of the above Source Reliability and Content Validity designations, *except* for the combination of "Unknown" for Source Reliability and "Cannot Be Judged" for Content Validity—this particular combination does not meet reasonable suspicion criteria.

Dissemination Level

The dissemination level is the classification of information and how it is to be shared with other Participating Agencies, if at all. If more than one agency submits information on the same subject and the information is linked in the automated database, the dissemination level viewed in the system must reflect the most restrictive dissemination level. Examples of levels of dissemination of information are:

- OPEN (All Information Released)—All information maintained in the system may be released to the inquiring party. No restrictions of dissemination are applied.
- RELEASE AGENCY NAME ONLY—Only the contributing Agency Name, Unit, Contact, and Contact Phone Number are released. No detailed information on the subject of the inquiry is released. The inquiring agency may contact the submitting agency for detailed information.
- RESTRICTED (No Information Released)—"Hits" or potential "hits" are NOT released. Access to information is restricted and, unless the inquiring party is the contributor of the information, the information may only be viewed by designated Lead Agency personnel. The contributing agency is notified of the "hit" either electronically or by telephone. The contributing agency has the option of whether or not to contact the inquiring agency.

Access Rights

Restrictions on release of the information based on the designated dissemination level are always enforced in the agency inquiry environment with the exception that a contributor of information may view the data he or she submitted regardless of the designated dissemination level.

For system administration and maintenance purposes, designated Lead Agency personnel may have access to all information regardless of the dissemination level.

Participating Agencies have access to any information they submit to the SIS and are responsible for the content, validity, and usefulness. The Primary Representative determines who within the Participating Agency has a need to access the agency's records and to what extent. For example, clerks may be limited to data entry and may not be able to perform queries.

Telephone, e-mail, and facsimile requests for criminal intelligence information will be addressed only after the requester's authorization is determined. If online electronic access is allowed, confirmation may be through use of passwords or other security devices.

Inquiry Procedures

Inquiries can be made without reasonable suspicion of criminal activity; however, for information to be placed in the SIS, reasonable suspicion must be established. [Note: A more restrictive policy may be adopted requiring that reasonable suspicion of criminal activity be established prior to making an inquiry.]

Any authorized Participating Agency employee may initiate an inquiry to the SIS, but information will be disseminated only to designated personnel [such as the Primary Access Officer or Alternate Access Officer] who have authorized access.

Prior to dissemination of information, the identity of the inquiring Access Officer must be confirmed. If online electronic access is allowed, confirmation may be through use of passwords or other security devices.

If access is by telephone, mail, e-mail, or facsimile, the Lead Agency may use a personal data sheet or security control card maintained on file. In this instance, release of information shall be made on a call-back basis only after verification of the identity of the Access Officer.

Dissemination of Information Procedures

The Lead Agency or authorized recipient shall disseminate criminal intelligence information only where there is a need-to-know and a right-to-know the information in the performance of a law enforcement activity.

The Lead Agency shall disseminate criminal intelligence information only to law enforcement or criminal investigative authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with these operating policies and procedures. CAVEAT: This paragraph shall

not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

Dissemination Record

An audit trail or dissemination record is required when information is disseminated from the database. The record shall contain the following information:

- Date of dissemination of the information
- Name of the individual requesting the information
- Name of the agency requesting the information
- Reason for the release of the information (need-to-know/right-to-know)
- Information provided to the requester
- Name of the SIS staff member disseminating the information

This record can be created automatically by the database, or policies and procedures can be implemented to handle the audit trail/dissemination record manually.

Review and Purge Procedures

Reviewing and purging information in the SIS should be done on an ongoing basis. The maximum retention period is five years. [NOTE: Policies can be adopted for a retention period of less than five years.] If the information has not been updated and/or validated, it must be removed from the system at the end of the retention period. The submitting agency may update and/or validate the submission and extend the retention period at any time. Updated or new criminal activity from any Participating Agency may be used to extend the retention period if the original submitting agency is contacted and agrees.

The review, validation, and purge process may be a manual process, or an automated process, or a combination of both. A data field is required so that a determination can be made of how long the information has been in the SIS and when it is due for purging. Purge dates are initially calculated based on the submittal date and the submittal type and can be generated automatically, or the purge date could be manually entered. If a purge date is modified, then all links to the records must be evaluated and modified appropriately.

Procedures for Purge of Information

The Lead Agency may adopt a policy to purge information without notification to the submitting agency or adopt a policy to notify the submitting agency prior to purge of information to provide the submitting agency an opportunity to validate the submission and extend the retention period. The process adopted should not delay purge of information that has reached the end of its retention period; i.e., information may not remain in the database longer than the retention period without validation and updating.

Purge Without Notification to Submitting Agency

The Lead Agency should inform all Participating Agencies of the policy to purge information without notification. It is then incumbent on the submitting agency to track their submissions. If there has been no update or resubmission of the information by the submitting agency, then it is automatically purged at the end of the five-year period.

Notification Prior to Purge

The information can be returned to the submitting agency prior to the end of the established purge period with a request to resubmit the information.

Once a month the Primary Representative for each Participating Agency will be provided with a list of their submissions scheduled to be purged within the next 90 days. If the Participating Agency chooses to retain a submission, it must be validated by an Access Officer. Failure to review and validate the submission will result in the submission being purged at the end of a five-year period [or shorter period established by the Lead Agency].

The Access Officer conducting the review shall make a determination that some or all of the information contained in the submission continues to comply with 28 CFR Part 23 requirements. Information concerning each individual, group, association, corporation, business, or partnership named in the submission shall be reviewed to determine if that individual, group, association, corporation, business, or partnership continues to be reasonably suspected of being involved in the criminal activity described in the submission. If this determination is made, the Access Officer will notify the Lead Agency and the retention period will be extended. All information retained as a result of this review shall reflect the name of the reviewer, date of review, and explanation of decision to retain. If this cannot be established, the name of the individual, group, association, corporation, business, or partnership will be deleted from the database.

The decision to purge information should be guided by the following considerations:

- The number of requests for the file/individual
- The validity of the data

- The reliability of the data
- Federal/state law
- The time in the file
- Present or future strategic or tactical intelligence utility
- Continuing compliance with 28 CFR Part 23 reasonable suspicion criteria and investigative interest of the submitting agency

Any information that is found to be misleading, obsolete, or otherwise unreliable will be purged on an ongoing basis by the Lead Agency and recipient agencies advised of such changes.

Destruction of Information

Material purged from the SIS will be returned to the submitting agency or confidentially destroyed. Only an administrative record of the purge will be maintained. No record of the names of individuals, organizations, etc., that are purged will be maintained by the Lead Agency.

Inspection and Audit of Files

The Lead Agency will periodically conduct audits and inspections of Participating Agency records that support submissions to the SIS database and compliance with operating principles set forth in 28 CFR Section 23.20 with regard to submissions made to the SIS.

The audits and inspections of Participating Agency files will be conducted randomly by a representative of the Lead Agency and are designed to review backup information to ensure continuing compliance with 28 CFR Part 23 is maintained by the submitting agency. A random number of Participating Agencies and a random number of submissions from those agencies will be selected for audit and inspection. The audit and inspection may be conducted onsite at the participating agency or through a mail process requiring certification of continuing compliance by the head of the agency.

Agencies participating in the SIS are not required to, but may, maintain files that support submissions to the SIS and that support compliance with these SIS operating policies and procedures (which incorporate compliance with 28 CFR Part 23) separately from other agency files. Inspection and audit of Participating Agency files will be conducted in such a manner so as to protect the confidentiality and sensitivity of Participating Agency intelligence records.

Security of SIS Files

In order to maintain the confidentiality of stored criminal intelligence information and to ensure the protection of the individual's right to privacy, the [Head] of the Lead Agency, or designee, shall be responsible for implementing the following security requirements for the SIS:

- The SIS database, manual or electronic, shall be located in a physically secured area that is restricted to designated authorized personnel.
- Only designated authorized personnel will have access to information stored in the SIS database.
- All authorized visitors, regardless of agency, are required to register with designated authorized personnel prior to gaining admission to the facility and physical location housing the SIS database.
- All authorized registered visitors will be escorted by designated authorized personnel for the duration of the visit.
- All hardcopy submissions and/or manual files will be secured by Lead Agency designated authorized personnel when not being used and at the end of each shift.
- Employment policies and procedures for screening/rejecting, transferring, or removing personnel having direct access to the SIS will be adopted.
- When direct remote terminal access is authorized by participating agencies, policies and procedures addressing the following additional security measures shall be adopted:
    - Identification of authorized remote terminals and security of terminals
    - Identification and verification of authorized access officer (remote terminal operator)
    - Levels of dissemination of information as directed by the submitting agency
    - Rejection of submissions unless critical data fields are completed
    - Technological safeguards on SIS access, use, dissemination, and review and purge
    - Physical security of the SIS
    - Training and certification of SIS Participating Agency personnel
    - Audits and inspections of SIS Participating Agencies, including: file data supporting submissions to the SIS, security of access terminals, and policy and procedure compliance
    - Documentation for audit trails of the entire SIS operation

Definitions

For the purposes of these operating policies and procedures:

"Criminal activity" is defined as any activity which violates state statutes, ordinances, or codes, and constitutes a criminal act under the law (excluding traffic violations).

"Criminal associate" is defined as an individual who is suspected of maintaining criminal associations and involvement with any individual, group, or organization reasonably suspected of engaging in criminal activity.

"Criminal intelligence information" is defined as data which has been evaluated to determine that it (1) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity; and (2) meets SIS submission criteria.

"Criminal intelligence system" or **"intelligence system"** is defined as the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

"Jurisdictional boundaries" are defined as the area within any city, village, township, or county within the area served by the SIS.

"Lead Agency" is defined as the organization that operates a statewide intelligence system on behalf of a group of Participating Agencies.

"Modus Operandi" is defined as a unique method of operation for a specific type of crime and may not be immediately linked to an identifiable suspect.

"Multijurisdictional" criminal activity is defined as criminal activity that crosses jurisdictional lines and involves two or more separate and distinct jurisdictions.

"Need-to-know" is defined as the necessity to obtain or receive criminal intelligence information in the performance of official responsibilities as a law enforcement or criminal justice authority.

"Organized crime" is defined as any organized group that has its leadership insulated from direct involvement in criminal acts and ensures organizational integrity in the event of a loss of leadership.

"Participating Agency" is defined as 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 a Statewide Intelligence System. A Participating Agency may be a member or a nonmember of a Statewide Intelligence System.

"Reasonable suspicion" or **"criminal predicate"** is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

"Right-to-know" is defined as the legal authority to obtain or receive criminal intelligence information pursuant to court order, statute, or decisional law.

"Statewide Intelligence System" is defined as an intelligence system or criminal intelligence system that involves two or more agencies representing different governmental units or jurisdictions.

"Traveling criminals" is defined as individuals, groups, or organizations engaged in or otherwise associated with criminal activity that traverses jurisdictional boundaries.