Appendices

APPENDIX A

Advisory Board

Advisory Board Members

Doug Bodrero President and CEO Institute for Intergovernmental Research Post Office Box 12729 Tallahassee, FL 32317-2729	Theron Bowman, Ph.D. Chief Arlington, Texas Police Department 620 West Division Street Arlington, TX 76011
Michael A. Braun Acting Assistant Administrator Intelligence Drug Enforcement Administration 700 Army-Navy Drive Arlington, VA 22202	Melvin J. Carraway Superintendent Indiana State Police IGCN - 100 North Senate Avenue Indianapolis, IN 46204-2259
Robert Casey, Jr. Deputy Assistant Director Office of Intelligence, FBI Headquarters 935 Pennsylvania Avenue, NW Washington, DC 20535	Eileen Garry Deputy Director Bureau of Justice Assistance U.S. Department of Justice 810 Seventh Street, NW Washington, DC 20531
Ellen Hanson Chief Lenexa Police Department 12500 W. 87th St. Parkway Lenexa, KS 66215	Gil Kerlikowske Chief Seattle Police Department 610 Fifth Avenue Seattle, WA 98124-4986
William Mizner Chief Norfolk Police Department 202 N. 7th Street Norfolk, NE 68701	William Parrish Senior Representative Dept. of Homeland Security, Liaison Office FBI HQ Room 5885 935 Pennsylvania Avenue, NW Washington, DC 20535
Theodore Quasula Chief Law Enforcement Officer Las Vegas Paiute Tribe Police 1 Paiute Drive Las Vegas, NV 89106	Darrel Stephens Chief Charlotte-Mecklenburg Police Department 601 East Trade Street Charlotte, NC 28202
Bill Young Sheriff Las Vegas Metropolitan Police Department 400 Stewart Avenue Las Vegas, NV 89101-2984	

APPENDIX B

Law Enforcement Intelligence Unit (LEIU) Criminal Intelligence File Guidelines [212]

I. CRIMINAL INTELLIGENCE FILE GUIDELINES

These guidelines were established to provide the law enforcement agency with an information base that meets the needs of the agency in carrying out its efforts to protect the public and suppress criminal operations. These standards are designed to bring about an equitable balance between the civil rights and liberties of citizens and the needs of law enforcement to collect and disseminate criminal intelligence on the conduct of persons and groups who may be engaged in systematic criminal activity.

II. CRIMINAL INTELLIGENCE FILE DEFINED

A criminal intelligence file consists of stored information on the activities and associations of:

A. Individuals who:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

2. Are suspected of being involved in criminal activities with known or suspected crime figures.

B. Organizations, businesses, and groups that:

1. Are suspected of being involved in the actual or attempted planning, organizing, financing, or commission of criminal acts; or

2. Are suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures for use in an illegal manner.

III. FILE CONTENT

Only information with a criminal predicate and which meets the agency's criteria for file input should be stored in the criminal intelligence file. Specifically excluded material includes:

212 Reproduced with permission of the Law Enforcement Intelligence Unit. See the LEIU Homepage at http://www.leiu-homepage.org/.

A. Information on an individual or group merely on the basis that such individual or group supports unpopular causes.

B. Information on an individual or group merely on the basis of ethnic background.

C. Information on any individual or group merely on the basis of religious or political affiliations.

D. Information on an individual or group merely on the basis of non-criminal personal habits.

E. Criminal Offender Record Information (CORI), should be excluded from an intelligence file. This is because CORI may be subject to specific audit and dissemination restrictions which are designed to protect an individual's right to privacy and to ensure accuracy.

F. Also excluded are associations with individuals that are not of a criminal nature.

State law or local regulations may dictate whether or not public record and intelligence information should be kept in separate files or commingled. Some agencies believe that separating their files will prevent the release of intelligence information in the event a subpoena is issued. This belief is unfounded, as all information requested in the subpoena (both public and intelligence) must be turned over to the court. The judge then makes the determination on what information will be released.

The decision to commingle or separate public and intelligence documents is strictly a management decision. In determining this policy, administrators should consider the following:

A. Records relating to the conduct of the public's business that are prepared by a state or local agency, regardless of physical form or characteristics, may be considered public and the public has access to these records.

B. Specific types of records (including intelligence information) may be exempt from public disclosure.

C. Regardless of whether public record information is separated from or commingled with intelligence data, the public may have access to public records.

D. The separation of public information from criminal intelligence information may better protect the confidentiality of the criminal file. If a request is made for public records, an agency can release the public file and leave the intelligence file intact (thus less apt to accidentally disclose intelligence information).

E. Separating of files is the best theoretical approach to maintaining files; however, it is not easy to do. Most intelligence reports either reference public record information or else contain a combination of intelligence and public record data. Thus, it is difficult to isolate them from each other. Maintaining separate public and intelligence files also increases the amount of effort required to index, store, and retrieve information.

IV. FILE CRITERIA

All information retained in the criminal intelligence file should meet file criteria prescribed by the agency. These criteria should outline the agency's crime categories and provide specifics for determining whether subjects involved in these crimes are suitable for file inclusion.

File input criteria will vary among agencies because of differences in size, functions, resources, geographical location, crime problems, etc. The categories listed in the suggested model below are not exhaustive.

A. Permanent Status

1. Information that relates an individual, organization, business, or group is suspected of being involved in the actual or attempted planning, organizing, financing, or committing of one or more of the following criminal acts:

- Narcotic trafficking/manufacturing
- Unlawful gambling
- Loan sharking
- Extortion
- Vice and pornography
- Infiltration of legitimate business for illegitimate purposes
- Stolen securities
- Bribery
- Major crime including homicide, sexual assault, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing stolen property, and arson
- Manufacture, use, or possession of explosive devices for purposes of fraud, intimidation, or political motivation
- Threats to public officials and private citizens.

2. In addition to falling within the confines of one or more of the above criminal activities, the subject/entity to be given permanent status must be identifiable–distinguished by a name and unique identifying characteristics (e.g., date of birth, criminal identification number, driver's license number, address). Identification at the time of file input is necessary to distinguish the subject/entity from existing file entries and those that may be entered at a later time. NOTE: The exception to this rule involves modus operandi (MO) files. MO files describe a unique method of operation for a specific type of crime (homicide, fraud) and may not be immediately linked to an identifiable suspect. MO files may be retained indefinitely while additional identifiers are sought.

B. Temporary Status:

Information that does not meet the criteria for permanent storage but may be pertinent to an investigation involving one of the categories previously listed should be given “temporary” status. It is recommended the retention of temporary information not exceed 1 year unless a compelling reason exists to extend this time period. (An example of a compelling reason is if

several pieces of information indicate that a crime has been committed, but more than a year is needed to identify a suspect.) During this period, efforts should be made to identify the subject/entity or validate the information so that its final status may be determined. If the information is still classified temporary at the end of the 1 year period, and a compelling reason for its retention is not evident, the information should be purged. An individual, organization, business, or group may be given temporary status in the following cases:

1. Subject/entity is unidentifiable – subject/entity (although suspected of being engaged in criminal activities) has no known physical descriptors, identification numbers, or distinguishing characteristics available.

2. Involvement is questionable – involvement in criminal activities is suspected by a subject/entity which has either:

    - Possible criminal associations – individual, organization, business, or group (not currently reported to be criminally active) associates with a known criminal and appears to be jointly involved in illegal activities.

    - Criminal history – individual, organization, business, or group (not currently reported to be criminally active) that has a history of criminal conduct, and the circumstances currently being reported (i.e., new position or ownership in a business) indicates they may again become criminally active.

3. Reliability/validity unknown – the reliability of the information sources and/or the validity of the information cannot be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while verification attempts are made.

V. INFORMATION EVALUATION

Information to be retained in the criminal intelligence file should be evaluated and designated for reliability and content validity prior to filing. The bulk of the data an intelligence unit receives consists of unverified allegations or information. Evaluating the information's source and content indicates to future users the information's worth and usefulness. Circulating information which may not have been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to the agency's operations and contrary to the individual's right to privacy.

To ensure uniformity with the intelligence community, it is strongly recommended that stored information be evaluated according to the criteria set forth below.

Source Reliability:

(A) Reliable – The reliability of the source is unquestioned or has been well tested in the past.

(B) Usually Reliable – The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proven to be reliable.

(C) Unreliable – The reliability of the source has been sporadic in the past.

(D) Unknown –The reliability of the source cannot be judged. Its authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity:

(1) Confirmed – The information has been corroborated by an investigator or another independent, reliable source.

(2) Probable – The information is consistent with past accounts.

(3) Doubtful – The information is inconsistent with past accounts.

(4) Cannot Be Judged – The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

VI. INFORMATION CLASSIFICATION

Information retained in the criminal intelligence file should be classified in order to protect sources, investigations, and the individual's right to privacy. Classification also indicates the internal approval which must be completed prior to the release of the information to persons outside the agency. However, the classification of information in itself is not a defense against a subpoena duces tecum.

The classification of criminal intelligence information is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security classification assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher or lesser degree of document security is required to ensure that information is released only when and if appropriate.

Classification systems may differ among agencies as to the number of levels of security and release authority. In establishing a classification system, agencies should define the types of information for each security level, dissemination criteria, and release authority. The system listed below classifies data maintained in the Criminal Intelligence File according to one of the following categories:

Sensitive

1. Information pertaining to significant law enforcement cases currently under investigation.

2. Corruption (police or other government officials), or other sensitive information.

3. Informant identification information.

4. Criminal intelligence reports which require strict dissemination and release criteria.

Confidential

1. Criminal intelligence reports not designated as sensitive.

2. Information obtained through intelligence unit channels that is not classified as sensitive and is for law enforcement use only.

Restricted

1. Reports that at an earlier date were classified sensitive or confidential and the need for high-level security no longer exists.

2. Nonconfidential information prepared for/by law enforcement agencies.

Unclassified

1. Civic-related information to which, in its original form, the general public had direct access (i.e., public record data).

2. News media information – newspaper, magazine, and periodical clippings dealing with specified criminal categories.

VII. INFORMATION SOURCE

In all cases, source identification should be available in some form. The true identity of the source should be used unless there is a need to protect the source. Accordingly, each law enforcement agency should establish

criteria that would indicate when source identification would be appropriate.

The value of information stored in a criminal intelligence file is often directly related to the source of such information. Some factors to consider in determining whether source identification is warranted include:

- The nature of the information reported.
- The potential need to refer to the source's identity for further or prosecutorial activity.
- The reliability of the source.

Whether or not confidential source identification is warranted, reports should reflect the name of the agency and the reporting individual. In those cases when identifying the source by name is not practical for internal security reasons, a code number may be used. A confidential listing of coded sources of information can then be retained by the intelligence unit commander. In addition to identifying the source, it may be appropriate in a particular case to describe how the source obtained the information (for example "S- 60, a reliable police informant heard" or "a reliable law enforcement source of the police department saw" a particular event at a particular time).

VIII. INFORMATION QUALITY CONTROL

Information to be stored in the criminal intelligence file should undergo a thorough review for compliance with established file input guidelines and agency policy prior to being filed. The quality control reviewer is responsible for seeing that all information entered into the criminal intelligence files conforms with the agency's file criteria and has been properly evaluated and classified.

IX. FILE DISSEMINATION

Agencies should adopt sound procedures for disseminating stored information. These procedures will protect the individual's right to privacy as well as maintain the confidentiality of the sources and the file itself.

Information from a criminal intelligence report can only be released to an individual who has demonstrated both a "need-to-know" and a "right-to-know."

> **"Right-to-know"** Requestor has official capacity and statutory authority to the information being sought.
>
> **"Need-to-know"** Requested information is pertinent and necessary to the requestor agency in initiating, furthering, or completing an investigation.

No "original document" which has been obtained from an outside agency is to be released to a third agency. Should such a request be received, the requesting agency will be referred to the submitting agency for further assistance.

Information classification and evaluation are, in part, dissemination controls. They denote who may receive the information as well as the internal approval level(s) required for release of the information. In order to encourage conformity within the intelligence community, it is recommended that stored information be classified according to a system similar to the following.

The integrity of the criminal intelligence file can be maintained only by strict adherence to proper dissemination guidelines. To eliminate unauthorized use and abuses of the system, a department should utilize a dissemination control form that could be maintained with each stored document. This control form would record the date of the request, the name of the agency and individual requesting the information, the need-to-know, the information provided, and the name of the employee handling the request. Depending upon the needs of the agency, the control form also may be designed to record other items useful to the agency in the management of its operations. This control form also may be subject to discovery.

Security Level	Dissemination Criteria	Release Authority
Sensitive	Restricted to law enforcement personnel having a specific need-to-know and right-to-know	Intelligence Unit Commander
Confidential	Same as for Sensitive	Intelligence Unit Manager or Designee
Restricted	Same as for Sensitive	Intelligence Unit Supervisor or Designee
Unclassified	Not Restricted	Intelligence Unit Personnel

X. FILE REVIEW AND PURGE

Information stored in the criminal intelligence file should be reviewed periodically for reclassification or purge in order to: ensure that the file is current, accurate, and relevant to the needs and objective of the agency; safeguard the individual's right of privacy as guaranteed under federal and state laws; and, ensure that the security classification level remains appropriate.

Law enforcement agencies have an obligation to keep stored information on subjects current and accurate. Reviewing of criminal intelligence should be done on a continual basis as agency personnel use the material in carrying out day-to-day activities. In this manner, information that is no longer useful or that cannot be validated can immediately be purged or reclassified where necessary.

To ensure that all files are reviewed and purged systematically, agencies should develop purge criteria and schedules. Operational procedures for the purge and the method of destruction for purged materials should be established.

A. Purge Criteria:

General considerations for reviewing and purging of information stored in the criminal intelligence file are as follows:

1. Utility

   – How often is the information used?
   – For what purpose is the information being used?
   – Who uses the information?

2. Timeliness and Appropriateness

   – Is this investigation still ongoing?
   – Is the information outdated?
   – Is the information relevant to the needs and objectives of the agency?
   – Is the information relevant to the purpose for which it was collected and stored?

3. Accuracy and Completeness

   Is the information still valid?
   Is the information adequate for identification purposes?
   Can the validity of the data be determined through investigative techniques?

B. Review and Purge Time Schedule:

Reclassifying and purging information in the intelligence file should be done on an ongoing basis as documents are reviewed. In addition, a complete review of the criminal intelligence file for purging purposes should be undertaken periodically. This review and purge schedule can vary from once each year for documents with temporary status to once every 5 years for permanent documents. Agencies should develop a schedule best suited to their needs and should contact their legal counsel for guidance.

C. Manner of Destruction:

Material purged from the criminal intelligence file should be destroyed. Disposal is used for all records or papers that identify a person by name. It is the responsibility of each agency to determine that their obsolete records are destroyed in accordance with applicable laws, rules, and state or local policy.

XI. FILE SECURITY

The criminal intelligence file should be located in a secured area with file access restricted to authorized personnel.

Physical security of the criminal intelligence file is imperative to maintain the confidentiality of the information stored in the file and to ensure the protection of the individual's right to privacy.

GLOSSARY

Public Record

Public record includes any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics.

“Member of the public” means any person, except a member, agent, officer, or employee of a federal, state, or local agency acting within the scope of his or her membership in an agency, office, or employment.

For purposes of these guidelines, public record information includes only that information to which the general public normally has direct access, (i.e., birth or death certificates, county recorder's information, incorporation information, etc.)

Criminal Offender Record Information (CORI)

CORI is defined as summary information to arrests, pretrial proceedings, sentencing information, incarcerations, parole, and probation.

a. Summary criminal history records are commonly referred to as “rap sheets.” Data submitted on fingerprint cards, disposition of arrest and citation forms and probation flash notices create the entries on the rap sheet.

APPENDIX C

Intelligence Unit Management Audit

Audit Factors for the Law Enforcement Intelligence Function[213]

213 Prepared by David L. Carter, Michigan State University, for an audit of the Denver, Colorado Police Department Intelligence Bureau in compliance with a U.S. District Court settlement. Copyright © 2004 by David L. Carter. All rights reserved.

214 http://it.ojp.gov/topic.jsp?topic_id=8

215 http://it.ojp.gov/topic.jsp?topic_id=93

216 http://www.ojp.usdoj.gov/odp/docs/ODPPrev1.pdf

217 http://www.calea.org/newweb/accreditation%20Info/descriptions_of_standards_approv.htm

218 http://it.ojp.gov/process_links.jsp?link_id=3774

219 http://it.ojp.gov/process_links.jsp?link_id=3773

220 http://www.theiacp.org/documents/index.cfm?fuseaction=document&document_type_id=1&document_id=95

221 http://www.theiacp.org/documents/index.cfm?fuseaction=document&document_type_id=1&document_id=94

222 As one good example, see the Santa Clara, CA Police Department's Value Statements at http://www.scpd.org/value_statement.html.

223 http://www.iir.com/28cfr/

Section A. Meeting National Standards

1. Does the police department subscribe to the tenets and standards of the ***Global Justice Information Sharing Initiative***?[214]
   ❑ Yes ❑ No
2. Does the police department subscribe to the standards of the ***National Criminal Intelligence Sharing Plan***?[215]
   ❑ Yes ❑ No
3. Does the police department subscribe to the guidelines for information and intelligence sharing of the Office of Domestic Preparedness ***Guidelines for Homeland Security***?[216]
   ❑ Yes ❑ No
4. Does the police department subscribe to the guidelines of the Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 51.1.1 ***Criminal Intelligence***?[217]
   ❑ Yes ❑ No
5. Does the police department subscribe to the provisions of the International Association of Chiefs of Police (IACP) ***Model Criminal Intelligence Policy***?[218]
   ❑ Yes ❑ No
6. Does the police department subscribe to the standards of the Law Enforcement Intelligence Unit (LEIU) ***Criminal Intelligence File Guidelines***?[219]
   ❑ Yes ❑ No
7. Does the police department subscribe to the IACP ***Code of Ethics***[220] or have an articulated Code of Ethics?
   ❑ Yes ❑ No
8. Does the police department subscribe to the IACP ***Code of Conduct***[221] or have an articulated Code of Conduct?
   ❑ Yes ❑ No
9. Does the police department have an articulated Statement of Values?[222]
   ❑ Yes ❑ No
10. Does the police department adhere to the regulations of 28 CFR Part 23[223] for its Criminal Intelligence Records System?
    ❑ Yes ❑ No

a. Does the police department operate a federally funded multi-jurisdictional criminal intelligence records system?

❑ Yes ❑ No

11. Does the police department subscribe to the tenets of the ***Justice Information Privacy Guidelines***?[224]

❑ Yes ❑ No

12. Does the police department subscribe to the tenets for information system security defined in the report, ***Applying Security Practices to Justice Information Sharing***?[225]

❑ Yes ❑ No

13. Does the law enforcement agency subscribe to the philosophy of ***Intelligence-Led Policing***?[226]

❑ Yes ❑ No

14. Are defined activities for the intelligence unit designed exclusively to prevent and control crime with no political, religious or doctrinal purpose?

❑ Yes ❑ No

224 http://www.ncja.org/pdf/privacyguideline.pdf

225 http://it.ojp.gov/documents/asp/

226 http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport%2Epdf

227 E.g., collection, analysis, collation, dissemination, contact point for other agencies, clearinghouse, etc.

Section B: Management Issues

1. Has a mission statement been written for the Intelligence Unit?

❑ Yes ❑ No

2. Is the purpose and role of the Unit clearly articulated and related to the Police Department's Mission Statement?

❑ Yes ❑ No

3. Have priorities been established for the types of crimes the Unit will address?

❑ Yes ❑ No

a. Is any written rationale provided for these priorities?

❑ Yes ❑ No

4. Are expected activities of the unit articulated?[227]

❑ Yes ❑ No

5. Does the mission statement express ethical standards?

❑ Yes ❑ No

6. Does the mission statement express the importance of protecting citizens' rights?

❑ Yes ❑ No

1. Policies and Procedures

228 The questions in this audit outline the parameters of 28 CFR Part 23 as of the date of this writing. This guideline specifies standards that are required for state and local law enforcement agencies that are operating a federally funded multijurisdictional criminal intelligence system. While the guideline does not apply to all state and local Intelligence Records Systems, the law enforcement intelligence community considers it good practice that all law enforcement agencies should adhere to the standards regardless of whether or not it is formally applicable.

1. Are there written and officially articulated policies and procedures for management of the intelligence function?
   ❑ Yes ❑ No
2. Have intelligence policies been formed to minimize the discretion of information collectors?
   ❑ Yes ❑ No
   If Yes, Describe:

3. Is there a policy and procedures on "Information Collection"?
   ❑ Yes ❑ No
   If Yes, Describe:

2. Management of Information:[228] Definitional Standards (see chart on next page)

1. Are there standard terms used in intelligence activities that have been operationally defined in writing so that all persons in the department know the explicit meaning and implications of the terms?
   ❑ Yes ❑ No
2. What is the source of the definitions?
   ❑ NCISP ❑ Federal Agency
   ❑ Mixed ❑ N/A
3. Has the department articulated standards for classifying information in the Intelligence Unit?
   ❑ Yes ❑ No

Priority	Classification	Description	Release Authority
Highest Level	Sensitive	Current corruption case; complex criminality; confidential informants	Dept Executive or Intelligence Cmdr.
Medium Level	Confidential	Non-sensitive information through intelligence channels; Law Enforcement only	Intelligence Unit Cmdr or Supervisor
Lowest Level	Restricted	LE use but no need for high security	Intell Unit Personnel
Unclassified	Public Access	Information that may be released to public and media	Intell Unit Personnel

4. How are those standards monitored and enforced?
   ❑ Supervisor ❑ Other
5. Does the department have a system for assessing the reliability of sources that provide information that will be retained in the Intelligence Records System?
   ❑ Yes ❑ No
6. Are there standardized definitions of the reliability scale?
   ❑ Yes ❑ No
7. Does the department have a system for assessing the validity of the information that will be retained in the Intelligence Records System?
   ❑ Yes ❑ No
8. Are there standardized definitions of the validity scale?
   ❑ Yes ❑ No
9. Does the Intelligence Unit have operational definitions that can be applied to a person under investigation or a series of related crimes where the perpetrator is not identifiable in order to classify the case file as either a “permanent file” or a “temporary file”?
   ❑ Yes ❑ No
   If Yes…
   a. Are the types of identifying information that should be placed in the file articulated?
   ❑ Yes ❑ No
   b. Is there a procedure for requiring the articulation of the criminal predicate for the permanent file?
   ❑ Yes ❑ No

c. Is there a procedure articulating the conditions wherein a temporary file may be created?

❑ Yes ❑ No

d. Does the procedure specify a time limit that the temporary file can be kept?

❑ Yes ❑ No

e. Is there an operational definition of "Non-Criminal Identifying Information" and procedures for recording and retaining this information?

❑ Yes ❑ No

f. Are there clear procedures that ***describe*** the types of information that should not be entered into the Intelligence Records System?

❑ Yes ❑ No

3. Management of Information: Source Documents

1. Does the department have a written directive explaining the different types of source documents that will be entered in the Intelligence Records System?

   ❑ Yes ❑ No

2. What types of source documents are entered into the Intelligence Records System?[229]

   Describe:

3. Does the police department have a written directive that the rationale for each source document entered into the Intelligence Records System must be articulated in a report or notation?

   ❑ Yes ❑ No

229 For example, Intelligence reports generated by the police department; intelligence reports generated by other agencies; offense reports; arrest reports; criminal history checks; output from consolidated data bases; field interview reports, newspaper and open-source materials, informant statements, etc.

4. Management of Information: Data Entry

1. Who is responsible for entering information into the Intelligence Records System?
   Position/Classification:

2. Who supervises the information entry process?
   Position/Classification:

5. Management of Information: Accountability

1. Who is the Custodian of the Intelligence Records System that ensures all regulations, law, policy and procedures are being followed?
   Position/Classification:
2. Is there a person external to the Intelligence Unit who is designated to monitor the Intelligence Records System and related processes?
   ❑ Yes ❑ No
   If Yes, Position/Classification):

3. Does the department have written procedures for the retention of records in the Intelligence Records System?
   ❑ Yes ❑ No

6. Management of Information: Retention and Purging of Records

1. Does the retention process adhere to the guidelines of 28 CFR Part 23?
   ❑ Yes ❑ No
2. Does the retention policy and procedure include written criteria for purging information?
   ❑ Yes ❑ No

3. How often does a review and purge process occur?
   Frequency:

4. What is the purge process?
   Describe:

5. Does the purge process include a system review of information to confirm its continuing propriety, accuracy and relevancy?
   ❑ Yes ❑ No
6. Does the purge process require destruction of the source document and removal of all references to the document to be purged if the information is no longer appropriate for retention?
   ❑ Yes ❑ No
7. What is the destruction process for purged "hard copy" records?
   Describe:

8. After information has been purged from a computerized Intelligence Records System, is free space on the hard drive and/or specific purged files electronically "wiped"?
   ❑ Yes ❑ No
   a. Are back-ups wiped?
   ❑ Yes ❑ No

b. What is the accountability system for purging back-ups?
Describe:

9. Does the purge process require the elimination of partial information that is no longer appropriate if the source document is to be kept because the remaining information in the source documents merits retention?
❑ Yes ❑ No
10. What is the process for purging partial information from "hard copy" source documents?
Describe:

11. Who is responsible for ensuring compliance of the purge process?
Position/Classification:

7. Management of Information: Personal/Individually-Held Records and Files

1. Is there an intelligence unit policy and procedures concerning the retention of individual notes and records that identifies persons wherein criminality is suspected but is not in either a temporary or permanent file and is not entered into any formal records system or database?
❑ Yes ❑ No

a. How is the possession of personal records monitored?

❑ Yes ❑ No

b. How is the policy enforced?

❑ Yes ❑ No

8. Management of Information: Accessing Intelligence Records

1. Is access to the Intelligence Records limited?

   ❑ Yes ❑ No

2. If yes, who may access the Intelligence Records System?
   Describe:

3. What security controls exist for accessing computerized records?
   Describe:

4. Can the computerized records system be accessed through remote access?

   ❑ Yes ❑ No

   a. If so, what security controls exist for remote access?
   Describe:

5. How are physical records stored?
   Describe:

6. Who grants access privileges to Intelligence Records?
   Position/Classification:

7. Who has access to records?
   Position/Classification:

8. Does the police department apply the Third Agency Rule to information that is shared with other agencies?
   ❑ Yes ❑ No
9. What audit process is in place for access to computerized records?
   Describe:

10. What audit process is in place for access to physical records?
    Describe:

11. How are physical records secured?
    Describe:

12. What process is in place to handle unauthorized access to intelligence physical records?
    Describe:

13. What sanctions are in place for a police department employee who accesses and/or disseminates intelligence records without authorization?
    Describe:

9. Physical Location of the Intelligence Unit and Records

1. Sufficiency: Is the Intelligence Unit in a physical location that has sufficient space to perform all of its responsibilities?
   ❑ Yes ❑ No
2. Security: Is the Intelligence Unit in a physical location wherein the entire workspace may be completely secured?
   ❑ Yes ❑ No

a. Is there adequate secured storage cabinets (or a vault) for (1) documents classified by the Intelligence Unit and (2) sensitive records storage within the Intelligence Unit's physical location?

❑ Yes ❑ No

b. Is there adequate security and segregated storage for federally classified documents within the Intelligence Unit?

❑ Yes ❑ No

1) Is that storage accessible only by persons with a federal top secret security clearance?

❑ Yes ❑ No

3. Convenience: Is the Intelligence Unit in a physical location that is convenient to the people, equipment, and resources necessary to maximize efficiency and effectiveness of operations?

❑ Yes ❑ No

10. Tangential Policy Issues: Criminal Informants and Undercover Operations[230]

1. Is there a formally articulated policy and procedures for managing criminal informants?

❑ Yes ❑ No

a. Is a background investigation conducted and a comprehensive descriptive file completed on each confidential informant?

❑ Yes ❑ No

b. Are informant files secured separately from intelligence files?

❑ Yes ❑ No

2. Is there a formally articulated policy and procedures concerning undercover operations that apply to members of the Intelligence Unit?

❑ Yes ❑ No

3. Does the police department have a policy on alcohol consumption for officers working undercover?

❑ Yes ❑ No

a. Does the police department have a policy requiring designated drivers for undercover officers who have consumed alcohol?

❑ Yes ❑ No

230 The use of criminal informants and undercover operations varies between law enforcement agencies. In some cases these resources may be a functional part of the Intelligence Unit, in other cases they are relied on by the unit for information collection. Understanding the management and control of these activities can be important for the intelligence commander for they can reflect the validity, reliability, and constitutional admissibility of the information collected.

4. Does the police department have a "narcotics simulation" policy and training for undercover officers?
   ❑ Yes ❑ No
5. Does the police department have a policy for the issuance of fictitious identification for undercover officers and the proper use of such fictitious identification?
   ❑ Yes ❑ No
6. Do undercover officers receive training specifically related to proper conduct and information collection while working in an undercover capacity?
   ❑ Yes ❑ No
7. With respect to undercover operating funds:
   a. Is there a 1-tier or 2-tier process to approve use of the funds?
   ❑ 1 Tier ❑ 2 Tier
   b. Is a written report required to document expenditure of the funds?
   ❑ Yes ❑ No
   c. What is the maximum time that may pass between the expenditure of funds and personnel accountability for the funds?
   Days ❑ No Set Time
   d. Is there a regular external audit of undercover funds?
   ❑ Yes [How Often?] ❑ No

Section C: Personnel

1. Is a position classification plan in place that provides a clear job description for each position in the unit?
   ❑ Yes ❑ No
2. Is a position classification plan in place that articulates Knowledge, Skills and Abilities (KSAs) for each position?
   ❑ Yes ❑ No
3. Is there sufficient hierarchical staff (managers/supervisors) assigned to the unit to effectively perform supervisory responsibilities?
   ❑ Yes ❑ No
4. Is there sufficient functional staff (analysts and/or investigators) to effectively fulfill defined unit responsibilities?
   ❑ Yes ❑ No

5. Is there sufficient support staff (secretaries, clerks) to effectively support the unit's activities?
   ❑ Yes ❑ No
6. Does the screening process for nonsworn employees of the intelligence unit require:
   a. Fingerprint check?
   ❑ Yes ❑ No
   b. Background investigation
   ❑ Yes ❑ No
7. If the Intelligence Unit has non-PD employees assigned to it – e.g., National Guard analysts, personnel from the state or local law enforcement agencies – would there be a screening process for those persons?
   ❑ Yes ❑ No
   If Yes, Describe:

1. Training

1. What types of training do preservice and newly assigned personnel receive?
   ❑ None ❑ Some–Describe:

   a. Are newly assigned sworn employees to the Intelligence Unit required to attend 28 CFR Part 23 training?
   ❑ Yes ❑ No
   b. Are newly hired or assigned non-sworn employees required to attend 28 CFR Part 23 training?
   ❑ Yes ❑ No

2. What types of training do in-service personnel receive?[231]

❑ None ❑ Some

Describe:

3. Have members of the Intelligence Unit attended any of the following federal government intelligence training programs which are open to state and local law enforcement officers?

   a. DEA Federal Law Enforcement Analyst Training (FLEAT)?

      ❑ Yes ❑ No

   b. FBI College of Analytic Studies?

      ❑ Yes ❑ No

   c. Federal Law Enforcement Training Center (FLETC) Criminal Intelligence Analysis Training Course?

      ❑ Yes ❑ No

   d. National Drug Intelligence Center Basic Intelligence Analysis Course?

      ❑ Yes ❑ No

   e. National White Collar Crime Center Foundations of Intelligence Analysis?

   ❑ Yes ❑ No

   f. Regional Counterdrug Training Academy Intelligence Operations Course?

   ❑ Yes ❑ No

231 Note: Training should go beyond "the basics" and include updates of law, current crime issues, and trends; new technologies, new resources, etc.

2. Supervision

1. Does supervision effectively monitor adherence to written procedures?

   ❑ Yes ❑ No

2. Does supervision effectively monitor adherence to guidelines adopted by the department?

   ❑ Yes ❑ No

3. Are performance evaluations tied directly to the job descriptions?[232]
   ❑ Yes ❑ No
4. Does supervision effectively monitor the performance of required duties (Including the quality of performance)?
   ❑ Yes ❑ No
5. Is supervision effectively monitoring personnel to ensure civil rights allegations cannot be made with respect to negligent:
   a. Failure to train?
      ❑ Yes ❑ No
   b. Hiring?
      ❑ Yes ❑ No
   c. Failure to supervise?
      ❑ Yes ❑ No
   d. Assignment?
      ❑ Yes ❑ No
   e. Failure to direct?
      ❑ Yes ❑ No
   f. Failure to discipline?
      ❑ Yes ❑ No
   g. Entrustment?
      ❑ Yes ❑ No
6. Is there effective supervision of the Intelligence Unit throughout the chain of command external to the Intelligence Unit?
   ❑ Yes ❑ No

232 Intelligence Unit staff responsibilities are sufficiently different from other police positions that standard performance evaluations typically do not apply (particularly those evaluations that have a quantitative component.

Section D: Fiscal Management

1. Is the budget sufficient to fulfill the stated mission?
   ❑ Yes ❑ No
2. Does the Intelligence Commander have input into the budget planning process?
   ❑ Yes ❑ No

3. Is there over-reliance on "soft money" to operate the unit?[233]
   ❑ Yes ❑ No
4. Are equipment and personnel line items assigned directly to the Intelligence Unit?[234]
   ❑ Yes ❑ No
5. Is there an established process for reliably monitoring credit cards assigned to personnel?
   ❑ Yes ❑ No ❑ NA

Section E: Unit Evaluation

1. As a whole, is the unit effective with respect to:
   a. Providing information to prevent crime?
      ❑ Yes ❑ No
   b. Providing information to apprehend criminals?
      ❑ Yes ❑ No
   c. Effectively analyzing information to identify criminal enterprises, crime trends, criminal anomalies, etc.?
      ❑ Yes ❑ No
2. Are data collected on the following factors and reported in an annual report as indicators of the intelligence unit's productivity as an organizational entity?
   a. Number and type of analytic products delivered for investigative purposes?
      ❑ Yes ❑ No ❑ NA
   b. Number and type of analytic products that led to arrest?
      ❑ Yes ❑ No ❑ NA
   c. Assets seized from illegal activities wherein intelligence contributed to the arrest and/or seizure?
      ❑ Yes ❑ No ❑ NA
   d. Number and types of strategic intelligence products delivered to the command staff?
      ❑ Yes ❑ No ❑ NA
   e. Number of intelligence-sharing meetings attended by unit staff?
      ❑ Yes ❑ No ❑ NA
   f. Number of briefings provided by the intelligence staff?
      ❑ Yes ❑ No ❑ NA

233 For example, grants, cooperative agreements, contracts with other agencies, etc.

234 N.B.: If they are not specifically assigned, then they can be withdrawn more easily.

g. Total number of queries into the intelligence data base?
❑ Yes ❑ No ❑ NA

h. Number of permanent files opened?
❑ Yes ❑ No ❑ NA

i. Number of temporary files investigated?
❑ Yes ❑ No ❑ NA

j. Number of requests for information to the unit from outside agencies?
❑ Yes ❑ No ❑ NA

3. Are products produced by the Intelligence Unit:
   a. In a consistent format?
   ❑ Yes ❑ No
   b. Easily consumed and used (i.e., understandable and actionable)?
   ❑ Yes ❑ No
   c. Contain timely information and disseminated in a timely manner?
   ❑ Yes ❑ No
   d. Have substantive contact to aid in preventing or controlling crime?
   ❑ Yes ❑ No

4. Given the confidential nature of the information contained in the Intelligence Unit, is there a policy and procedures if a city, county, state, or federal fiscal or program auditor seeks to audit the Intelligence Unit?
   ❑ Yes ❑ No
   If Yes, Describe:

Section F. Collection

1. Is there an articulated collection plan for the Intelligence Unit?
   ❑ Yes ❑ No
   If Yes, Describe:

   a. How often and when is the plan updated?
      Describe:

2. Have the following activities been performed by the Intelligence Unit:
   a. An inventory of threats in the region posed by criminal enterprises, terrorists, and criminal extremists?
   ❑ Yes ❑ No
   b. An assessment of the threats with respect to their probability of posing a criminal or terrorist threat to the region?
   ❑ Yes ❑ No
   c. A target or criminal commodity analysis of the region?
   ❑ Yes ❑ No
   d. A target or criminal commodity vulnerability assessment in the region?
   ❑ Yes ❑ No
3. For each identified threat, have intelligence requirements been articulated?
   ❑ Yes ❑ No

a. If Yes, Describe the methods of collection that will be used to fulfill those intelligence requirements.

Section G: Technology and Networking

1. Are any members of the Intelligence Unit subscribed members to the FBI's secure Email system Law Enforcement Online (LEO)?
   ❑Yes-All ❑ Yes-Some ❑ No
2. Are any members of the Intelligence Unit subscribed members to the secure Regional Information Sharing System (RISS) email system riss.net?
   ❑ Yes-All ❑ Yes-Some ❑ No
   a. If yes, are the RISS databases (e.g., RISS.gang, ATIX, etc.) regularly used?
   ❑ Yes ❑ No
3. Is the police department a member of the Regional Information Sharing System?[235]
   ❑ Yes ❑ No
4. Is a systematic procedure in place to ensure that advisories and notifications transmitted via the National Law Enforcement Teletype System (NLETS) are forwarded to the Intelligence Unit?
   ❑ Yes ❑ No
5. Are you connected to any state-operated intelligence or information networks?
   ❑ Yes ❑ No
   If Yes, Describe:

235 The six Regional Information Sharing System centers are: MAGLOCLEN, MOCIC, NESPIN, RMIN, ROCIC, WSIN. See http://www.iir.com/riss/RISS_centers.htm.

6. Are you connected to any regional intelligence or information networks (including HIDTA)?
   ❑ Yes ❑ No
   If Yes, Describe:

7. Does the intelligence have access and use the National Virtual Pointer[236] System (NVPS)?[237]
   ❑ Yes ❑ No
8. Is there a formal approval process for entering into a memorandum of understanding (MOU) for information and intelligence sharing with other law enforcement agencies or law enforcement intelligence entities?
   ❑ Yes ❑ No
   If Yes, Describe the process:

   Who must approve the MOU?

236 A Pointer System – also known as a deconfliction center – determines when two different agencies are investigating the same criminal incident to same person. Since two agencies are investigating the same entity, they are possibly in conflict. In order to "deconflict", the pointer system notifies both agencies of their mutual interest in a case/person in order to avoid duplication of effort, conflicting approaches, and increasing efficiency and effectiveness.

237 NVPS integrates HIDTA, NDPIX, and RISS pointers via secure web-based communications.

Section H: Legal Issues

1. Is there a designated person in the police department who reviews Freedom of Information Act requests directed to the intelligence unit?
   ❑ Yes ❑ No
2. Is there a designated person in the police department who responds to Privacy Act inquiries directed to the intelligence unit?
   ❑ Yes ❑ No

3. Is there a designated person the police department contacts in response to a subpoena for a file in the Intelligence Records System?
   ❑ Yes ❑ No
4. Does the Intelligence Unit Commander have a legal resource for advice to help protect intelligence records from objectionable access?
   ❑ Yes ❑ No
5. Does the Intelligence Unit Commander have a legal resource for advice on matters related to criminal procedure and civil rights?
   ❑ Yes ❑ No
6. Does the Intelligence Unit Commander have a legal resource for advice on matters related to questions of civil liability as it relates to all aspects of the intelligence function?
   ❑ Yes ❑ No
7. Has legal counsel reviewed and approved all policies and procedures of the intelligence unit?
   ❑ Yes ❑ No

APPENDIX D

28 CFR Part 23

28 CFR Part 23
Criminal Intelligence Systems Operating Policies[238]

1. Purpose.
2. Background.
3. Applicability.
4. Operating principles.
5. Funding guidelines.
6. Monitoring and auditing of grants for the funding of intelligence systems.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

238 Based on Executive Order 12291, February 17, 1981. The list of executive orders can be found at the National Archive website: http://www.archives.gov/. The most current text of 28 CFR Part 23 can be found at the Library of Congress website by retrieving the regulation from the Code of Federal Regulations (CFR) search engine at: http://www.gpoaccess.gov/cfr/index.html.

§ 23.3 Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) 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 (ii) meets criminal intelligence system submission criteria; (4) 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; (5) 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; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only 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.

(b) A project 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.

(c) 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. In an interjurisdictional intelligence system, the project 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 a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered 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 a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project 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.

(f) (1) Except as noted in paragraph (f) (2) of this section, a project shall disseminate criminal intelligence information only to law enforcement

authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f) (1) of this section 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.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines.

The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits 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.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity, and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20.

The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

28 CFR Part 23: 1993 Revision and Commetary Criminal Intelligence Systems Operating Policies

AGENCY: Office of Justice Programs, Justice.

ACTION: Final Rule

SUMMARY: The regulation governing criminal intelligence systems operating through support under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, is being revised to update basic authority citations and nomenclature, to clarify the applicability of the regulation, to define terms, and to modify a number of the regulation's operating policies and funding guidelines.

EFFECTIVE DATE: September 16, 1993

FOR FURTHER INFORMATION CONTACT: Paul Kendall, Esquire, General Counsel, Office of Justice Programs, 633 Indiana Ave., NW, Suite 1245-E, Washington, DC 20531, Telephone (202) 307-6235.

SUPPLEMENTARY INFORMATION: The rule which this rule supersedes had been in effect and unchanged since September 17, 1980. A notice of proposed rulemaking for 28 CFR part 23, was published in the Federal Register on February 27, 1992, (57 FR 6691).

The statutory authorities for this regulation are section 801(a) and section 812(c) of title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). 42 U.S.C. 3789g (c) and (d) provide as follows:

CONFIDENTIALITY OF INFORMATION

Sec. 812....

(c) All criminal intelligence systems operating through support under this title shall collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the

funding and operation of these systems furthers the purpose of this title and to assure that such systems are not utilized in violation of the privacy and constitutional rights of individuals.
(d) Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law.

28 CFR Part 23: 1998 Policy Clarification Criminal Intelligence Systems Operating Policies

[Federal Register: December 30, 1998 (Volume 63, Number 250)]
[Page 71752-71753]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
DEPARTMENT OF JUSTICE
28 CFR Part 23
[OJP(BJA)-1177B]
RIN 1121-ZB40

CRIMINAL INTELLIGENCE SHARING SYSTEMS; POLICY CLARIFICATION

AGENCY: Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), Justice.

ACTION: Clarification of policy.

SUMMARY: The current policy governing the entry of identifying information into criminal intelligence sharing systems requires clarification. This policy clarification is to make clear that the entry of individuals, entities and organizations, and locations that do not otherwise meet the requirements of reasonable suspicion is appropriate when it is done solely for the purposes of criminal identification or is germane to the criminal subject's criminal activity. Further, the definition of “criminal intelligence system” is clarified.

EFFECTIVE DATE: This clarification is effective December 30, 1998.

FOR FURTHER INFORMATION CONTACT: Paul Kendall, General Counsel, Office of Justice Programs, 810 7th Street N.W, Washington, DC 20531, (202) 307-6235.

SUPPLEMENTARY INFORMATION: The operation of criminal intelligence information systems is governed by 28 CFR Part 23. This regulation was written to both protect the privacy rights of individuals and to encourage and expedite the exchange of criminal intelligence information between and among law enforcement agencies of different jurisdictions. Frequent interpretations of the regulation, in the form of policy guidance and correspondence, have been the primary method of ensuring that advances in technology did not hamper its effectiveness.

COMMENTS

The clarification was opened to public comment. Comments expressing unreserved support for the clarification were received from two Regional Intelligence Sharing Systems (RISS) and five states. A comment from the Chairperson of a RISS, relating to the use of identifying information to begin new investigations, has been incorporated. A single negative comment was received, but was not addressed to the subject of this clarification.

Use of Identifying Information

28 CFR 23.3(b)(3) states that criminal intelligence information that can be put into a criminal intelligence sharing system is "information 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 *** [m]eets criminal intelligence system submission criteria." Further, 28 CFR 23.20(a) states that a system shall only collect information on 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." 28 CFR 23.20(b) extends that limitation to collecting information on groups and corporate entities.

In an effort to protect individuals and organizations from the possible taint of having their names in intelligence systems (as defined at 28 C.F.R. Sec. 23.3(b)(1)), the Office of Justice Programs has previously interpreted this

section to allow information to be placed in a system only if that information independently meets the requirements of the regulation. Information that might be vital to identifying potential criminals, such as favored locations and companions, or names of family members, has been excluded from the systems. This policy has hampered the effectiveness of many criminal intelligence sharing systems.

Given the swiftly changing nature of modern technology and the expansion of the size and complexity of criminal organizations, the Bureau of Justice Assistance (BJA) has determined that it is necessary to clarify this element of 28 CFR Part 23. Many criminal intelligence databases are now employing "Comment" or "Modus Operandi" fields whose value would be greatly enhanced by the ability to store more detailed and wide-ranging identifying information. This may include names and limited data about people and organizations that are not suspected of any criminal activity or involvement, but merely aid in the identification and investigation of a criminal suspect who independently satisfies the reasonable suspicion standard.

Therefore, BJA issues the following clarification to the rules applying to the use of identifying information. Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information 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; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23. This information may be a searchable field in the intelligence system.

For example: A person reasonably suspected of being a drug dealer is known to conduct his criminal activities at the fictional "Northwest Market." An agency may wish to note this information in a criminal intelligence database, as it may be important to future identification of the suspect. Under the previous interpretation of the regulation, the entry of "Northwest Market" would not be permitted, because there was no

reasonable suspicion that the "Northwest Market" was a criminal organization. Given the current clarification of the regulation, this will be permissible, provided that the information regarding the "Northwest Market" was clearly noted to be non-criminal in nature. For example, the data field in which "Northwest Market" was entered could be marked "Non-Criminal Identifying Information," or the words "Northwest Market" could be followed by a parenthetical comment such as "This organization has been entered into the system for identification purposes only-it is not suspected of any criminal activity or involvement." A criminal intelligence system record or file could not be created for "Northwest Market" solely on the basis of information provided, for example, in a comment field on the suspected drug dealer. Independent information would have to be obtained as a basis for the opening of a new criminal intelligence file or record based on reasonable suspicion on "Northwest Market." Further, the fact that other individuals frequent "Northwest Market" would not necessarily establish reasonable suspicion for those other individuals, as it relates to criminal intelligence systems.

THE DEFINITION OF A "CRIMINAL INTELLIGENCE SYSTEM"

The definition of a "criminal intelligence system" is given in 28 CFR 23.3(b)(1) as the "arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information ***." Given the fact that cross-database searching techniques are now common-place, and given the fact that multiple databases may be contained on the same computer system, BJA has determined that this definition needs clarification, specifically to differentiate between criminal intelligence systems and non-intelligence systems.

The comments to the 1993 revision of 28 CFR Part 23 noted that "[t]he term 'intelligence system' is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation ***." 58 FR 48448-48449 (Sept. 16,

1993.) The comments further noted that materials that "may assist an agency to produce investigative or other information for an intelligence system ***" do not necessarily fall under the regulation. Id.

The above rationale for the exclusion of non-intelligence information sources from the definition of "criminal intelligence system," suggests now that, given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, and other public record information on-line, such sources shall not be considered part of criminal intelligence systems, and shall not be covered by this regulation, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23. There is also no limitation on such non-intelligence information being stored on the same computer system as criminal intelligence information, provided that sufficient precautions are in place to separate the two types of information and to make it clear to operators and users of the information that two different types of information are being accessed.

Such precautions should be consistent with the above clarification of the rule governing the use of identifying information. This could be accomplished, for example, through the use of multiple windows, differing colors of data or clear labeling of the nature of information displayed.

APPENDIX E

FBI Security Clearance

Federal Security Clearance Process for the FBI

It is the policy of the Federal Bureau of Investigation (FBI) to share with Law Enforcement personnel pertinent information regarding terrorism. In the past, the primary mechanism for such information sharing was the Joint Terrorism Task Force (JTTF). In response to the terrorist attack on America on September 11, 2001, the FBI established the State and Local Law Enforcement Executives and Elected Officials Security Clearance Initiative. This program was initiated to brief officials with an established "need-to-know" on classified information that would or could affect their area of jurisdiction.

Most information needed by state or local law enforcement can be shared at an unclassified level. In those instances where it is necessary to share classified information, it can usually be accomplished at the Secret level. This brochure describes when security clearances are necessary and the notable differences between clearance levels. It also describes the process involved in applying and being considered for a clearance. State and local officials who require access to classified material must apply for a security clearance through their local FBI Field Office. The candidate should obtain from their local FBI Field Office a Standard Form 86 (SF 86), Questionnaire for National Security Positions; and two FD-258 (FBI applicant fingerprint cards). One of two levels of security clearance, Secret or Top Secret, may be appropriate.

The background investigation and records checks for Secret and Top Secret security clearance are mandated by Presidential Executive Order (EO). The EO requires these procedures in order for a security clearance to be granted; the FBI does not have the ability to waive them.

Secret Clearances

A Secret security clearance may be granted to those persons that have a "need-to-know" national security information, classified at the Confidential or Secret level. It is generally the most appropriate security clearance for state and local law enforcement officials that do not routinely work on an

FBI Task Force or in an FBI facility. A Secret security clearance takes the least amount of time to process and allows for escorted access to FBI facilities.

The procedure is as follows:

FBI performs record checks with various Federal agencies and local law enforcement, as well as, a review of credit history.

Candidate completes forms SF-86 and FD-258. Once favorably adjudicated for a Secret security clearance, the candidate will be required to sign a Non-Disclosure Agreement.

Top Secret Clearances

A Top Secret clearance may be granted to those persons who have a "need-to-know" national security information, classified up to the Top Secret level, and who need unescorted access to FBI facilities, when necessary. This type of clearance will most often be appropriate for law enforcement officers assigned to FBI Task Forces housed in FBI facilities. In addition to all the requirements at the Secret level, a background investigation, covering a 10-year time period, is required. Once favorably adjudicated for a Top Secret security clearance, the candidate will be required to sign a Non-Disclosure Agreement.

Questions and Answers (Q&A)

Q: Who should apply for a security clearance?
A: State or local officials whose duties require that they have access to classified information, and who are willing to undergo a mandatory background investigation.
Q: What is the purpose of a background investigation?
A: The scope of the investigation varies with the level of the clearance being sought. It is designed to allow the government to assess whether a candidate is sufficiently trustworthy to be granted access to classified information. Applicants must meet certain criteria, relating to

their honesty, character, integrity, reliability, judgment, mental health, and association with undesirable persons or foreign nationals.

Q: If an individual occupies an executive position with a law enforcement agency, must he or she still undergo a background investigation in order to access classified information?

A: An Executive Order (EO), issued by the President, requires background investigations for all persons entrusted with access to classified information. The provisions of the EO are mandatory, cannot be waived, and apply equally to all federal, state, and local law enforcement officers. This is true of both Secret and Top Secret security clearances.

Q: How long does it normally take to obtain a Secret security clearance?

A: It is the goal of the FBI to complete the processing for Secret security clearances within 45 to 60 days, once a completed application is submitted. The processing time for each individual case will vary depending upon its complexity.

Q: How long does it normally take to obtain a Top Secret security clearance?

A: It is the goal of the FBI to complete the processing for Top Secret security clearances within 6 to 9 months, once a completed application is submitted. The processing time for each individual case will vary depending upon its complexity

Q: What kind of inquiries will the FBI make into my background?

A: Credit and criminal history checks will be conducted on all applicants. For a Top Secret security clearance, the background investigation includes additional record checks which can verify citizenship for the applicant and family members, verification of birth, education, employment history, and military history. Additionally, interviews will be conducted of persons who know the candidate, and of any spouse divorced within the past ten years. Additional interviews will be conducted, as needed, to resolve any inconsistencies. Residences will be confirmed, neighbors interviewed, and public records queried for information about bankruptcies, divorces, and criminal or civil litigation. The background investigation may be expanded if an applicant has resided abroad, or has a history of mental disorders, or drug or alcohol abuse. A personal interview will be conducted of the candidate.

Q: If I have a poor credit history, or other issues in my background, will this prevent me from getting a security clearance?

A: A poor credit history, or other issues, will not necessarily disqualify a candidate from receiving a clearance, but resolution of the issues will likely take additional time. If the issues are significant, they may prevent a clearance from being approved.

Q: If I choose not to apply for a security clearance, will I still be informed about counterterrorism issues important to my jurisdiction?

A: Absolutely. If the FBI receives information relevant to terrorism which may impact your jurisdiction, you will be informed by your local Field Office, through the Law Enforcement On- Line network, via NLETS, and through other available mechanisms which are approved for the transmission of unclassified information. Most terrorism-related information can be provided in an unclassified form.

Q: Are there any other advantages or disadvantages to receiving unclassified or classified terrorism related information?

A: An additional advantage of receiving unclassified terrorism-related information is that there may be fewer restrictions on your ability to further disseminate it within your jurisdiction. Classified information may only be disseminated to other cleared persons, who also have a need-to-know.

Q: What is the difference between an interim and a full security clearance?

A: Interim clearances are granted in exceptional circumstances where official functions must be performed before completion of the investigative and adjudicative processes associated with the security clearance procedure. There is no difference between an interim and a full security clearance as it relates to access to classified information. However, when such access is granted, the background investigation must be expedited, and, if unfavorable information is developed at anytime, the interim security clearance may be withdrawn.

If you have any additional questions, and/or wish to apply for a security clearance, please contact your local FBI field office. (See http://www.fbi.gov/contact/fo/fo.htm to locate the nearest field office.)

APPENDIX F

Biography of David L. Carter, Ph.D.

David L. Carter (Ph.D., Sam Houston State University) is a professor in the School of Criminal Justice and director of the Intelligence Program at Michigan State University. A former Kansas City, Missouri police officer, Dr. Carter was chairman of the Department of Criminal Justice at the University of Texas-Pan American in Edinburg, Texas for 9 years prior to his appointment at Michigan State in 1985. He has served as a trainer, consultant, and advisor to many law enforcement agencies throughout the U.S., Europe, and Asia on matters associated with officer behavior, community policing, law enforcement intelligence, and computer crime. In addition, he has presented training sessions at the FBI National Academy, the FBI Law Enforcement Executive Development Seminar (LEEDS); the International Law Enforcement Academy in Budapest, Hungary; the United Nations Asia and Far East Institute (UNAFEI) in Tokyo; police "command colleges" of Texas, Florida, Ohio, Massachusetts, Wisconsin, and Kentucky; and served at the FBI Academy's Behavioral Science Services Unit the first academic faculty exchange with the Bureau. Dr. Carter is also an instructor in the Bureau of Justice Assistance SLATT program, author of the COPS-funded publication, ***Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement***, and project director of the managerial intelligence training program funded by the Department of Homeland Security. He is a fellowship recipient from the Foundation for Defending Democracies where he studied terrorism in Israel. In addition to teaching graduate and undergraduate courses at Michigan State, Dr. Carter is director of the Criminal Justice Overseas Study Program to England. He is the author or co-author of five books and numerous articles and monographs on policing issues and is a member of the editorial boards of various professional publications. His most recent book is the seventh edition of the widely-used community relations textbook, ***The Police and Community***, (published by Prentice-Hall). He has another book forthcoming from Prentice-Hall entitled ***Homeland Security for State and Local Police***.

APPENDIX G

Intelligence Unit Management Audit
(Tear-Out Section)

Audit Factors for the Law Enforcement Intelligence Function

Section A. Meeting National Standards

1. Does the police department subscribe to the tenets and standards of the ***Global Justice Information Sharing Initiative***?
   ❑ Yes ❑ No
2. Does the police department subscribe to the standards of the ***National Criminal Intelligence Sharing Plan***?
   ❑ Yes ❑ No
3. Does the police department subscribe to the guidelines for information and intelligence sharing of the Office of Domestic Preparedness ***Guidelines for Homeland Security***?
   ❑ Yes ❑ No
4. Does the police department subscribe to the guidelines of the Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 51.1.1 ***Criminal Intelligence***?
   ❑ Yes ❑ No
5. Does the police department subscribe to the provisions of the International Association of Chiefs of Police (IACP) ***Model Criminal Intelligence Policy***?
   ❑ Yes ❑ No
6. Does the police department subscribe to the standards of the Law Enforcement Intelligence Unit (LEIU) ***Criminal Intelligence File Guidelines***?
   ❑ Yes ❑ No
7. Does the police department subscribe to the IACP ***Code of Ethics*** or have an articulated Code of Ethics?
   ❑ Yes ❑ No
8. Does the police department subscribe to the IACP ***Code of Conduct*** or have an articulated Code of Conduct?
   ❑ Yes ❑ No
9. Does the police department have an articulated Statement of Values?
   ❑ Yes ❑ No

Law Enforcement Intelligence:
A Guide for State, Local, and Tribal Law Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University

10. Does the police department adhere to the regulations of 28 CFR Part 23 for its Criminal Intelligence Records System?
    ❑ Yes ❑ No
    a. Does the police department operate a federally funded multi-jurisdictional criminal intelligence records system?
    ❑ Yes ❑ No
11. Does the police department subscribe to the tenets of the ***Justice Information Privacy Guidelines***?
    ❑ Yes ❑ No
12. Does the police department subscribe to the tenets for information system security defined in the report, ***Applying Security Practices to Justice Information Sharing***?
    ❑ Yes ❑ No
13. Does the law enforcement agency subscribe to the philosophy of ***Intelligence-Led Policing***?
    ❑ Yes ❑ No
14. Are defined activities for the intelligence unit designed exclusively to prevent and control crime with no political, religious or doctrinal purpose?
    ❑ Yes ❑ No

Section B: Management Issues

1. Has a mission statement been written for the Intelligence Unit?
   ❑ Yes ❑ No
2. Is the purpose and role of the Unit clearly articulated and related to the Police Department's Mission Statement?
   ❑ Yes ❑ No
3. Have priorities been established for the types of crimes the Unit will address?
   ❑ Yes ❑ No
   a. Is any written rationale provided for these priorities?
   ❑ Yes ❑ No
4. Are expected activities of the unit articulated?
   ❑ Yes ❑ No
5. Does the mission statement express ethical standards?
   ❑ Yes ❑ No

6. Does the mission statement express the importance of protecting citizens' rights?
   ❑ Yes ❑ No

1. Policies and Procedures

1. Are there written and officially articulated policies and procedures for management of the intelligence function?
   ❑ Yes ❑ No
2. Have intelligence policies been formed to minimize the discretion of information collectors?
   ❑ Yes ❑ No
   If Yes, Describe:

3. Is there a policy and procedures on "Information Collection"?
   ❑ Yes ❑ No
   If Yes, Describe:

2. Management of Information: Definitional Standards

1. Are there standard terms used in intelligence activities that have been operationally defined in writing so that all persons in the department know the explicit meaning and implications of the terms?
   ❑ Yes ❑ No
2. What is the source of the definitions?
   ❑ NCISP ❑ Federal Agency
   ❑ Mixed ❑ N/A

3. Has the department articulated standards for classifying information in the Intelligence Unit?

❑ Yes ❑ No

Priority	Classification	Description	Release Authority
Highest Level	Sensitive	Current corruption case; complex criminality; confidential informants	Dept Executive or Intelligence Cmdr.
Medium Level	Confidential	Non-sensitive information through intelligence channels; Law Enforcement only	Intelligence Unit Cmdr or Supervisor
Lowest Level	Restricted	LE use but no need for high security	Intell Unit Personnel
Unclassified	Public Access	Information that may be released to public and media	Intell Unit Personnel

4. How are those standards monitored and enforced?

❑ Supervisor ❑ Other

5. Does the department have a system for assessing the reliability of sources that provide information that will be retained in the Intelligence Records System?

❑ Yes ❑ No

6. Are there standardized definitions of the reliability scale?

❑ Yes ❑ No

7. Does the department have a system for assessing the validity of the information that will be retained in the Intelligence Records System?

❑ Yes ❑ No

8. Are there standardized definitions of the validity scale?

❑ Yes ❑ No

9. Does the Intelligence Unit have operational definitions that can be applied to a person under investigation or a series of related crimes where the perpetrator is not identifiable in order to classify the case file as either a “permanent file” or a “temporary file”?

❑ Yes ❑ No

If Yes…

a. Are the types of identifying information that should be placed in the file articulated?

❑ Yes ❑ No

b. Is there a procedure for requiring the articulation of the criminal predicate for the permanent file?

❑ Yes ❑ No

c. Is there a procedure articulating the conditions wherein a temporary file may be created?
❑ Yes ❑ No

d. Does the procedure specify a time limit that the temporary file can be kept?
❑ Yes ❑ No

e. Is there an operational definition of "Non-Criminal Identifying Information" and procedures for recording and retaining this information?
❑ Yes ❑ No

f. Are there clear procedures that ***describe*** the types of information that should not be entered into the Intelligence Records System?
❑ Yes ❑ No

3. Management of Information: Source Documents

1. Does the department have a written directive explaining the different types of source documents that will be entered in the Intelligence Records System?
❑ Yes ❑ No
2. What types of source documents are entered into the Intelligence Records System?
Describe:

3. Does the police department have a written directive that the rationale for each source document entered into the Intelligence Records System must be articulated in a report or notation?
❑ Yes ❑ No

4. Management of Information: Data Entry

1. Who is responsible for entering information into the Intelligence Records System?
   Position/Classification:

2. Who supervises the information entry process?
   Position/Classification:

5. Management of Information: Accountability

1. Who is the Custodian of the Intelligence Records System that ensures all regulations, law, policy and procedures are being followed?
   Position/Classification:

2. Is there a person external to the Intelligence Unit who is designated to monitor the Intelligence Records System and related processes?
   ❑ Yes ❑ No
   If Yes, Position/Classification):

3. Does the department have written procedures for the retention of records in the Intelligence Records System?
   ❑ Yes ❑ No

6. Management of Information: Retention and Purging of Records

1. Does the retention process adhere to the guidelines of 28 CFR Part 23?
   ❑ Yes ❑ No
2. Does the retention policy and procedure include written criteria for purging information?
   ❑ Yes ❑ No

3. How often does a review and purge process occur?
   Frequency:

4. What is the purge process?
   Describe:

5. Does the purge process include a system review of information to confirm its continuing propriety, accuracy and relevancy?
   ❑ Yes ❑ No
6. Does the purge process require destruction of the source document and removal of all references to the document to be purged if the information is no longer appropriate for retention?
   ❑ Yes ❑ No
7. What is the destruction process for purged "hard copy" records?
   Describe:

8. After information has been purged from a computerized Intelligence Records System, is free space on the hard drive and/or specific purged files electronically "wiped"?
   ❑ Yes ❑ No
   a. Are back-ups wiped?
   ❑ Yes ❑ No

b. What is the accountability system for purging back-ups?
Describe:

9. Does the purge process require the elimination of partial information that is no longer appropriate if the source document is to be kept because the remaining information in the source documents merits retention?
❑ Yes ❑ No
10. What is the process for purging partial information from "hard copy" source documents?
Describe:

11. Who is responsible for ensuring compliance of the purge process?
Position/Classification:

7. Management of Information: Personal/Individually-Held Records and Files

1. Is there an intelligence unit policy and procedures concerning the retention of individual notes and records that identifies persons wherein criminality is suspected but is not in either a temporary or permanent file and is not entered into any formal records system or database?
❑ Yes ❑ No

a. How is the possession of personal records monitored?
❑ Yes ❑ No

b. How is the policy enforced?
❑ Yes ❑ No

8. Management of Information: Accessing Intelligence Records

1. Is access to the Intelligence Records limited?
❑ Yes ❑ No
2. If yes, who may access the Intelligence Records System?
Describe:

3. What security controls exist for accessing computerized records?
Describe:

4. Can the computerized records system be accessed through remote access?
❑ Yes ❑ No
a. If so, what security controls exist for remote access?
Describe:

5. How are physical records stored?
   Describe:

6. Who grants access privileges to Intelligence Records?
   Position/Classification:

7. Who has access to records?
   Position/Classification:

Law Enforcement Intelligence:
A Guide for State, Local, and Tribal Law Enforcement Agencies

David L. Carter, Ph.D.
School of Criminal Justice
Michigan State University

8. Does the police department apply the Third Agency Rule to information that is shared with other agencies?
   ❑ Yes ❑ No

9. What audit process is in place for access to computerized records?
   Describe:

10. What audit process is in place for access to physical records?
    Describe:

11. How are physical records secured?
    Describe:

12. What process is in place to handle unauthorized access to intelligence physical records?
    Describe:

13. What sanctions are in place for a police department employee who accesses and/or disseminates intelligence records without authorization?
    Describe:

9. Physical Location of the Intelligence Unit and Records

1. Sufficiency: Is the Intelligence Unit in a physical location that has sufficient space to perform all of its responsibilities?
   ❑ Yes ❑ No
2. Security: Is the Intelligence Unit in a physical location wherein the entire workspace may be completely secured?
   ❑ Yes ❑ No
   a. Is there adequate secured storage cabinets (or a vault) for (1) documents classified by the Intelligence Unit and (2) sensitive records storage within the intelligence unit's physical location?
      ❑ Yes ❑ No

b. Is there adequate security and segregated storage for federally classified documents within the intelligence unit?
❑ Yes ❑ No

1) Is that storage accessible only by persons with a federal top secret security clearance?
❑ Yes ❑ No

3. Convenience: Is the Intelligence Unit in a physical location that is convenient to the people, equipment, and resources necessary to maximize efficiency and effectiveness of operations?
❑ Yes ❑ No

10. Tangential Policy Issues: Criminal Informants and Undercover Operations

1. Is there a formally articulated policy and procedures for managing criminal informants?
❑ Yes ❑ No
   a. Is a background investigation conducted and a comprehensive descriptive file completed on each confidential informant?
   ❑ Yes ❑ No
   b. Are informant files secured separately from intelligence files?
   ❑ Yes ❑ No
2. Is there a formally articulated policy and procedures concerning undercover operations that apply to members of the Intelligence Unit?
❑ Yes ❑ No
3. Does the police department have a policy on alcohol consumption for officers working undercover?
❑ Yes ❑ No
   a. Does the police department have a policy requiring designated drivers for undercover officers who have consumed alcohol?
   ❑ Yes ❑ No
4. Does the police department have a "narcotics simulation" policy and training for undercover officers?
❑ Yes ❑ No
5. Does the police department have a policy for the issuance of fictitious identification for undercover officers and the proper use of such fictitious identification?
❑ Yes ❑ No

6. Do undercover officers receive training specifically related to proper conduct and information collection while working in an undercover capacity?
   ❑ Yes ❑ No
7. With respect to undercover operating funds:
   a. Is there a 1-tier or 2-tier process to approve use of the funds?
   ❑ 1 Tier ❑ 2 Tier
   b. Is a written report required to document expenditure of the funds?
   ❑ Yes ❑ No
   c. What is the maximum time that may pass between the expenditure of funds and personnel accountability for the funds?
   Days ❑ No Set Time
   d. Is there a regular external audit of undercover funds?
   ❑ Yes [How Often?] ❑ No

Section C: Personnel

1. Is a position classification plan in place that provides a clear job description for each position in the unit?
   ❑ Yes ❑ No
2. Is a position classification plan in place that articulates Knowledge, Skills and Abilities (KSAs) for each position?
   ❑ Yes ❑ No
3. Is there sufficient hierarchical staff (managers/supervisors) assigned to the unit to effectively perform supervisory responsibilities?
   ❑ Yes ❑ No
4. Is there sufficient functional staff (analysts and/or investigators) to effectively fulfill defined unit responsibilities?
   ❑ Yes ❑ No
5. Is there sufficient support staff (secretaries, clerks) to effectively support the unit's activities?
   ❑ Yes ❑ No
6. Does the screening process for nonsworn employees of the intelligence unit require:
   a. Fingerprint check?
   ❑ Yes ❑ No
   b. Background investigation
   ❑ Yes ❑ No

7. If the Intelligence Unit has non-PD employees assigned to it – e.g., National Guard analysts, personnel from the state or local law enforcement agencies – would there be a screening process for those persons?

❑ Yes ❑ No

If Yes, Describe:

1. Training

1. What types of training do preservice and newly assigned personnel receive?

❑ None ❑ Some–Describe:

a. Are newly assigned sworn employees to the Intelligence Unit required to attend 28 CFR Part 23 training?

❑ Yes ❑ No

b. Are newly hired or assigned non-sworn employees required to attend 28 CFR Part 23 training?

❑ Yes ❑ No

2. What types of training do in-service personnel receive?

❑ None ❑ Some

Describe:

3. Have members of the Intelligence Unit attended any of the following federal government intelligence training programs which are open to state and local law enforcement officers?
   a. DEA Federal Law Enforcement Analyst Training (FLEAT)?
      ❑ Yes ❑ No
   b. FBI College of Analytic Studies?
      ❑ Yes ❑ No
   c. Federal Law Enforcement Training Center (FLETC) Criminal Intelligence Analysis Training Course?
      ❑ Yes ❑ No
   d. National Drug Intelligence Center Basic Intelligence Analysis Course?
      ❑ Yes ❑ No
   e. National White Collar Crime Center Foundations of Intelligence Analysis?
      ❑ Yes ❑ No
   f. Regional Counterdrug Training Academy Intelligence Operations Course?
      ❑ Yes ❑ No

2. Supervision

1. Does supervision effectively monitor adherence to written procedures?
   ❑ Yes ❑ No
2. Does supervision effectively monitor adherence to guidelines adopted by the department?
   ❑ Yes ❑ No
3. Are performance evaluations tied directly to the job descriptions?
   ❑ Yes ❑ No
4. Does supervision effectively monitor the performance of required duties (Including the quality of performance)?
   ❑ Yes ❑ No
5. Is supervision effectively monitoring personnel to ensure civil rights allegations cannot be made with respect to negligent:
   a. Failure to train?
      ❑ Yes ❑ No

b. Hiring?
   ❑ Yes ❑ No
c. Failure to supervise?
   ❑ Yes ❑ No
d. Assignment?
   ❑ Yes ❑ No
e. Failure to direct?
   ❑ Yes ❑ No
f. Failure to discipline?
   ❑ Yes ❑ No
g. Entrustment?
   ❑ Yes ❑ No

6. Is there effective supervision of the Intelligence Unit throughout the chain of command external to the Intelligence Unit?
   ❑ Yes ❑ No

Section D: Fiscal Management

1. Is the budget sufficient to fulfill the stated mission?
   ❑ Yes ❑ No
2. Does the Intelligence Commander have input into the budget planning process?
   ❑ Yes ❑ No
3. Is there over-reliance on "soft money" to operate the unit?
   ❑ Yes ❑ No
4. Are equipment and personnel line items assigned directly to the Intelligence Unit?[235]
   ❑ Yes ❑ No
5. Is there an established process for reliably monitoring credit cards assigned to personnel?
   ❑ Yes ❑ No ❑ NA

Section E: Unit Evaluation

1. As a whole, is the unit effective with respect to:
   a. Providing information to prevent crime?
      ❑ Yes ❑ No

b. Providing information to apprehend criminals?
❑ Yes ❑ No

c. Effectively analyzing information to identify criminal enterprises, crime trends, criminal anomalies, etc.?
❑ Yes ❑ No

2. Are data collected on the following factors and reported in an annual report as indicators of the intelligence unit's productivity as an organizational entity?

a. Number and type of analytic products delivered for investigative purposes?
❑ Yes ❑ No ❑ NA

b. Number and type of analytic products that led to arrest?
❑ Yes ❑ No ❑ NA

c. Assets seized from illegal activities wherein intelligence contributed to the arrest and/or seizure?
❑ Yes ❑ No ❑ NA

d. Number and types of strategic intelligence products delivered to the command staff?
❑ Yes ❑ No ❑ NA

e. Number of intelligence-sharing meetings attended by unit staff?
❑ Yes ❑ No ❑ NA

f. Number of briefings provided by the intelligence staff?
❑ Yes ❑ No ❑ NA

g. Total number of queries into the intelligence data base?
❑ Yes ❑ No ❑ NA

h. Number of permanent files opened?
❑ Yes ❑ No ❑ NA

i. Number of temporary files investigated?
❑ Yes ❑ No ❑ NA

j. Number of requests for information to the unit from outside agencies?
❑ Yes ❑ No ❑ NA

3. Are products produced by the Intelligence Unit:

a. In a consistent format?
❑ Yes ❑ No

b. Easily consumed and used (i.e., understandable and actionable)?
❑ Yes ❑ No

c. Contain timely information and disseminated in a timely manner?
❑ Yes ❑ No

d. Have substantive contact to aid in preventing or controlling crime?
❑ Yes ❑ No

4. Given the confidential nature of the information contained in the Intelligence Unit, is there a policy and procedures if a city, county, state, or federal fiscal or program auditor seeks to audit the Intelligence Unit?
❑ Yes ❑ No
If Yes, Describe:

Section F. Collection

1. Is there an articulated collection plan for the Intelligence Unit?
❑ Yes ❑ No
If Yes, Describe:

a. How often and when is the plan updated?
Describe:

2. Have the following activities been performed by the Intelligence Unit:
a. An inventory of threats in the region posed by criminal enterprises, terrorists, and criminal extremists?
❑ Yes ❑ No
b. An assessment of the threats with respect to their probability of posing a criminal or terrorist threat to the region?
❑ Yes ❑ No
c. A target or criminal commodity analysis of the region?
❑ Yes ❑ No
d. A target or criminal commodity vulnerability assessment in the region?
❑ Yes ❑ No

3. For each identified threat, have intelligence requirements been articulated?
❑ Yes ❑ No

a. If Yes, Describe the methods of collection that will be used to fulfill those intelligence requirements.

Section G: Technology and Networking

1. Are any members of the Intelligence Unit subscribed members to the FBI's secure Email system Law Enforcement Online (LEO)?
   ❑Yes–All ❑ Yes–Some ❑ No
2. Are any members of the Intelligence Unit subscribed members to the secure Regional Information Sharing System (RISS) email system riss.net?
   ❑ Yes–All ❑ Yes–Some ❑ No
   a. If yes, are the RISS databases (e.g., RISS.gang, ATIX, etc.) regularly used?
      ❑ Yes ❑ No
3. Is the police department a member of the Regional Information Sharing System?
   ❑ Yes ❑ No
4. Is a systematic procedure in place to ensure that advisories and notifications transmitted via the National Law Enforcement Teletype System (NLETS) are forwarded to the Intelligence Unit?
   ❑ Yes ❑ No
5. Are you connected to any state-operated intelligence or information networks?
   ❑ Yes ❑ No
   If Yes, Describe:

6. Are you connected to any regional intelligence or information networks (including HIDTA)?
   ❑ Yes ❑ No
   If Yes, Describe:

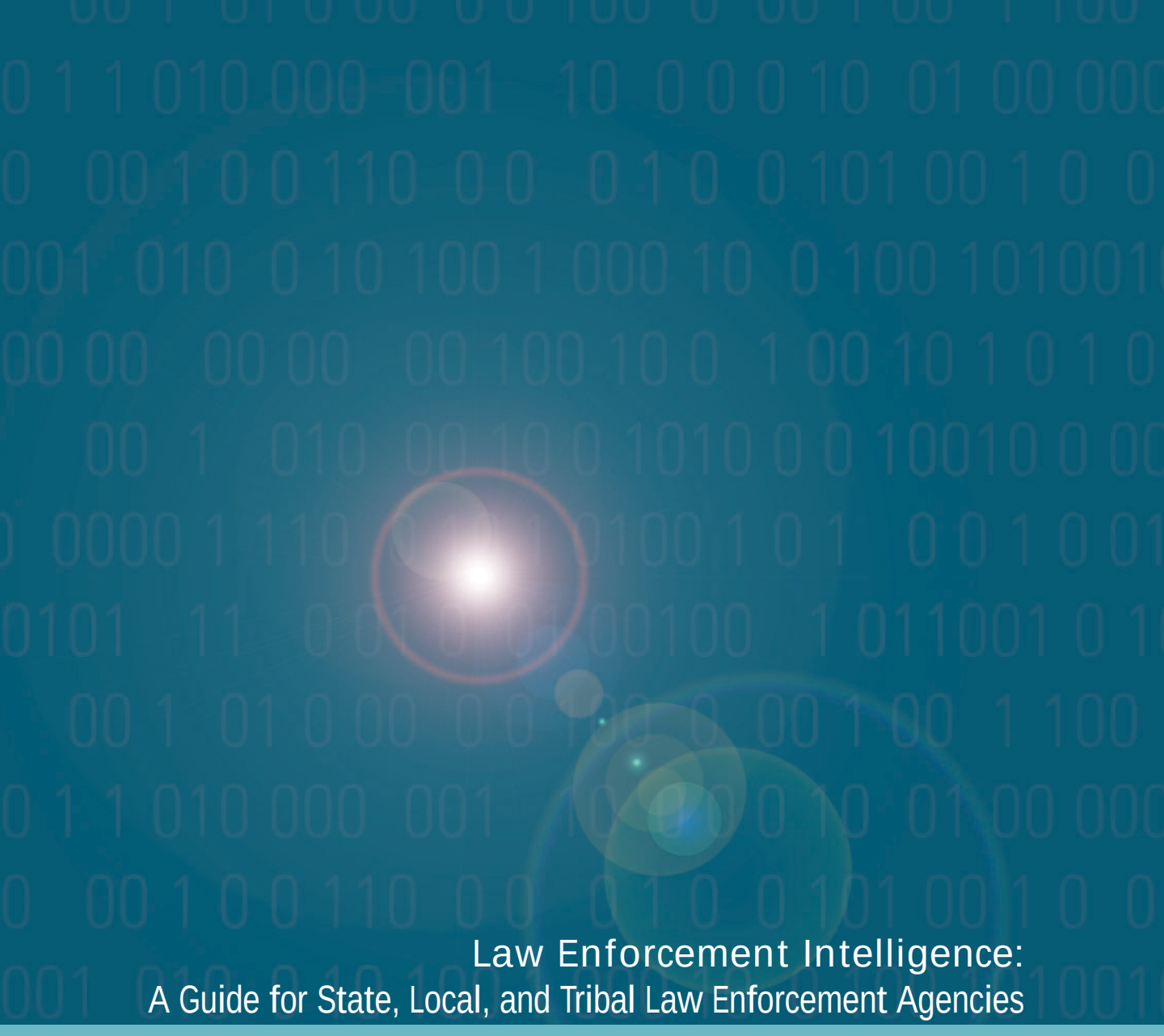
7. Does the intelligence have access and use the National Virtual Pointer System (NVPS)?
   ❑ Yes ❑ No
8. Is there a formal approval process for entering into a memorandum of understanding (MOU) for information and intelligence sharing with other law enforcement agencies or law enforcement intelligence entities?
   ❑ Yes ❑ No
   If Yes, Describe the process:

Who must approve the MOU?

Section H: Legal Issues

1. Is there a designated person in the police department who reviews Freedom of Information Act requests directed to the intelligence unit?
   ❑ Yes ❑ No
2. Is there a designated person in the police department who responds to Privacy Act inquiries directed to the intelligence unit?
   ❑ Yes ❑ No

3. Is there a designated person the police department contacts in response to a subpoena for a file in the Intelligence Records System?
   ❑ Yes ❑ No
4. Does the Intelligence Unit Commander have a legal resource for advice to help protect intelligence records from objectionable access?
   ❑ Yes ❑ No
5. Does the Intelligence Unit Commander have a legal resource for advice on matters related to criminal procedure and civil rights?
   ❑ Yes ❑ No
6. Does the Intelligence Unit Commander have a legal resource for advice on matters related to questions of civil liability as it relates to all aspects of the intelligence function?
   ❑ Yes ❑ No
7. Has legal counsel reviewed and approved all policies and procedures of the intelligence unit?
   ❑ Yes ❑ No



Law Enforcement Intelligence:
A Guide for State, Local, and Tribal Law Enforcement Agencies

To obtain details on COPS programs, call the COPS Office Response Center at 800.421.6770

Visit COPS Online at www.cops.usdoj.gov

e09042536 October 28, 2004
ISBN: 1-932582-44-4