OFFICE OF THE DIRECTOR OF POLICE
THE UNIVERSITY OF TEXAS SYSTEM
POLICY AND PROCEDURE MANUAL

Subject			Policy Number
Criminal Intelligence			**810**
Effective Date	Revision Date	Reevaluation Date	Number of Pages
November 7, 2012		Annually	10
Reference Standards		Resends or Amends Policy Number	
TPCA: 8.10 CALEA: 42.1.6,43.1.1,46.3.1 and 46.3.2 IACLEA: 16.2.1			

I. PURPOSE

It is the purpose of this policy to provide the University of Texas System Police and officers assigned to the intelligence function, in particular, with guidelines and principles for the collection, analysis, and distribution of intelligence information.

II. POLICY

Information gathering is a fundamental and essential element in the all-encompassing duties of any law enforcement agency. When acquired, the information is used to prevent crime, pursue and apprehend offenders, and obtain evidence necessary for a conviction. It is our policy to gather information directed toward specific individuals or organizations where there is reasonable suspicion (as defined in 28 *Code of Federal Regulations*, CFR, Part 23, Section 23.3 c) that said individuals or organizations may be planning or engaging in criminal activity, to gather it with due respect for the rights of those involved, and to disseminate it only to authorized individuals as defined. We 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. While criminal intelligence responsibilities may be assigned to specific personnel within a Criminal Investigations Unit, all members of this Department are responsible for reporting information that may help identify criminal offenders, conspirators and perpetrators. It is the policy of the University of Texas System Police to maintain a Criminal Intelligence function that:

A. Abides by the standards set forth in 28 CFR Part 23, which is the national standard for law enforcement intelligence operations in respect to citizen privacy during the analytical process, both in retention and dissemination, as well as complies with Criminal Intelligence Systems Operating Policies and the *Texas Code of Criminal Procedure*, Chapter 61, Compilation Pertaining to Criminal Combinations and Criminal Street Gangs,.

B. Collects information limited to specific criminal predicate and relates to activities that prevent threats to the University community and surrounding area.

C. Analyzes the value and quality of information received concerning criminal activity.

D. Disseminates criminal intelligence to proper units for action and/or information.

E. Abides by the Nationwide Suspicious Activity Reporting (SAR) Initiative in regard to sharing intelligence information with those Federal law enforcement agencies tasked with investigating possible terrorist activities.

III. DEFINITIONS

Criminal Information – Raw data that supports criminal intelligence investigative needs that may be gathered from tips, field contacts, open-source material, banking records, driver's license information, criminal history records, witness statements, officer observation, and suspicious activity reports.

Criminal Intelligence – Criminal Intelligence Information means data, which has been evaluated to determine that it:

1. is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and

2. meets criminal intelligence system submission criteria;

3. is compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity.

Criminal Intelligence Report - the completed product of a process that converts individual items of information either into evidence or, more often, into insights, conclusions, or assessments that can form the basis for the development of law enforcement strategies.

Criminal Intelligence Systems – the facility, arrangements, equipment and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

Criminal Predicate – established when information exists that establishes sufficient facts to give a trained law enforcement officer a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

Intelligence Function - 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 inter-jurisdictional intelligence system on behalf of a group of participating agencies.

Participating Agency - 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 inter-jurisdictional intelligence system. A participating agency may be a member or a nonmember of an inter-jurisdictional intelligence system;

Strategic Intelligence – information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies, for both short- and long-term investigative goals.

Tactical Intelligence – information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations, and provide for officer safety.

Threshold for Criminal Intelligence – the threshold for collecting information and producing criminal intelligence shall be the "reasonable suspicion" standard in 28 CFR, Part 23, Section 23.3c.

Validation of Information - the procedures governing the periodic review of criminal intelligence information to ensure its continuing compliance with system submission criteria established by regulation or program policy.

IV. PROCEDURES

A. Criminal Intelligence

1. The Criminal Intelligence function and activity will be determined by the institution's chief of police.

2. Primary responsibility for the direction of intelligence operations; coordination of personnel; and collection, evaluation, collation, analysis and dissemination of intelligence information should be stored and retained under the Criminal Investigations Unit Commander and/or Supervisor under advisement of the assigned Intelligence Officer.

3. The intelligence function is often confronted with the need to balance information-gathering requirements for law enforcement with the rights of individuals. To this end, members of this agency shall adhere to the following:

   a) Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable suspicion (as defined in 28 CFR, Part 23, Section 23.3c) in that information retained must be information relevant to the identification of, and the criminal activity engaged in by an individual, group of individuals or organizations that may be planning or engaging in criminal activity.

   b) Information that is collected and maintained in the intelligence files must be limited to actual or suspected criminal conduct that presents a threat to the community which may include, but not limited to:

      (1) Crimes or suspected criminal activity committed in the area.

      (2) Narcotic activity at the university and in the area.

      (3) Movements and locations of known and suspected criminals.

c) The intelligence function shall make every effort to ensure that information added to the criminal intelligence files or database is relevant to a current or on-going investigation and the product of dependable and trustworthy sources of information. A record shall be kept of the source of all information received and maintained by the intelligence function.

d) Information gathered and maintained by the intelligence function for intelligence purposes may be disseminated only to appropriate persons for legitimate law enforcement purposes in accordance with law and procedures established by this Department. A record shall be kept regarding the dissemination of all such information to persons within this or another law enforcement agency while maintain the original information.

4. Personnel, equipment, and other resources utilized in the Intelligence function will be based on the following criteria:

e) Seriousness of the criminal activity.

f) Quality of the information.

g) Threat level to the community.

h) Availability of resources.

5. Techniques for the validation of information may include surveillance, undercover operations, and decoy operations as detailed in institutional department Criminal Investigation Division procedures.

B. Authorized Personnel/Access

1. Information beneficial to an institutional department's intelligence effort shall be routed to the Criminal Investigations Supervisor by the person obtaining the information.

2. Each department 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.

3. Access to the criminal intelligence files shall be restricted to the:

a) Intelligence Officer

b) Criminal Investigations Commander and/ or Supervisor

c) ODOP Intelligence Coordinator Inspector

d) Chief of Police or a specific designee

4. Information entered into Intelligence files shall include the date of entry, source of information, and the name of the person making the entry. The Intelligence products will reflect the addition, deletion, or revision of information. The Intelligence products must contain information that is timely, accurate, thorough, pertinent, and actionable.

   a) A record indicating who has been given information, the reason for the release of the information and the date of each dissemination outside the function shall be kept. The information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials.

   b) Each departmental intelligence function must establish written definitions for the need to know and right to know standards for dissemination to other agencies. The function 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.

   c) Each intelligence function shall ensure that the following security requirements are implemented:

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

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

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

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

      (5) The function 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 function may authorize and utilize remote (off-premises) system databases, to the extent that they comply with these security requirements.

      (7) The unauthorized release, dissemination or access to criminal intelligence files may result in disciplinary action and potential criminal charges.

C. File Content

1. A function 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.

2. A 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 inter-jurisdictional intelligence system, the function 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 function. A function shall not collect or maintain criminal intelligence information about:

   a) 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.

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

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

3. A function 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 inter-jurisdictional intelligence system, the function 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 function.

4. 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.

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

D. Compiling Intelligence

1. Intelligence files/investigations or functions may be opened by the Intelligence Officer with sufficient information and justification. This includes but is not limited to the following types of information:

   a) Subject, victim(s) and complainant as appropriate; summary of suspected criminal activity;

   b) Anticipated investigative steps to include proposed use of informants, photographic, or electronic surveillance;

   c) Resource requirements, including personnel and equipment;

   d) Anticipated results; and

e) Problems, restraints, or conflicts of interest.

2. Officers shall not retain official intelligence documentation for personal reference or other purposes but shall submit reports and information directly to the Intelligence Officer or Criminal Investigations Supervisor.

3. Information gathering using confidential informants as well as electronic, photographic, and related surveillance devices shall be performed in a legally accepted manner and in accordance with federal and state law and applicable procedures.

E. Criminal Intelligence Analysis, Evaluation and Reports

1. The intelligence function shall establish and maintain a process to ensure that information gathered is subjected to review and analysis to derive its meaning and value. Where possible, information shall be evaluated with respect to reliability of source and validity of content. While evaluation may not be precise, this assessment must be made to the degree possible in order to guide others in using the information. A record shall be kept of the source of all information where known.

a) Source Reliability:

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

(2) **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.

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

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

b) Content Validity:

(1) **Confirmed** – The information had 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.

2. Analytical material (i.e., intelligence) shall be compiled and provided to only authorized law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security and dissemination which are consistent with these principles. The reports should identify meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or individuals.

3. Reports and other investigative material and information received by an institutional police department shall remain the property of the originating agency, but may be retained by the department. Such reports and other investigative material and

information shall be maintained in confidence, and no access shall be given to another agency except with the consent of the originating agency.

4. Information having relevance to active cases or that requires immediate attention shall be forwarded to responsible investigative personnel as possible.

5. Analytical material shall be compiled and provided to authorized recipients as soon as possible where meaningful trends, patterns, methods, characteristics, or intentions of criminal enterprises or figures emerge.

F. Dissemination

1. A function 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.

2. This 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.

3. In order to maximize the value of Intelligence information gathered by this and other agencies, the Intelligence Officer shall develop and maintain a liaison with federal, State, and local Criminal Justice agencies for the purpose of the exchange of intelligence information. This exchange may be through informal channels or through formal meetings of persons involved in the Intelligence function.

4. The Intelligence Officer shall ensure that applicable intelligence information is distributed to the various departmental Units as needed. The Criminal Investigations Supervisor shall, at his/her discretion but not less than twice each year, solicit feedback from the various departmental Units as to the utility and timeliness of Intelligence information being provided.

G. File Status

Intelligence file status will be classified as either "open" or "closed," in accordance with the following:

1. Open – Intelligence files that are actively being investigated. In order to remain open, officers working such cases must file intelligence status reports covering case developments every 180 days.

2. Closed – Intelligence files in which investigations have been completed, where all logical leads have been exhausted, or where no legitimate law enforcement interest is served. All closed files must include a final case summary report prepared by or with the authorization of the lead investigator.

H. Classification

Intelligence files will be classified in order to protect sources, investigations, lives of potential suspects as well as law enforcement officers, and individual's rights to privacy, as well as to provide a structure that will enable this agency to control access to intelligence. These classifications shall be reevaluated whenever new information is added to an existing intelligence file.

1. **Restricted** - intelligence files include those that contain information that could adversely affect an on-going investigation, create safety hazards for officers, informants, or others and/or compromise their identities. Restricted intelligence may only be released by approval of the Intelligence Officer, Criminal Investigations Unit Commander and/or Supervisor, or the Chief of Police to authorized law enforcement agencies with a need and a right to know.

   Note: Information that implicates, suggests implication or complicity of any public official in criminal activity or corruption shall be immediately reported to the departments Chief or/and the Office of Director of Police.

2. **Confidential** - intelligence is less sensitive than restricted intelligence. It may be released to agency personnel when a need and a right to know have been established by the Intelligence Officer or his designee or to another law enforcement agency.

3. **Unclassified** - intelligence contains information from the news media, public records, and other sources of a topical nature to which, in its original form, the general public had direct access.

I. Auditing and Purging Files

1. The Intelligence Officer is responsible for ensuring that files are maintained in accordance with the goals and objectives of the intelligence function and include information that is both timely and relevant. To that end, all intelligence files shall be audited and purged at the maximum retention period of five years as established in 28 CFR, Part 23. Each institutional department shall conduct an annual review and audit for all intelligence documents to ensure compliance.

2. When a file has no further information value and/or meets the criteria of any applicable law, it shall be destroyed. Documentation of files destroyed shall be maintained by the intelligence officer or function.

J. Database User Training

Persons who enter information into or retrieves information from a UTSP intelligence database shall complete continuing education training, at least once for each continuous two-year period if the person has primary responsibility for performing this function.

K. Annual Review

The Chief of Police will cause an annual review of criminal intelligence procedures and processes to be conducted. Copies of that review will be shared with the Director of Police and the ODOP Intelligence Coordinator Inspector.

Michael J. Heidingsfield
Director of Police