	STANDARD OPERATING PROCEDURE State Form 39870(R/ S- 06)	Reference Number INV-018
	Subject Criminal Intelligence	
	Special Instructions Replaces INV-004 dated January 15, 2015	Effective Date **August 15, 2024**

I. PURPOSE

Establish guidelines for the Department's collection, handling, communication, and analysis of criminal intelligence information as defined in and authorized by I.C. 5-2-4-1 through I.C. 5-2-4- 7 and 28 CFR (Code of Federal Regulations), Part 23.

II. POLICY

Officers shall report any suspicious or suspected criminal activity to the ISP Criminal Intelligence Section.

All ISP personnel shall adhere to criminal intelligence information processes and elements identified in I.C. 5-2-4-1 through I.C. 5-2-4-7 ISP Criminal Intelligence Operations Manual, and operate within guidelines outlined in 28 CFR, Part 23.

The Special Investigations Division (SID) Commander or designee is specifically delegated the authority to build criminal intelligence files within the Department and to structure and organize procedures that provide the security of those files required by law.

Intelligence files shall be used to support federal, state, local and tribal agencies, and to meet legitimate informational needs of criminal justice agencies with a valid Need to Know and Right to Know.

III. DEFINITIONS

A. NEED TO KNOW – When a person requesting information is actively involved in a criminal investigation on the information being sought. The information is to be used for targeting a criminal investigation or developing an assessment of general crime problems, or the information is related to officer safety.

B. RIGHT TO KNOW – Department employees or employees of any criminal justice agency or department, at any level of government; that performs, as its principal function, the apprehension, prosecution, adjudication, incarceration, or rehabilitation of criminal offenders. Criminal intelligence information may be disseminated when that person is acting in an official capacity and is a designated representative; or is a representative from a law enforcement agency belonging to a network or association with which the Department is also a member, e.g., EPIC, INTERPOL, LEIU, NW3C, MAGLOCLEN, etc.

IV. PROCEDURE

A. ISP Criminal Intelligence Analysts

1. ISP Criminal Intelligence Analysts shall be the initial recipient of all criminal intelligence.

2. ISP Criminal Intelligence Analysts is responsible for collecting, evaluating, collating, analyzing, maintaining, and disseminating criminal intelligence information on any individual, group, or organization that is engaged in, or is suspected of being engaged in, conduct defined as a criminal act by federal or state statutes.

3. All ISP Criminal Intelligence Analysts shall adhere to criminal intelligence information processes and elements identified in I.C. 5-2-4-1 through I.C. 5-2-4-7, ISP Criminal Intelligence Operations Manual, and operate within guidelines outlined in 28 CFR, Part 23.

B. The Special Investigations Division (SID) Commander or designee, with the approval of the Superintendent, shall prescribe the procedures to be followed for the collection, dissemination, and retention of criminal intelligence information and for maintaining liaison with federal, state, and local criminal justice agencies for the exchange of criminal intelligence.

C. Criminal intelligence files shall only be held at the ISP Criminal Intelligence Section and the IIFC, except for the time required for expeditious processing.

D. Criminal intelligence files shall only be held with the ISP Criminal Intelligence Section.

E. Written Intelligence Bulletins and Reports

1. ISP Criminal Intelligence Section personnel are authorized, with approval from the SID Commander or designee, to prepare written intelligence summaries, assessments, and other necessary work products.

2. Periodically, the SID Commander or a designee will disseminate written intelligence bulletins and reports to Department enforcement personnel and criminal justice agency officials, at all levels, acting in an official capacity and having a valid Right to Know and Need to Know.

3. Written intelligence bulletins and reports may contain raw, unevaluated intelligence information concerning time-sensitive criminal activity, or officer safety considerations.

4. The ISP Criminal Intelligence Analysts shall collect material for the bulletins and reports from open sources, reported suspicious criminal activities, investigative and intelligence support requests made to ISP Criminal Intelligence Analysts, requests from Department commanders, information sent to ISP Criminal Intelligence Analysts by the IIFC and other criminal justice agency liaison functions, and other appropriate sources.

5. The ISP Criminal Intelligence Analysts shall review material for bulletins and reports considering source type, reliability and credibility of informational content. The ISP Criminal Intelligence Analysts shall obtain expressed permission to disseminate the information from the initial source, to

include Department enforcement personnel or criminal justice agency officials; and

6. Written bulletins and reports shall be sent through the most secure methods available, contain restrictive statements, and at a minimum shall relate to one of three issues:

a. Ongoing criminal investigations,
b. Identification of crime trends or problems, or
c. Provision of officer safety considerations.

F. Security

1. All written confidential material shall be stored in secure file cabinets. When not under the physical control of ISP Criminal Intelligence Section personnel, mechanical or electrical protective devices shall be utilized.

2. Any automated intelligence system or electronic communication system, in which confidential material is communicated or stored shall be protected as required by 28 C.F.R. part 23 and any applicable federal or state statutes.

3. Personnel security checks and periodic review of security clearances of those personnel with direct access to raw criminal intelligence shall be reviewed at the direction of the SID Commander or designee.

4. Periodic inspections and audits may be conducted to ensure compliance with this section. This shall not include access to intelligence data.

5. Criminal intelligence information containing real, actual data shall not be sent to anyone through Department email via the statewide network unless the message includes a confidentiality notice as outlined in CIS-006.

G. Reproduction/dissemination of intelligence information

1. Reproduction of any criminal intelligence information shall be accomplished only with prior approval of the SID Commander or designee.

2. All requests for criminal intelligence information shall be directed to the ISP Criminal Intelligence Analysts. Dissemination of all written reports shall be completed by the ISP Criminal Intelligence Analysts. Requests must be specific as to what is needed and about whom. This applies to requests initiated both by Departmental personnel and requests initiated by other criminal justice agencies.

3. The requestor shall provide the ISP Criminal Intelligence Analysts with the reason for the request (e.g. murder investigation witness, a narcotic investigation target, or the information is needed to assess possible burglars prior to a burglary investigation, etc).
4. Criminal intelligence information shall be disseminated only to authorized persons on a Need to Know and Right to Know basis, and then only if the information is for use in the performance of a related law enforcement activity within the scope of their duties and there is assurance that the

confidentiality of the information shall be maintained.

5. This section shall not limit dissemination of a criminal intelligence information assessment to an individual when necessary to avoid imminent danger to life or property.

6. All disseminated reports containing criminal intelligence information shall be marked confidential or contain a restrictive statement.

7. Employees of the Department receiving criminal intelligence information shall be responsible for properly safeguarding the information. Misuse or prohibited dissemination or filing may result in disciplinary action and criminal prosecution.

H. The SID Commander or designee shall provide support to the Department's Training Section and enforcement personnel in the areas of criminal intelligence operations and counter-terrorism.

I. This procedure is to be used in conjunction with all relevant Department regulations, rules, policies, and procedures.