INDIANA STATE POLICE	***STANDARD OPERATING PROCEDURE*** State Form 39870(R/ S- 06)	Reference Number INV-018
	Subject Criminal Intelligence, Criminal Activity Report, CIU, Crime Analysis	
	Special Instructions Replaces INV-004 dated July June 27, 2011	Effective Date **January 15, 2015**

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 Criminal Intelligence Unit (CIU) using the electronic Criminal Activity Report (CAR). CARs shall be reviewed and evaluated by the CIU and information of value shall be developed and investigated or forwarded to the appropriate section or agency.

All CIU and Indiana Intelligence Fusion Center (IIFC) 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, CIU Operations Manual, and operate within guidelines outlined in 28 CFR, Part 23.

The CIU Commander and the IIFC Executive Director are 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 Indiana State Police operations and to meet legitimate informational needs of criminal justice agencies with a valid Need to Know and Right to Know.

III. DEFINITIONS

A. **Criminal Activity Report** (CAR) – An electronic report used to record suspicious or suspected criminal activity and report that information to the CIU for further review.

B. **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.

C. **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. CRIMINAL ACTIVITY REPORT (CAR)

A. Personnel shall not retain copies of a CAR but may retain, in a secure manner, a specific item of criminal intelligence information contained within the CAR.

B. There shall be no reference to criminal intelligence files or Criminal Activity Reports in any Initial/Supplemental Criminal Incident Report, Non-Criminal Incident Report, or affidavit in support of probable cause.

C. CAR submissions:

1. CARs may be submitted by any member of the Department;

2. Only the approved electronic Criminal Activity Report, located on the Department's MyShare home page shall be used; and

3. The CAR shall only be transmitted when directly (direct wire connection) connected to the network or when using an issued air-card.

D. Completing the Criminal Activity Report:

1. Complete the CAR as outlined in the CAR Users Guide;

2. If possible, fully identify all names submitted to include the subject's full name, race, sex, date of birth, social security number, driver's license number, and address ;

3. When this is not possible, at least two (2) identifiers should accompany the name and may include any combination of race/sex, address, telephone number, date of birth/age, social security number, FBI number, SID number, height, weight, aliases, etc.; and

4. The information submitted must define a suspected or known criminal activity, defined by Indiana State Statute or Federal law. NOTE: An infraction is not a crime and should not be the basis for a CAR submission.

E. CIU responsibilities.

1. Each CAR submitted shall be reviewed by the CIU to ensure the intelligence activity and report content meet established criteria, to include:

a. That information exists connecting the individual, group, business, or organization named with known or suspected criminal activity and the information is relevant to that activity, and

b. The CAR contains no information referring to the political, religious, or social views, association or activities of any individual, group, business, or organization unless that information directly relates to an investigation of past or threatened criminal acts and there is reasonable grounds to suspect that any individual, group, business, or organization is or may be involved in criminal activity.

2. Only CARs receiving final CIU approval shall be maintained by CIU. If the report does not meet established standards, the CIU Commander or CIU Assistant Commander shall determine the disposition of the report.

3. CARs shall not be copied, except as required by a CIU analyst, who receives prior approval of the CIU Commander.

4. Disposition of relative or sensitive information:

a. Received by any officer that is relevant to the operational and tactical plans of any specific section of the Department should be shared directly with a supervisor in that section;

b. That is immediate in nature shall be forwarded verbally to the appropriate supervisor or commander, as soon as practical, upon receipt;

c. Identified as being related to international or domestic terrorism activities shall be forwarded to the CIU Commander or Assistant Commander as soon as practical. The CIU Commander or Assistant Commander shall direct the information to the FBI JTTF (Joint Terrorism Task Force) and/or the IIFC as necessary; and

d. The CIU Commander or Assistant Commander shall further evaluate information related to international or domestic terrorism activities, and brief the Primary and Superintendent's Staff, as soon as practical.

IV. **CRIMINAL INTELLIGENCE UNIT (CIU)**

A. CIU shall be the initial recipient of all CARs. The CIU shall also be the primary operational-point of contact with the IIFC.

B. CIU is responsible for collecting, evaluating, collating, analyzing, maintaining, and disseminating criminal intelligence information and crime analysis data 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.

C. All CIU and IIFC 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, CIU Operations Manual, and operate within guidelines outlined in 28 CFR, Part 23.

D. The Special Investigations Command (SIC)Commander, 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.

E. Criminal intelligence files shall only be held at the CIU and the IIFC, except for the time required for expeditious processing.

F. Criminal intelligence information shall not be placed in a criminal history file nor shall a criminal history file suggest that a criminal intelligence file exists.

G. CIU personnel are authorized, with approval from the CIU commander, to prepare written intelligence summaries, assessments, and other necessary work products.

I. **Written Intelligence Bulletins and Reports**.

Periodically, the CIU 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.

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

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

3. The CIU shall review material for bulletins and reports considering source type, reliability and credibility of informational content. The CIU shall obtain expressed permission to disseminate the information from the initial source, to include Department enforcement personnel or criminal justice agency officials; and

4. 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.

J. Security.

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

2. Any automated intelligence system, electronic communication system in which confidential material is communicated, or digital media containing confidential material shall be protected as follows:

a. Data storage components shall be physically and logically housed at the Indiana Office of Technology (IOT).

b. Data processing resources, utilized for the automated intelligence information system, shall be under the management control of the Assistant Chief of Staff (AC/S) Communications and Information Systems (CIS); and

c. The AC/S CIS shall be responsible for establishing procedures for system security, system backup, and system auditing.

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 SIC Commander.

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 SOP CIS-006.

K. Reproduction/dissemination of intelligence information.

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

2. All requests for criminal intelligence information shall be directed to the CIU. Dissemination of all written reports shall be completed by the CIU. 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 CIU 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. The CIU shall maintain a record for all reproduction and dissemination of original CARs.

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

L. 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.

M. The CIU Commander shall routinely contact the AC/S CIS to coordinate the activities, security measures, and data processing resources necessary to manage and support the CIU operations.

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

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