INDIANA STATE POLICE	***STANDARD OPERATING PROCEDURE*** State Form 39870(R/S-06)	Reference Number INV-019
	Subject Intercept Warrant Application	
	Special Instructions Replaces INV-005 dated October 7, 2011	Effective Date **March 1, 2015**

I. **PURPOSE**

Establish procedures for requesting an Intercept Warrant Application pursuant to Indiana Code 35-33.5.

II. **POLICY**

Department employees shall follow prescribed procedures when requesting an Intercept Warrant Application.

III. **PROCEDURE**

A. INTERCEPT WARRANT APPLICATION – A court approved acquisition of an electronic communication without the consent of the sender or the receiver.

B. Requests for an Intercept Warrant Application.

1. Shall be submitted by a police employee, through channels, to the Commander of the Special Investigations Command (SIC).

2. The SIC Commander and the Chief (Legal) Counsel shall analyze the case and tentatively determine that all criteria of IC 35-33.5-2-2 (a) (2)-(6) (c) have been fulfilled. This criterion shall include:

a. Facts establishing probable cause for a belief that a designated offense has been, is being, or may be committed,

b. A description of the nature and location of the facility, place, or device from which communication is to be intercepted;

c. The identity, if known, of the person allegedly committing the designated offense whose communication is to be intercepted; and

d. A description of the type of communication(s) to be intercepted.

3. A statement specifying that other investigative procedures:

a. Have been tried and failed; or

b. May not succeed or are too dangerous to attempt;

4. A statement of the duration necessary for the interception. However, if the applicant requests that the authorization for the interception not automatically terminate once the described type of communication is initially obtained the application must also include a description of facts supporting the belief that additional communication of the same type will occur.

5. A statement of facts and any action taken by the court concerning any previous application for a warrant or an extension that:

a. Has been made to a court under this article;
b. Sought to obtain communications from any of the same person, place, or facilities as the current application; and
c. Is known to exist by the persons making the current application.

6. If it is reasonably necessary to make a secret entry upon private property to install an interception device, a statement describing the following:

a. The private property;
b. Who owns and who occupies the private property; and
c. The reasons necessitating a secret entry.

7. In addition to the information required in subsection (a), if an application is for an extension, the application must contain a statement setting forth the results obtained from the original warrant or a reasonable explanation of the failure to obtain results under the original warrant.

8. The court may require an applicant to furnish additional testimony or evidence in support of an application.

9. The duration necessary of the intercept (a maximum of 30 days per initial request); and

10. Any action taken by a court concerning any previous application for an intercept warrant sought for the same person or facility.

C. The SIC Commander and the Chief Counsel will review and verify that all criteria required has been met as outlined within the statute. Requests from within the Department shall be submitted to the Superintendent for final approval. Notification will be made to the Cybercrimes and Investigative Technologies Section Electronic Surveillance Unit (CITS-ESU) that such a request has been made and is currently under court review. The SIC Commander or Chief Counsel will make notification to the Superintendent on applications originating from other law enforcement agencies.

D. The court orders will be immediately forwarded to the CITS-ESU for implementation. CITS command will keep the SIC Commander and the Chief Counsel apprised of intercept activations and de-activations.

E. Prior to monitoring any equipment, entering the wiretap room, or any other area where wiretap information is readily available all personnel must attend minimization training on each phone line or other means of communication to be intercepted.

F. In situations where a warrant intercept is being sought by another agency, the CITS Commander will assign a supervisor to serve as a liaison to assist in facilitating the process. The assigned supervisor will be responsible to ensure the SIC Commander and the Chief Counsel are apprised that a warrant intercept is being sought by an outside agency.

G. The CITS Commander will be responsible to create an in-house numbering system to securely store and track all intercept orders, requests, and the recorded communication. The recorded communications shall be kept for a minimum of 10 years. After 10 years the court ordering the intercept shall be petitioned by the Chief Counsel to determine the disposition of the recordings.

H. This procedure is to be used in conjunction with state and federal law, with all relevant Department regulations, rules, policies, and procedures.