CrimeNtel

Interjurisdictional Criminal Intelligence System
MEMORANDUM OF UNDERSTANDING

Between the

South Carolina State Law Enforcement Division (SLED)

and the

City of Hartsville Police Department.
(Hereinafter referred to as the Participating Agency)

I. Background

The interjurisdictional criminal intelligence system is designed to be used by all South Carolina law enforcement agencies that wish to participate in order to maintain and share criminal intelligence information. The system is currently funded through the South Carolina Law Enforcement Division (SLED) by the Department of Homeland Security, and is provided to Participating Agencies at no cost. This secure system is web-based, and no special equipment or software is needed. The system is administered by the SLED Fusion Center, officially known as the SC Information and Intelligence Center (SCIIC), a joint intelligence center operated by SLED in an "all-crimes", "all-threats" posture to counter criminal and terrorist activity.

II. Concept

The exposure of ongoing criminal activity is aided by the pooling of intelligence information across jurisdictional lines. Participating Agencies may use the system to collect, maintain, share, and query criminal intelligence information on an individual or an organization when reasonable suspicion exists that the individual or organization is involved in criminal conduct or activity, and the information is relevant to that criminal conduct or activity.

III. Purpose

This Memorandum of Understanding (MOU) sets forth an agreement between SLED and the Participating Agency in order to define the roles and responsibilities of each party.

IV. Definitions

A. *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.

B. *Interjurisdictional Intelligence System* means an intelligence system which involves two or more Participating Agencies representing different governmental units or jurisdictions.

C. *Criminal Intelligence Information* means data which has been evaluated to determine that it 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 that it meets criminal intelligence system submission criteria.

D. *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.

E. *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.

F. *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.

G. *Need to Know* means that a *bona fide* criminal investigative requirement or law enforcement activity exists, and the intelligence information in the system is relevant to the investigation or activity.

H. *Right to Know* means that the recipient of information is a law enforcement officer or a civilian employee of a law enforcement agency who is working in support of a *bona fide* criminal investigation to which the intelligence information is pertinent.

V. Operating Principles

A. The Project shall adhere to the Criminal Intelligence Systems Operating Policies set forth in the Code of Federal Regulations 28CFR23.

B. The 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.

C. The 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.

D. 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. 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.

E. The 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. 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.

F. The 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.

G. The 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. 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 is authorized.

H. The Project maintains the authority to screen and remove personnel authorized to have direct access to the system.

I. Information submitted to the System shall be reviewed by the Project Coordinator, or Designee, prior to being made available for viewing by the Participating Agencies. In the event that information submitted does not meet the criteria for final entry into the System, the Project Coordinator, or designee, shall contact the submitting Participating Agency in a timely manner to resolve the matter. Information retained in the system shall be reviewed by the Project Coordinator, or Designee, 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.

J. The Project and Participating Agencies are jointly responsible for ensuring that all System users and recipients are aware that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

K. Unauthorized access, utilization, or disclosure of information contained in the system, may result in termination from participation in the system and/or criminal prosecution.

L. 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.

M. The Chief of SLED or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in V. Operating Principles 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.

VI. Responsibilities

A. South Carolina State Law Enforcement Division

The roles and responsibilities of the SLED SCIIC in this MOU are as follows:

1. Serves as the organizational unit, or Project, which operates the interjurisdictional criminal intelligence system on behalf of the Participating Agencies, in compliance with 28CFR23.
2. Validate information submitted to the system to ensure compliance with 28CFR23, and purge data not in compliance.

3. Conduct annual audits of information in the system, to include ensuring proper dissemination and record-keeping.
4. Conduct ongoing assessment of data in the system to ensure that records maintained by the Project are relevant and important, and that no records are maintained that are misleading, obsolete, or otherwise unreliable.
5. Advise recipient agencies immediately upon the discovery that information disseminated to them contains errors.
6. Disseminate only pertinent information to law enforcement officers or civilian employees (right to know) of a law enforcement agency participating in an ongoing criminal investigation (need to know).
7. Maintain the infrastructure of the system, to include all hardware, software, and associated costs.
8. Train, certify, and grant access to users of the system. Notify all approved users of their obligations under applicable statutes and policies, and obtain acknowledgement in writing.
9. Comply with procedures to maintain and to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster, as set forth in the SCIIC Privacy Policy and the SCIIC Standard Operating Procedure (SOP).
10. Maintain administrative, technical, and physical safeguards (including audit trails) 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.

11. Maintain effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;
12. Restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the Project;
13. Store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;
14. Authorize and utilize remote (off-premises) system data bases to the extent that they comply with security requirements.
15. Remove the credentials of users found to have violated applicable policies for protection of criminal intelligence. SLED employees found to have violated applicable policies may be subject to disciplinary action or criminal prosecution. SLED will notify the employers of non-SLED personnel found to have violated applicable policies.

B. Participating Agency

The roles and responsibilities of the Participating Agency in this MOU are as follows:

1. Comply with the rules set forth in the MOU.
2. Submit and receive criminal intelligence information through the system.
3. Promote the use of the system.
4. Provide qualified users to attend training and to become trainers.
5. Disseminate only pertinent information to law enforcement officers or civilian employees (right to know) of a law enforcement agency participating in an ongoing criminal investigation (need to know).

6. Restrict access to its facilities, operating environment and documentation to authorized organizations and personnel.
7. Upon notification by SLED that a Participating Agency employee has violated applicable policies, review the incident for possible disciplinary action.

VII. Funding

A. SLED has received and continues to pursue grant funding for the development and implementation of the Project. It is SLED's intent to place no financial burden on any Participating Agency.

VIII. General Provisions

A. Term and Termination

This Memorandum shall become effective upon the date of signature of both parties, as designated below, and shall remain in effect until terminated by mutual agreement or by either party upon 60 days advanced written notice to the other party.

This Memorandum shall remain in effect during the term in office of any successor leadership of either party unless terminated or modified.

B. Modification Procedures

Either Party may propose to modify this Memorandum at any time. All proposed modifications shall be in writing and shall become effective only upon written concurrence of both parties.

C. Survival and Severability

If any provisions of this Memorandum are determined to be invalid or unenforceable, the remaining provisions shall continue in force and unaffected to the fullest extent permitted by law and regulation.

D. Liability and Indemnification

Each party shall be responsible for any liability arising from its own conduct and retain immunity and all defenses available pursuant to federal and state law. Neither party agrees to insure, defend, or indemnify the other party.

Each party shall cooperate with the other party in the investigation and resolution of administrative claims and/or litigation arising from conduct related to the provisions of this Memorandum.

E. Third Party Claims

This Memorandum is for the sole and exclusive benefit of the signatory parties, and shall not be construed to bestow any legal right or benefit upon any other persons or entities.

Acknowledgement

This Memorandum of Understanding will be effective upon signature of all parties.

_____ Date: _____

Natalie M. Zeigler,
City Manager
Authorized Signature
Participating Agency

_____ Date: _____

Authorized Signature
South Carolina State Law
Enforcement Division