OVERLAND PARK POLICE DEPARTMENT
STANDARD OPERATING PROCEDURE

NUMBER: 3320
TOPIC: CRIMINAL INTELLIGENCE
EFFECTIVE DATE: 09/27/2018
SUPERCEDES: 02/13/2017

SIGNATURE: */s/ Frank Donchez* — **Chief of Police**; */s/ Simon Happer* — **Bureau Commander**

CALEA references: see below

I. PURPOSE 40.2.3(A)

To establish Department policy and procedures for the collection, processing, analysis, dissemination, and retention of criminal intelligence information.

II. POLICY

The Overland Park Police Department will collect and maintain intelligence information in an effort to anticipate, prevent, or monitor criminal or potential criminal activity and document suspicious incidents which may present a threat to the jurisdiction.

Members will protect the privacy, civil rights and civil liberties of the citizens of Overland Park, and the United States by complying with the requirements of Title 28, Part 23 of the Code of Federal Regulations (28 CFR Part 23) and the policies and procedures outlined in this written directive.

III. PROCEDURE

A. DEFINITIONS

Criminal intelligence is data which has been evaluated to determine that it: (i) 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 (ii) meets criminal intelligence system submission criteria.

Confidential Information is privileged, private or sensitive information and communications. It is the responsibility of all agency personnel to protect and follow the guidelines throughout this written directive regarding confidential information. Such information will only be shared with limited and/or approved personnel for certain purposes such as public safety, on-going criminal investigations, and/or briefing command staff. The dissemination of any confidential information is determined on a need to know basis.

B. PROCEDURES FOR SAFEGUARDING, SECURING, AND STORING INFORMATION 40.2.3(B)

The Department's criminal intelligence file system (the project) is maintained by designated CID personnel and operated out of the Investigations Division. The criminal intelligence file system will meet accepted collection, storage, and dissemination standards, which include administrative, technical, and physical safeguards (including audit trails) to ensure 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 will be kept. Information will be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials.

The project 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 project.

The project will assure that the following security requirements are implemented:

- Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

- The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

- The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

- The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

- The project 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

- The project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

C. TRAINING OF PERSONNEL

The Department will provide appropriate training to Members involved in collecting, sharing, storing and reporting criminal intelligence.

Members involved in criminal intelligence will be responsible for assuring the access, storage and dissemination of intelligence information respects the privacy and Constitutional Rights of individuals, groups and organizations.

All Department Members will receive training on the importance of privacy, Civil Rights, and Civil Liberties protection, intelligence gathering, procedures for reporting and disseminating intelligence information, and the identification of suspicious activity. The Training Unit will be responsible for the coordination of all training provided to commissioned personnel.

D. GUIDELINES

The procedures for ensuring that information collected is limited to criminal conduct or relates to activities that present a potential threat to the jurisdiction are as follows.

Criminal intelligence may be collected on the activities and associations of individuals and groups known or suspected to be involved in criminal acts or threatening, planning, organizing, or financing of criminal acts. Legal and privacy requirements are set forth in 28 CFR Part 23 identify the types of information that may be collected and retained in a criminal intelligence system and are as follows.

Persons who are currently involved in or suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or, are suspected of being or having been involved in criminal activities with known or suspected crime figures.

Organizations, and businesses which are currently involved in or suspected of being involved in the planning, organizing, threatening, financing, or commission of criminal acts; or, are operated, controlled, financed, or infiltrated by known or suspected crime figures.

Criminal intelligence information collected will be limited to the criminal conduct and activities which may present a threat to the jurisdiction such as:

- Organized Crime
- Terrorist Activity
- White-Collar crime
- Narcotics trafficking
- Extortion
- Vice activities
- Infiltration for creation of legitimate business for illegitimate purposes

Intelligence may be gathered from all legal sources. These sources may include, but are not limited to, informants, citizens, other law-enforcement agencies, and public records.

E. LEGAL AND PRIVACY REQUIREMENTS AND PROHIBITIONS

The following types of information shall not be placed in the criminal intelligence file system.

- Information suggesting or concerning lawful political, religious, or sexual preferences, associations or opinions.
- Information relating to a person, the person's family, or associates unless, as a matter of investigative necessity and pertinent to establishing a relationship of association with known or suspected criminal activity.
- Confidential information relating to a criminal investigation whereby documentation is required to support the furtherance of the investigation.

F. DOCUMENTATION AND REPORTING

Information relating to criminal and or suspicious activities should be recorded.

The Department's manner for documenting suspected criminal intelligence and suspicious incidents are via:

- Incident report; and/or
- Field Interrogation report

Reports approved by the unit supervisor will be sent to the designated Investigations Division supervisor using the Department's RMS system.

The designated Criminal Intelligence supervisor will review all information contained in the report to ensure it pertains to criminal conduct and relates to activities that present a threat to the jurisdiction.

G. MAINTENANCE, SECURITY, AND DISSEMINATION OF INTELLIGENCE INFORMATION 40.2.3(C)(D)

The Investigations Division Major and /or his/her designee will ensure that intelligence files contain information on the activities and associations of individuals, organizations, businesses, and groups known or suspected to be involved in criminal acts or in threatening, planning, organizing, or financing of criminal activities.

Intelligence files will be securely maintained and kept separate from other agency reports on an in-house database server.

The Chief of Police is the custodian of the records, and direct access is restricted to specific personnel.

An Investigations Division Captain or designee will review intelligence files on an annual basis to ensure the intelligence information meets the legal requirements for retention. Information is to be purged when it meets any of the following criteria: 40.2.3(E)

- No longer useful
- No longer relevant
- Invalid
- Inaccurate
- Outdated

- Unverifiable

The Chief of Police will designate the Professional Standards Unit the responsibility for seeing all information entered into the criminal intelligence files conforms to the Department's file criteria and has been properly evaluated and classified. An inspection/audit will be conducted on an annual basis.

Information from intelligence files will only be provided to Department Members as well as the personnel of Criminal Justice agencies on a right-to-know authority and need-to-know responsibility, when the information received will aid in the investigation of current criminal activity.

Stored intelligence information will be classified according to the following system.

Security Level, Dissemination Criteria, Release Authority

Sensitive - Restricted to law enforcement personnel having a specific need to know and right to know. Authority to release Sensitive level information will require Investigations Commander or higher authority approval.

Confidential - Restricted to law enforcement personnel having a specific need to know and right to know. Authority to release Confidential level information will require Investigations Commander or designee approval.

Restricted to Law Enforcement - Restricted to law enforcement personnel having a specific need to know and right to know. Authority to release Restricted level information will require Investigations Captain or designee approval.

Unclassified - Not restricted. Authority to release permitted by those assigned to the Investigations Intelligence area.

An Investigations Captain or designee will account for all written disclosures of criminal intelligence information. Each file will maintain a record of the request, recording dissemination information, person/agency requesting, and date of request, need-to-know information, and method of dissemination.

Origin Date: 01/06/2016
Review Date: 02/13/2017
Review Date: 09/27/2018

CALEA references:
40.2.3 (A)(B)(C)(D)(E)