*Please Note: This is a working draft of Directive 0660.00. The PPB has not implemented any portion of this draft. Submit your comments using the "Provide Feedback Here" link located at the end of the directive.

The Bureau is reposting new Directive 0660.00 for 1st universal review to solicit additional feedback. We will consider all comments received during this public comment period, as well as those that the Bureau received in Fall 2018.

660.00 Management of Criminal Intelligence Files (NEW)

Refer:

- 28 CFR § Part 23, Operating Policies
- ORS § 181A.250, Specific information not to be collected or maintained
- OAR Chapter 137, Division 90, Criminal Intelligence Unit
- City of Portland Human Resources Administrative Rule 11.04, Protection of Restricted and Confidential Information
- City of Portland Records Retention Schedule LE-0110, Criminal Intelligence Records
- DIR 0310.70, Dissemination of Information
- DIR 0344.05, Bias-Based Policing/Policing Prohibited
- DIR 0614.50, Release of Information
- DIR 0631.30, Cooperation with Other Agencies
- Law Enforcement Intelligence Units (LEIU) Criminal Intelligence File Guidelines

Definitions:

- Criminal Intelligence: Investigative information that has been collected; analyzed and validated through police reports, field notes, records, systems, or databases to establish a link between entities and criminal activity. Intelligence includes information pertaining to the activities and associations of: 1) Individuals who, based upon reasonable suspicion, are suspected of being or having been involved in a) the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or b) criminal activities with known or suspected crime figures. 2) Organizations, businesses, and groups which based upon reasonable suspicion are suspected of being or having been a) involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or b) illegally operated, controlled, financed, or infiltrated by known or suspected crime figures.

- Criminal Intelligence File: Stored information containing criminal intelligence or a compilation of criminal intelligence.

- Criminal Intelligence System: A designated records system (e.g., database, application, physical equipment) that collects, stores, and allows for the interagency exchange or dissemination, and analysis of criminal intelligence.

- Criminal Investigation: For the purposes of this directive, the process of gathering information and/or evidence about an alleged crime to determine if a crime has been committed, to identify and arrest the perpetrator(s), and provide evidence to support a conviction in court.

- Investigative Information: Data and/or documentation derived from a criminal investigation. Investigative information may not constitute criminal intelligence, but criminal intelligence can include investigative information that has been analyzed and validated.

- Reasonable grounds: As used in these rules, reasonable grounds means reasonable suspicion. Reasonable suspicion is suspicion that is reasonable under the totality of the circumstances. It is less than probable cause and more than mere suspicion.

Policy:

1. This policy establishes guidelines for the Portland Police Bureau's (PPB) management of criminal intelligence files relating to an individual or group/organization suspected of engaging in criminal conduct or activity. The Bureau comports with federal and state regulations regarding the collection and maintenance of criminal intelligence.

2. Information gathering is a fundamental duty of law enforcement. The Bureau maintains a variety of basic information (e.g., reports, files, and databases that contain investigative or management information, public record information, commercial databases, and other fact-based information) that is not subject to criminal intelligence regulations. Members must be able to distinguish basic information and investigative information from criminal intelligence, which is subject to specific rules and regulations. If questions about the distinction exist, members should go through their chain of command to consult with a the Bureau's Criminal Intelligence Unit (CIU)

3. PPB recognizes the significance and impact of collecting, gathering, creating, maintaining, and disseminating criminal intelligence files related to people and organizations. The Bureau expects its members to appropriately manage and safeguard any criminal intelligence in order to preserve the privacy and constitutional rights afforded to individuals. Unauthorized uses of criminal intelligence files shall be investigated and may subject the member to disciplinary action.

Procedure:

1. In accordance with ORS § 181A.250, members shall not collect or maintain information about the political, religious, or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership unless such information directly relates to an investigation of criminal activities, and there are reasonable grounds to suspect the subject of the information is or may be involved in criminal conduct.

2. Criminal Intelligence File Types.
   2.1. All information the Bureau collects for intended retention in a criminal intelligence file must satisfy the reasonable grounds standard, be routinely evaluated for accuracy and validity, and be consistent with applicable laws. CIU shall oversee all of the Bureau's criminal intelligence matters. Therefore, the Bureau authorizes members assigned to CIU to create and maintain criminal intelligence. All other members shall work with CIU if there is a need to create criminal intelligence. CIU members shall only collect and retain raw data and information as established in Oregon Administrative Rules, the United States Code of Federal Regulations, and as described below.
      2.1.1. Working File.

2.1.1.1. Members of CIU shall create working files when reviewing and analyzing newly-acquired raw data to determine if the information constitutes criminal intelligence.

2.1.2. Temporary File.

2.1.2.1. Members of CIU shall create temporary files when there are reasonable grounds that criminal activity has been, is being, or will be committed, but where the subject(s) is unidentifiable; the subject's criminal involvement is questionable; or the reliability of the information source and/or the validity of the information content cannot be determined at the time of receipt.

2.1.3. Permanent File.

2.1.3.1. Members of CIU shall create a permanent file when they have positively identified an individual, group, or organization and have established reasonable grounds that the individual, group, or organization has been, is, or will be involved in criminal activity. These files shall not be permanently retained, as the Bureau is required to purge permanent files after five years.

3. Creation and Maintenance of Criminal Intelligence Files.

3.1. Only members assigned to CIU are authorized to create and maintain criminal intelligence and criminal intelligence files. Members not assigned to CIU who seek to create a criminal intelligence file shall coordinate with CIU to ensure compliance with existing laws, regulations, and criminal intelligence maintenance standards.

3.2. Authorized members must be able to articulate reasonable grounds to collect, gather, and maintain intelligence on an individual(s), group(s), or organization(s) involved or potentially involved in criminal activity or activity that supports criminal conduct.

3.3. Authorized members shall not create criminal intelligence files related to individuals or organizations without first establishing reasonable grounds that definable criminal conduct or criminal activity is occurring, has occurred, or will occur.

3.4. CIU shall review incoming and known information for relevancy, evaluate source reliability and content validity, and ensure the information is valid prior to establishing it as criminal intelligence or creating a criminal intelligence file, and entering it into a criminal intelligence system.

3.4.1. CIU members shall ensure the date and time are recorded on all products (e.g., documents, spreadsheets, etc.) within a criminal intelligence file (printed or electronic) for retention, purging, and auditing purposes.

3.5. Noncriminal Identifying Information.

3.5.1. Authorized members may include in a criminal intelligence file the names of individuals, groups or organizations not suspected of criminal involvement, so long as the information is relevant to the subject of the criminal intelligence file or criminal activity in which the subject has, is, or will be engaged. Noncriminal identifying information is descriptive and/or identifying in nature and intended to provide Bureau members with context regarding the criminal subject or criminal activity being investigated.

3.5.1.1. Authorized members shall clearly label "noncriminal identifying information" in the file to distinguish it from the subject(s) of the criminal intelligence file.

3.5.2. Authorized members shall not use noncriminal identifying information as an independent basis to satisfy reasonable grounds requirements that are necessary to create a criminal intelligence file.

3.5.3. The "noncriminal identifying information" label may be removed if the non-suspect individual or organization becomes reasonably suspected of criminal activity.

3.6. File Classification.

3.6.1. CIU shall classify intelligence to indicate the degree to which it must be kept secure, consistent with LEIU guidelines.

3.7. Criminal Intelligence Review.

3.7.1.1. The CIU supervisor/sergeant or a designee assigned to CIU shall review criminal intelligence files on an ongoing basis to ensure the intelligence is valid, accurate, relevant, and current. Review schedules shall be based on file type: Working File: 30-day review cycle.

3.7.1.1.1. Temporary File: Six-month review cycle.

3.7.1.1.2. Permanent Files: Annual review cycle.

4. Dissemination.

4.1. Only members assigned to CIU are authorized to disseminate criminal intelligence and criminal intelligence files.

4.2. CIU members who are authorized to access criminal intelligence files shall obtain approval from their supervisor prior to posting or disseminating criminal intelligence files or information internally or externally to other law enforcement agencies.

4.3. Authorized members may provide requested criminal intelligence information to the Records Division upon request.

4.3.1. The requesting member from the Records Division shall note any confidentiality or privacy concerns identified by the member providing the information. Some records contained in criminal intelligence files may be exempt from disclosure.

5. Retention and Disposition.

5.1. Any criminal intelligence document or file created for law enforcement purposes are subject to public records requests and CIU must maintain the intelligence in accordance with federal and state regulations. The Bureau shall adhere to the following retention schedules for each category of criminal intelligence files:

5.1.1. Working files: 30 business days. During the 30-day timeframe, CIU shall continue to analyze the information to determine if it constitutes criminal intelligence and is eligible for entry into a criminal intelligence system.

5.1.2. Temporary files: One year, unless updated information is added to the file during the one-year timeframe. If an authorized member(s) has not added supplementary

information to the file by the end of the year, the Records Division shall purge and destroy the information.

5.1.3. Permanent files: Five years, after which CIU shall evaluate the intelligence for its relevance and legal suitability.

5.2. CIU shall submit to the Records Division any criminal intelligence document or file that is no longer needed for an active criminal investigation and that has not satisfied retention or purging requirements.

5.2.1. Members shall send a summary of the different sources where information was found or located (e.g., Regional Justice Information Network [RegJIN], Law Enforcement Data System [LEDS], commercial databases), as well as any work product not available in an existing system (i.e., any work product created by the member as it pertains to the criminal case), to the Records Division.

5.3. Any criminal intelligence document or file exceeding the allotted retention timeframe shall be purged by the CIU supervisor or a designee assigned to CIU, or the Records Division. Members shall refer to Directive 1200.00, Inspections, Maintenance, Responsibility and Authority, for more information.

6. Criminal Intelligence Audit.

6.1. The Bureau's Office of the Inspector General (OIG) shall conduct routine audits of the Bureau's criminal intelligence and related functions to ensure members are acting in accordance with applicable laws pertaining to the collection, dissemination, review, retention, and purging of criminal intelligence files and information.

Provide feedback here.