The Oregon Administrative Rules contain OARs filed through January 15, 2013

QUESTIONS ABOUT THE CONTENT OR MEANING OF THIS AGENCY'S RULES?
CLICK HERE TO ACCESS RULES COORDINATOR CONTACT INFORMATION

DEPARTMENT OF JUSTICE

DIVISION 90

CRIMINAL INTELLIGENCE UNIT

137-090-0000

Purpose

The purpose of these rules is to provide standards, policies and procedures for the operation of the Criminal Intelligence Unit (CIU) of the Organized Crime Section, and to ensure compliance with 28 CFR Part 23.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4) & 28 CFR Part 23
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0010

Authority

The Criminal Intelligence unit operates under the authority of ORS 180.610(2), (3), and (4).

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610 (2), ORS 180.610(3) & ORS 180.610(4)
Hist.: JD 2-1989, f. & cert. ef. 9-13-89

137-090-0020

Abbreviations

(1) CIU: Criminal Intelligence Unit.

(2) CIUS: Criminal Intelligence Unit Supervisor.

(3) CJD: Criminal Justice Division.

(4) AIC: Attorney in Charge of the Organized Crime Section.

(5) CIU/AAG: Assistant Attorney General assigned to the Criminal Intelligence Unit.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3) & ORS 180.610(4)
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0030

Criminal Intelligence Unit Mission

The mission of the Criminal Intelligence Unit is to provide the Department of Justice and Oregon law enforcement agencies with a statewide criminal information base and analyses which meets their needs to protect the public and suppress criminal activity.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3) & ORS 180.610(4)
Hist.: JD 2-1989, f. & cert. ef. 9-13-89

137-090-0040

Public Access

(1) The Criminal Intelligence Unit will comply with the the Oregon Public Records law in responding to requests by members of the public for file information to the extent that the law allows and to the degree the materials requested are not classified according to defined restrictions on dissemination.

(2) The Criminal Intelligence Unit will comply with the "Third Agency Rule" which is explained as follows: Reports and other investigative material and information received by the Criminal Intelligence Unit shall remain the property of the originating agency, but may, subject to consideration of official need, be retained by the Criminal Intelligence Unit. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given thereto except, with the consent of the investigative agency concerned, to other departments and agencies on a right to know, need to know basis. This policy also applies to individuals, groups or organizations requesting specific records or material under the Freedom of Information Act or Oregon Public Records Law.

(3) The originating agency shall determine whether the investigative report, material or other information may be released to the requestor, or whether the requestor should be referred to that agency for disposition of the case. In any case, the decision by the originating agency shall not be contested by the Criminal Intelligence Unit.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3) & ORS 192.410 et seq.
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0050

Definition of 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.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), (3) & (4)
Hist.: JD 2-1989, f. & cert. ef. 9-13-89

137-090-0060

Definition of Criminal Intelligence File

A criminal intelligence file consists of stored information on the activities and associations of:

(1) Individuals who:

(a) Based upon reasonable suspicion are suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or

(b) Based upon reasonable suspicion are suspected of being or having been involved in criminal activities with known `or suspected crime figures.

(2) Organizations, businesses, and groups which:

(a) Based upon reasonable suspicion are suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or

(b) Based upon reasonable suspicion are suspected of being or having been illegally operated, controlled, financed, or infiltrated by known or suspected crime figures.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4), ORS 181.575 & 28 CFR §23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89

137-090-0070

File Content

Only information meeting the CIU's criteria for file input will be stored in the criminal intelligence files. No information will be collected or maintained about the political, religious, racial, or social views, sexual orientation, 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.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3) ORS 180.610(4), ORS 181.575 & 28 CFR §23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89

137-090-0080

File Categories

All information to be retained in the criminal intelligence files must meet the stated guidelines for file definition and content. Information will only be retained in one of three file categories as set forth below:

(1) Working File:

(a) The working file is the receiving phase of newly acquired raw data. The CIU staff review the new materials for its acceptability to the CIU's criminal intelligence system.

(b) Retention Period: The retention period is thirty working days during which effort is made to determine the value of the raw data and its acceptability to the CIU's criminal intelligence system.

(2) Temporary File:

(a) The temporary file includes individuals, groups, businesses, and organizations which have *not* been positively identified by one or more distinguishing characteristics, or whose criminal involvement is questionable;

(b) Individuals, groups, and organizations are given temporary file status *only* in the following situations:

(A) The subject is unidentifiable because there are no physical descriptors, identification numbers, or distinguishing characteristics available; and

(B) The subject's involvement in criminal or gang activities is questionable; and

(C) The subject has a history of criminal or gang conduct, and the circumstances afford him an opportunity to again become active; and/or

(D) The reliability of the information source and/or the validity of the information content cannot be determined at the time of receipt; and

(E) The information appears to be significant and merits temporary storage.

(c) Retention Period: The retention period is one year during which time effort is made to secure additional data verification. If the information still remains in the temporary file at the end of one year with no update information added, and no information is available, the information is purged and destroyed.

(3) Permanent File:

(a) This file includes individuals, groups, businesses, and organizations which have been positively identified by one or more distinguishing characteristics and criminal involvement;

(b) Retention Period: The retention period is five years after which the information is evaluated for its file acceptability.

Stat. Auth.: ORS 180

Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4), ORS 181.575 & 28 CFR §23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89

137-090-0090

Information Input

Information to be stored in the CIU's criminal intelligence file must first undergo a review for relevancy and an evaluation for source reliability and information validity prior to filing:

(1) Relevancy Review: Incoming information is reviewed by the CIUS, or a designee of the Chief Counsel, to determine its relevancy to the CIU's mission.

(2) Source Reliability: The term, source, relates to the individual, group, or organization providing the information to the CIU. Source reliability will be determined according to the criteria set forth in **Table 1**. [Table not included. See ED. NOTE]

(3) Information Validity: The term, information, relates to written, oral, and/or pictorial materials provided to the CIU by the individual, group, or organization. Information validity will be determined according to the criteria set forth in **Table 2**. [Table not included. See ED. NOTE]

[ED. NOTE: Tables referenced are available from the agency.]

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4) & 28 CFR sec. 23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0100

Information Classification

(1) General: In order to protect sources, investigations and individual rights to privacy, information retained in the CIU's criminal intelligence file is classified to indicate the degree to which it must be kept secure. Many documents received by the CIU have classifications assigned to them by the senders. In such cases, CIU personnel must take care to review and to assign levels of security classification not below that given by senders. The classification of criminal intelligence information is subject to continual change. The passage of time, the conclusion of investigations, and other factors may affect the security classification assigned to particular documents. Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher or lesser degree of document security is required and to insure that information is released only when and if appropriate.

(2) Classification: Criminal intelligence information is classified according to the following system:

(a) Sensitive:

(A) The classification, sensitive, is assigned by the contributor agency or by the CIUS in consultation with the Chief Counsel, Attorney-in-Charge of the Organized Crime Section or the Chief Investigator and is given only to documents which relate to:

(i) Information pertaining to significant law enforcement cases currently under investigation;

(ii) Public Corruption;

(iii) Informant identification information;

(iv) Criminal intelligence reports which require strict dissemination and release criteria;

(v) Documents which have been designated sensitive by another law enforcement agency;

(vi) A document bearing this classification cannot be disseminated without the approval of the contributor agency. When the Oregon Department of Justice is the contributor agency, a document bearing this classification cannot be disseminated without the approval of the Chief Counsel, Attorney-in-Charge of the Organized Crime Section or the Chief Investigator.

(b) Confidential:

(A) The classification, confidential, is assigned by the contributor agency or the CIUS and is given to the following documents:

(i) Criminal intelligence reports which are not designated sensitive;

(ii) Information obtained through intelligence unit channels which is not classified sensitive and is for law enforcement intelligence use only;

(iii) Documents which describe ongoing investigatory projects and open investigations;

(iv) Documents which describe law enforcement strategies and techniques;

(v) Documents which have been designated confidential by another law enforcement agency.

(B) A document bearing this classification can be released with the approval of the contributor agency.

(c) Restricted:

(A) The classification, restricted, is assigned by the contributor agency or the CIUS and is given to documents of general use in the CIU such as reports that at an earlier date were classified sensitive or confidential and the need for high level security no longer exists or non-confidential information prepared for/by law enforcement agencies;

(B) A document bearing this classification can be released for general law enforcement use with the approval of the CIUS.

(d) Unclassified: The classification, unclassified, is assigned by the CIUS and is used to identify documents of a public nature. Examples of unclassified materials include non-news related information to which, in its original form, the general public had direct access (i.e., birth and death certificates, corporation papers, etc.) and news media information such as newspapers, magazine and periodical clippings dealing with specified criminal categories;

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4), ORS 181.575 & 28 CFR §23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0110

Information Contributions

To the extent possible, all criminal intelligence maintained in CIU files must display the names and phone numbers of persons and agencies providing the information. When anonymity is requested by a contributor, a contributor code number may be used. All contributor code numbers will be provided and retained by the CIUS. When a contributor's name identification is difficult to obtain, it will suffice to describe the contributor in general terms. All information obtained from the public domain will be identified by document name, date and page number. In addition to identifying the source, the manner in which the source obtained the information is described.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4) & 28 CFR §23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89

137-090-0120

Quality Control

Information stored in the CIU's criminal intelligence file will undergo a review by the CIUS, or a designee of the Chief Counsel, for compliance with the law and with the standards, policies, and procedures of this chapter before its entry into the file. The CIU/AAG shall provide legal oversight and advice to CIU personnel in all matters involving the CIU to insure compliance with federal and state law.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4), ORS 181.575 & 28 CFR §23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0130

Dissemination

Criminal intelligence information is disseminated only to personnel of criminal justice agencies and only on a "right to know" authority and "need to know" responsibility.

(1) Definitions:

(a) "Right to know": Requester agency has official capacity and statutory authority to the information being requested.

(b) "Need to know": Requested information is pertinent and necessary to the requester agency in initiating, furthering, or completing an investigation.

(2) Control:

(a) It is the policy of the Organized Crime Section to account for date, nature and purpose of all disclosures of criminal intelligence by the CIU. The accounting includes names, title, and agency of the person or agency to whom the disclosure is made, what was disclosed and the name, if any, of the person making the disclosure. Disclosures are made in accordance with the security classification designated by the contributor agency, and the contributor agency shall be notified of all disclosures.

(b) The accounting required by (2)(a) of this rule will be electronically completed every time criminal intelligence is accessed

(c) All disclosures of criminal intelligence are logged and the records of the disclosures are retained for the life of disclosed documents.

(d) An accounting will be electronically completed every time the criminal intelligence files are queried. This accounting will be retained for a period of one year, and includes the inquirer's name and agency, the agency phone number, the nature of the inquiry, and the name of the person who is the subject of the inquiry.

(3) Unauthorized Access: The person requesting and receiving criminal intelligence is solely responsible for the security of that information. Any person possessing the disseminated criminal intelligence other than the original requester, except as provided in section (4) of this rule, is deemed to have unauthorized access.

(4) Unauthorized Dissemination: No CJD employee requesting and receiving CIU criminal intelligence will allow access to this information by other individuals except at meetings or during shared project assignments in which the subject of the criminal intelligence is being used and all the participants in these meetings and/or projects meet the dissemination criteria of this chapter.

(5) Dissemination Restriction: Any person accessing CIU criminal intelligence shall disseminate that information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these rules. This provision shall not limit 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.

(6) Dissemination Table: **Table 3** sets forth the classification level, dissemination criteria and release authority for information stored in CIU files. [Table not included. See ED. NOTE.]

[ED. NOTE: Tables referenced are available from the agency.]

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3) & ORS 180.610(4) & 28 CFR § 23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0140

Security

Because security and protection of the materials in the criminal intelligence file is of utmost importance, the following procedures shall be observed:

(1) Policy: All CIU employees shall be thoroughly familiar with access and dissemination policies of this chapter. All other persons authorized to access criminal intelligence information as provided in these rules shall agree to follow procedures regarding information access, security, and dissemination which are consistent with these rules.

(2) Access: Direct access to the CIU's criminal intelligence files is limited to CIU file section employees, the CIUS and personnel of criminal justice agencies as approved by the CIUS.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4) & 28 CFR §23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0150

File Review and Inspection

(1) Review Authority: All information in the criminal intelligence file is subject to review at any time by the Chief Counsel, Attorney-in-Charge of the Organized Crime Section, Chief Investigator, CIU/AAG, Deputy Attorney General and Attorney General.

(2) CIUS Document Review: By July 1 of each year, the CIUS shall review a representative random sample of the materials in the file to determine the need for document classification change in accordance with this chapter.

(3) CIUS Operational Inspection: By July 1 of each year, the CIUS will inspect all aspects of the intelligence file operation. This inspection shall include, but not be limited to, the following:

(a) Parameters of Review: Review the CIU rules to insure they are in accordance with current law and accurately reflect the standards, policies and procedures of CJD. Check recently submitted criminal intelligence to insure it meets CIU criteria. Review indexing for compliance with established CIU procedures. Check completed electronic source document for accuracy -- AKAs, monikers, categories, sequence numbers, and other requirements. Review the electronic accounting audit information to ensure it is properly maintained and functioning appropriately;

(b) Review Procedures: The CIU staff shall select at random five electronic source documents from each major crime category. Staff will review these documents to ensure that all materials meet file criteria. Staff will ensure that electronic purge information is accurate and complete. Staff will study all materials not meeting the criteria and will take immediate corrective action;

(c) Criminal Intelligence Unit Supervisor's Report: The CIUS shall compose a written report of the findings of this review and shall submit the report to the Chief Counsel through the Chief Investigator and Attorney-in-Charge of the Organized Crime Section. The report will describe the general condition of the files and any corrective measures taken.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4), ORS 181.575 & 28 CFR § 23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0160

Purging

All information in the Criminal Intelligence file is eventually removed and destroyed. Its removal and destruction is in accordance with the following purge and destruction criteria:

(1) Purging Constraints: All file material selected for purging and destruction will only be removed and destroyed when it meets the requirements of these rules.

(2) Purge Criteria: Information is only purged when it is:

(a) No longer useful;

(b) No longer relevant;

(c) Invalid;

(d) Inaccurate;

(e) Beyond retention period;

(f) Unverifiable; or

(g) Inconsistent with mission.

(3) Purging Process: The first step for determining which documents in file require purging begins with their selection according to purge criteria as described in section (2) of this rule.

(4) Process for Retention: When the CIUS wishes to retain information which has been recommended for purge, he/she must substantiate his/her reasons for retention to the Chief Investigator. Final decision on retention is made by the Attorney-in-Charge of the Organized Crime Section. In matters of great exception, the final decision will be made by the Chief

Counsel of the Criminal Justice Division.

(5) Retention Period: Any information ordered retained will be placed in the permanent section of the central file for a new retention period of five years from date of re-entry.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4), ORS 181.575 & 28 CFR § 23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0170

Destruction

Material purged from the criminal intelligence file shall be removed and destroyed under the supervision of the CIUS. Removal and destruction will be accomplished electronically consistent with statutes and rules relating to destruction of public records.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), (3) & (4) & 387.805 et seq.
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0180

File Integrity Officer

The CIUS will be CIU's File Integrity Officer. In this capacity, the CIUS is responsible for the contents of all intelligence files in the CIU and for their compliance with these rules.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), (3) & (4), 181.575 & 28 CFR § 23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0190

File Room Requirements

(1) The CIUS shall adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to information contained in the CIU criminal intelligence files.

(2) The CIUS shall restrict access to CIU facilities, operating environment and documentation to organizations and personnel authorized by these rules.

(3) The CIUS shall institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3) & ORS 180.610(4)
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0200

File Index Number System

(1) General Information:

(a) The CIU's criminal intelligence files are indexed according to a modified Dewey Decimal System. In the CIU's system, file categories and sub-categories are separated by decimal points;

(b) File categories are created or deleted at the request of CIU personnel as needs arise for more crime topic areas. The list of authorized crime topics is always in a state of change. A request for a change in the index system is first brought to the attention of the CIUS through the use of the memorandum. If approved by the CIUS, the index system is altered to reflect the change and an updated file index list is distributed to all CIU personnel possessing copies of file guidelines.

(2) Crime Topic:

(a) Crime topics are those authorized for collection, storage, and dissemination according to the mission of the CIU. The

crime topics list is classified *confidential* and is not to be duplicated or released outside the CIU without the express authorization of the CIUS. The list is for official staff use only;

(b) The crime topics list is not to be removed from the CIU file room without the approval of the CIUS.

(3) Use of Index Numbers: The file category, *general*, is only used when there is insufficient data available to indicate a more specific index selection.

(4) Spread of Index Numbers: The index system is displayed as several independent groupings of numbers separated by decimal points. The following defines the various groupings.

(a) Group 1 (Mission): Index numbers in the first position represent the subject of the file. As examples are the following: 10. Political Corruption; 20. Major Financial Crimes; 30. Traditional Organized Crime; 40. Emerging Criminal Gangs and Street Gangs; 50. General;

(b) Group 2 (Crime Group): Index numbers in the second position represent documented, definable criminal organizations.

(b) Group 3 (Crime): Index numbers in the third position represent crime the subject is involved in;

(c) Group 4 (Geographic Assignment): Index numbers in the fourth position represent geographic areas;

(d) Group 5 (File Position): Index numbers in this last group represent the document's position in the file. The numbers are assigned chronologically.

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3) & ORS 180.610(4)
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0210

Forms

The CIU will only use forms developed, tested, and approved for use by the Criminal Justice Division. Only the forms described below are authorized for use in the CIU file system.

(1) Criminal Intelligence Report (IR) (CJD Form 35).

(a) The Criminal Intelligence Report form is the CIU's standard collection document pertaining to criminal intelligence. It is designed to provide both collection and a more efficient way to analyze and disseminate what the CIU handles in the way of information;

(b) The IR is used by investigators and CJD staff alike as they collect criminal information in person, by mail, phone, and through access to public and controlled information;

(c) The IR is designed to collect information on one event only. It should never be used to report on several events at the same time such as a stakeout observation combined with information about a later meeting in which the stakeout findings were discussed;

(d) IR Preparation Guide: As a guide for the use of the IR, the following applies:

(A) Record one event per IR

(B) Write in the first person

(C) State and evaluate your sources

(D) Forward the IR promptly.

(2) Request for File Retention (CJD Form __).

(a) It is the policy of the CJD that all items of information contained in the CIU files will one day be purged and destroyed. Purging is an ongoing effort, thus creating daily voids of items of information in the file. The electronic "Purged and Destroyed" message is designed to earmark purged criminal intelligence information so that all voids are accounted for.

(b) When the CIUS wishes to retain information that has been scheduled for purge, the CIUS must substantiate the reasons for retention. Once an item of information has been identified as possibly meeting retention criteria, a hard copy of the

information is attached to the "Request for File Retention" form. The item is then routed to the Chief Investigator for initial review and decision. The Chief Investigator reviews the item of information and makes the initial decision regarding its retention or destruction. The item is then routed to the Attorney-in-Charge of the Organized Crime Section for final review and approval. Criminal intelligence information may be retained in the CIU file for the following reasons:

(A) Additional indices relating to the subject and criminal activities have been submitted and are contained in the CIU file system.

(B) The audit information indicates that the information has been significantly accessed by law enforcement in conjunction with criminal investigation(s).

(C) The subject is a major offender and there is reason to believe the subject still represents a criminal threat.

(D) The subject is an active member of a documented criminal organization and that organization represents a criminal threat.

(c) Criminal intelligence information meeting purge criteria will be removed from the system and destroyed.

[ED. NOTE: The Forms(s) referred to in this rule are available from the agency.]

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4), ORS 181.575, ORS 387.805 et seq. & 28 CFR § 23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0220

Statement of Understanding (CJD Form 34)

All Criminal Justice Division employees who are assigned to the Criminal Intelligence Unit shall read these rules and sign an understanding of such. All persons authorized to access criminal intelligence information as provided in these rules shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these rules.

[Publication: The Publication(s) referred to or incorporated by reference in this rule are available from the agency.]

Stat. Auth.: ORS 180
Stats. Implemented: ORS 180.610(2), ORS 180.610(3), ORS 180.610(4), ORS 181.575, ORS 387.805 et seq. & 28 CFR § 23.20
Hist.: JD 2-1989, f. & cert. ef. 9-13-89; DOJ 11-2000, f. & cert. ef. 8-9-00

137-090-0225

Transition Procedures

The handling of "hard-copy" criminal intelligence information submitted to the CIU prior to the effective date of these amended rules shall be governed by the provisions of former OAR Chapter 137, Division 90, adopted in September 1989. Once the information has been entered into the electronic database in compliance with these amended rules, adopted on August 8, 2000, the hard copy files may be purged and destroyed.

Stat. Auth.: ORS 180; ORS 357.805 et seq.
Stats. Implemented: ORS 180.610, ORS 181.575, ORS 357.805 et seq.
Hist.: DOJ 11-2000, f. & cert. ef. 8-9-00
