CHAPTER 81
CRIMINAL INTELLIGENCE INFORMATION

[Prior to 11/8/06, see 661—8.201(692) to 8.207(692)]

661—81.1(692) Definitions. The following definitions apply to rules 661—81.1(692) through 661—81.5(692).

"Criminal intelligence file" means information stored in a criminal intelligence system that is compiled in an effort to anticipate, prevent, or monitor possible criminal activity on:

1. An individual who, based upon reasonable grounds, is believed to be involved in the actual or attempted planning, organization, financing, promotion, or commission of criminal acts or is believed to be involved in criminal activities with known or suspected criminal offenders.

2. A group, organization or business which, based on reasonable grounds, is believed to be involved in the actual or attempted planning, organization, financing, promotion, or commission of criminal acts, or of being illegally operated, controlled, financed, promoted, or infiltrated by known or suspected criminal offenders.

3. An incident in which sufficient articulable facts give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that a definable criminal activity or enterprise is, has been, or may be committed.

"Criminal intelligence file" does not include surveillance data as defined in Iowa Code section 692.1.

"Criminal intelligence system" means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

"Need to know" is established if criminal intelligence information will assist a recipient in anticipating, investigating, monitoring, or preventing possible criminal activity or if criminal intelligence information is pertinent to protecting a person or property from a threat of imminent serious harm.

"Noncriminal identifying information" means information about the characteristics and associations of an identifiable person suspected of being involved in criminal activity.

"Reasonable grounds" means information that establishes sufficient articulable facts that give a trained law enforcement or criminal investigative agency officer, investigator, or employee a reasonable basis to believe that a definable criminal activity or enterprise is, has been, or may be committed.

"Right to know" is established when a recipient of criminal intelligence information is legally permitted to receive intelligence data or an intelligence assessment.

"Surveillance data" means information on individuals, pertaining to participation in organizations, groups, meetings or assemblies, where there are no reasonable grounds to suspect involvement or participation in criminal activity by any person. Noncriminal identifying information does not constitute surveillance data.

"Threat of imminent serious harm" means a credible impending threat to the safety of a person or property. A threat of imminent serious harm justifies the dissemination of intelligence data or an intelligence assessment for the purpose of protecting a person or property from the threat.

661—81.2(692) Iowa law enforcement intelligence network (LEIN) information system.

81.2(1) *LEIN information system.* The Iowa law enforcement intelligence network (LEIN) information system is the statewide interjurisdictional intelligence system maintained and operated by the intelligence bureau of the department of public safety, for the regular interagency exchange of criminal intelligence files. Criminal intelligence files contained in the LEIN information system may be disseminated or redisseminated by the intelligence bureau of the department of public safety, consistent with Iowa Code chapter 692.

81.2(2) *Direct computer access.* The commissioner of public safety may authorize a peace officer, criminal justice agency, or state or federal regulatory agency to access the LEIN information system directly via a remote computer terminal, provided that the authorized individual or agency follows

approved procedures regarding receipt, maintenance, dissemination, submission and security of information, and related training. Authorization may be provided in writing or electronically.

81.2(3) *Termination of authorization for direct computer access.* The commissioner of public safety may, at any time for good cause, terminate authorization for direct, remote computer access to the LEIN information system which has been previously approved. An individual or agency whose authorization to directly access the LEIN information system via remote computer has been terminated may appeal the termination in accordance with procedures for contested cases established in 661—Chapter 10.

81.2(4) *Reinstatement of authorization for direct computer access.* Any user whose authorization for direct, remote computer access to the LEIN information system has been terminated may apply for the authorization for access to be reinstated, provided that the problem which led to the termination has been corrected.

81.2(5) *Applications for direct computer access.* To apply for direct, remote computer access to the LEIN information system or to obtain further information about the LEIN information system, a person shall contact the Intelligence Bureau, Iowa Department of Public Safety, Wallace State Office Building, Des Moines, Iowa 50319, or by electronic mail via the Internet at intinfo@dps.state.ia.us.

81.2(6) *Entry of information—restrictions.* Information about the political, religious, racial, or social views, associations, activities or sexual orientation of any individual shall not be entered into the LEIN information system unless such information constitutes noncriminal identifying information or is relevant to an investigation of criminal conduct or activity involving an identifiable individual.

81.2(7) *Entry of information—conformance with applicable law.* No information that is deemed unreliable because it has been obtained in violation of any applicable federal, state, or local law or ordinance, or these rules, may be entered into the LEIN information system.

81.2(8) *Dissemination.* Intelligence data from the LEIN information system may be disseminated only to peace officers, criminal justice agencies, or state or federal regulatory agencies. Intelligence data from the LEIN information system may be disseminated only when there is a right to know and a need to know in the performance of a law enforcement activity. Intelligence data from the LEIN information system shall not be disseminated to any user whose authorization to access the LEIN information system has been terminated and has not been reinstated.

EXCEPTION: Intelligence assessments may be disseminated to any agency or organization for an official purpose or to a person in order to protect a person or property from the threat of imminent serious harm as defined in rule 661—81.1(692).

81.2(9) *Redissemination of intelligence data.* An agency, organization, or person receiving intelligence data from the department pursuant to Iowa Code chapter 692 may redisseminate the intelligence data only if authorized by the agency or peace officer who originally provided the data and if the data is for an official purpose in connection with the prescribed duties of the recipient. If the agency, organization, or person receiving the information is not a peace officer, criminal or juvenile justice agency, or state or federal regulatory agency, redissemination is allowed only if such redissemination is for an official purpose and if the information is redisseminated in order to protect a person or property from the threat of imminent serious harm. The department may also place restrictions on the redissemination by the agency, organization, or person receiving the intelligence data. Any agency, organization, or person who redisseminates intelligence data pursuant to Iowa Code chapter 692 must maintain a list of the agencies, organizations, and persons receiving the intelligence data and the purpose of the redissemination. Intelligence data must be maintained separately from and should not be included in any form in any investigative or prosecutorial files.

81.2(10) *Redissemination of intelligence assessment.* An agency, organization, or person receiving an intelligence assessment from the department pursuant to Iowa Code chapter 692 may redisseminate the intelligence assessment only if authorized by the department and only if the redissemination is for an official purpose in connection with the prescribed duties of the recipient. If the agency, organization, or person receiving the intelligence assessment is not a peace officer, criminal or juvenile justice agency, or state or federal regulatory agency, redissemination is allowed only if such redissemination is to protect a person or property from the threat of imminent serious harm. The department may also place restrictions on the redissemination by the agency, organization, or person receiving the

intelligence assessment. Any agency, organization, or person who redisseminates an intelligence assessment pursuant to Iowa Code chapter 692 must maintain a list of the agencies, organizations, and persons receiving the intelligence assessment and the purpose of the redissemination. An agency, organization, or person who redisseminates information without proper authorization may be prohibited from receiving further intelligence assessments.

661—81.3(692) Criminal intelligence file security. The intelligence bureau of the department of public safety shall adopt administrative, technical, and physical safeguards, including audit trails, to ensure against unauthorized access and against intentional or unintentional damage to the LEIN information system. These safeguards shall include, but are not limited to, the following:

81.3(1) Records indicating who has been given the information, the reason for release of information, and the date of any dissemination shall be maintained until the information has been purged.

81.3(2) Criminal intelligence files shall be labeled to indicate security level and identities of submitting agencies and submitting individual.

81.3(3) Where appropriate, effective and technologically advanced computer software and hardware designs shall be implemented to prevent unauthorized access.

81.3(4) Any access to criminal intelligence files and computing facilities in which the files are stored shall be restricted to authorized personnel.

81.3(5) Criminal intelligence files shall be stored in such a manner that the files cannot be modified, destroyed, accessed, purged, or overlaid in any fashion by unauthorized personnel.

81.3(6) Computer systems on which criminal intelligence files are stored shall be programmed to detect, reject, and record any unauthorized attempt to access, modify, or destroy criminal intelligence files or to otherwise penetrate the security safeguards on such a system.

81.3(7) Access to any information required to gain authorized access to criminal intelligence files, including access codes and passwords, shall be restricted only to personnel authorized to access these files. The intelligence bureau shall ensure that criminal intelligence files remain confidential when specific agreements are entered into with individuals or organizations that provide computer or programming support to the agency.

81.3(8) Procedures shall be adopted to protect criminal intelligence files from unauthorized access, theft, sabotage, fire, flood, wind, and natural or other disasters.

81.3(9) Procedures shall be adopted which establish the right of the intelligence bureau to screen and, if appropriate, reject for employment any personnel who would, if hired, have access to criminal intelligence files.

81.3(10) Procedures shall be established which allow the removal or transfer, based on good cause, of any existing employees from positions in which they have access to criminal intelligence files.

81.3(11) Any compromise, or suspected compromise, of information that would allow unauthorized access into criminal intelligence files shall be reported without delay and, in any event, by the end of the next business day, to a supervisor within the intelligence bureau of the department of public safety.

81.3(12) Any compromise, or suspected compromise, of information contained in criminal intelligence files shall be reported without delay and, in any event, by the end of the next business day, to a supervisor within the intelligence bureau of the department of public safety.

661—81.4(692) Review of criminal intelligence files—purging.

81.4(1) The intelligence bureau of the department of public safety shall regularly review the information in criminal intelligence files for reclassification or purging. Decisions to retain, reclassify, or purge criminal intelligence files shall:

a. Ensure that the information is current, accurate and relevant to the needs of the agency.

b. Safeguard individual privacy interests protected by federal and state laws.

c. Ensure that security classifications remain appropriate.

81.4(2) Information that is misleading, unreliable, or no longer useful shall be purged or reclassified when necessary, without delay and, in any event, within one business day of the discovery that the

information is misleading, unreliable, or no longer useful. Any person or agency to which the criminal intelligence file was disseminated shall be notified of the reclassification or purge.

81.4(3) All information shall be reviewed within a five-year period of its submission to ensure compliance with subrule 81.4(1).

81.4(4) All information retained as a result of a review shall reflect the name of the reviewer, date of review, and an explanation of the decision to retain.

81.4(5) Information that is not retained in a criminal intelligence file after a review shall be deleted from the LEIN information system.

661—81.5(692) Subpoenas and court orders. Any agency or individual shall notify the department of public safety in writing without delay and, in any event, by the end of the next business day of the receipt of any subpoena, court order, request for production, or other legal process demanding the production of a criminal intelligence file, so that the department has an opportunity to make a timely resistance.

These rules are intended to implement Iowa Code chapter 692.

[Filed 10/19/06, Notice 9/13/06—published 11/8/06, effective 1/1/07]