CHAPTER 8
CRIMINAL JUSTICE INFORMATION
[Prior to 4/20/88, see Public Safety Department[680] Ch 8]

661—8.1 to **8.100** Reserved.

DIVISION I
IOWA ON-LINE WARRANTS AND ARTICLES SYSTEM
[Prior to 8/16/95, see 661—8.1 to 8.101]

661—8.101(80,692) Iowa on-line warrants and articles (IOWA) criminal justice information system. The Iowa on-line warrants and articles (IOWA) criminal justice information system is administered by the division of administrative services, field services bureau. The IOWA system, created pursuant to Iowa Code paragraph 80.9(2)*"d"* and Iowa Code section 692.14, provides criminal justice agency access to traffic record and criminal justice databases through a dedicated telecommunications network. To be eligible for access to the IOWA system, an agency must be a criminal justice agency at the federal, state, or local level within Iowa, or an agency providing services to criminal justice agencies in Iowa.

661—8.102(80,692) Information available through the IOWA system. The IOWA system provides access to databases from various state agencies within Iowa, from the Federal Bureau of Investigation's National Crime Information Center (NCIC), and from the motor vehicle departments of other states nationally through the National Law Enforcement Telecommunications System (NLETS). Information on an international basis is also provided by NCIC and NLETS through interfaces to Canadian Police Information Centre and to INTERPOL. The NLETS system also provides administrative message traffic between Iowa criminal justice agencies and criminal justice agencies throughout the United States.

The IOWA system allows criminal justice agencies to:

1. Access nationwide computerized banks of information such as wanted, missing, and unidentified persons; stolen vehicles; stolen articles; stolen boats; stolen guns and stolen securities.
2. Access driver license and motor vehicle information in-state as well as out-of-state.
3. Exchange criminal history information on a national basis.
4. Communicate by use of administrative messages with other criminal justice agencies worldwide.

661—8.103(80) Human immunodeficiency virus-related information. An agency may enter human immunodeficiency virus-related (HIV) information into a wanted or missing person file of the IOWA system and the National Crime Information Center operated by the Federal Bureau of Investigation. HIV information shall be kept confidential and may be communicated only in accordance with this rule.

8.103(1) HIV information on an individual entered into the IOWA system or the National Crime Information Center operated by the Federal Bureau of Investigation shall be made available to terminal operators for the purpose of informing individuals who are authorized access pursuant to this rule.

8.103(2) HIV information may be communicated to:

a. Employees and supervisors of employees of a law enforcement agency who have, or are expected to have, direct physical control of an individual reported to be HIV positive.

b. Employees and supervisors of employees subject to the jurisdictional supervision of the Iowa department of corrections who have, or are expected to have, direct physical supervision of an individual reported to be HIV positive.

c. Employees and supervisors of employees of secure facilities for juveniles subject to the jurisdiction of the Iowa department of human services who have, or are expected to have, direct physical supervision of an individual reported to be HIV positive.

d. Employees and supervisors of employees of city and county jails who have, or are expected to have, direct physical supervision of an individual reported to be HIV positive.

8.103(3) HIV information shall not be transmitted over any law enforcement radio broadcasting system, cellular telephone system, radio telephone system, or any other radio-based communications system. This provision shall not apply to the transmission of HIV information in data form to or from mobile digital terminals or mobile digital computers authorized access to the IOWA system and operated by a law enforcement officer or certified IOWA system operator in the performance of official duties.

8.103(4) Individuals who receive HIV information pursuant to this rule shall use the information solely for the purpose of the protection of those individuals having or expected to have direct contact with individuals reported to be HIV positive, and for the prevention of the spread of the HIV virus. Information shall be provided only to individuals and their supervisors who have direct physical contact with persons reported to have the HIV virus. Except as provided in subrule 8.103(2), information obtained pursuant to this rule shall not be communicated to any person not employed by the agency employing the person providing it or used outside the agency for any purpose.

8.103(5) Individuals who are authorized to receive HIV information pursuant to this rule shall receive training developed and established by the commissioner of public safety, in cooperation with the department of corrections and the department of public health, regarding the confidentiality standards applicable to HIV information received from the IOWA system or the National Crime Information Center.

661—8.104(80,692) IOWA system security. IOWA system terminal access shall be available to criminal justice agencies as defined by Iowa Code section 692.1(7). Prior to being permitted terminal access to the IOWA system, a criminal justice agency shall meet the following criteria:

8.104(1) All terminals shall be located within the facilities or vehicles of authorized agencies where appropriate physical security can be maintained.

8.104(2) The immediate terminal areas shall be restricted to prevent access by unauthorized individuals.

8.104(3) All persons accessing NCIC and the criminal history files shall have been authorized to operate the terminal by the criminal justice agency administrator, been approved by the department of public safety, received the required training and achieved proficiency certification by the department of public safety.

Agencies shall complete a background investigation on all applicants for positions with access to NCIC and criminal history files. Agencies shall notify the department of public safety of the completion of the required background investigation. The background investigation shall be done to ensure the following:

a. That the applicant is 18 years of age or older at the time of appointment to the position.

b. That the applicant is not addicted to drugs or alcohol.

c. That the applicant is of good moral character and has not been convicted of a serious crime.

d. Agencies shall submit two fingerprint cards on all applicants to the Iowa division of criminal investigation. One card will be used to check for any Iowa criminal history and the second card will be forwarded to the FBI for a national search of criminal history records.

8.104(4) Where IOWA system terminals are not operated on a 24-hour-per-day basis, the terminals shall be physically secured when unattended.

8.104(5) The criminal justice agency administrator shall be directly responsible for ensuring that information received from the IOWA system is restricted for the official use of agency personnel, other criminal justice agencies, or other agencies authorized, in writing, by the department of public safety.

8.104(6) Any agency desiring direct access to IOWA system files shall make application to the department. Before authorization is granted, the administrator of the applying agency shall enter into a written agreement with the department of public safety agreeing to abide by all rules, policies and procedures promulgated by the department for system operation, security and discipline. The agreement shall reserve to the department the right to terminate furnishing criminal history or other file information to the applicant agency if abuses are discovered concerning either the security or dissemination requirements of this data.

8.104(7) Any agency which has had its authorization to IOWA system files terminated by the department may appeal the termination to the commissioner of public safety, in accordance with 661—Chapter 10.

661—8.105(80,692) Subpoenas and court orders. Any agency or individual in possession of criminal history data received from the department that is served with a subpoena, court order, request for production or other legal process demanding the production of criminal history data, shall notify the department in writing so that the department has an opportunity to make a timely resistance.

661—8.106 to **8.200** Reserved.

These rules are intended to implement Iowa Code sections 80.9 and 692.14.

DIVISION II
CRIMINAL INTELLIGENCE INFORMATION

661—8.201(692) Definitions.

8.201(1) *"Criminal intelligence file"* means stored information on:

a. 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 having involvement in criminal activities with known or suspected criminal offenders.

b. 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.

"Criminal intelligence file" does not include arrest data, conviction data, correctional data, criminal history data, criminal investigative data, disposition data, or surveillance data as defined in Iowa Code section 692.1.

8.201(2) *"Criminal intelligence system"* means any system of criminal intelligence files maintained and operated by a criminal justice agency in Iowa from which information is shared with any other agency. In addition to the criminal intelligence files, it includes any arrangements, equipment, facilities, and procedures used for the receipt, storage, submission, dissemination, or analysis of criminal intelligence files.

8.201(3) *"Need to know"* is established if criminal intelligence information will assist a recipient in anticipating, investigating, monitoring, or preventing possible criminal activity.

8.201(4) *"Reasonable grounds"* means information that establishes sufficient articulable facts that 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.

8.201(5) *"Right to know"* is established when a recipient of criminal intelligence information is a peace officer, a criminal justice agency, or a state or federal regulatory agency.

8.201(6) *"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.

8.201(7) *"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 for the purpose of protecting a person or property from the threat.

661—8.202(692) Iowa criminal intelligence system (ICIS). The Iowa Criminal Intelligence System (ICIS) is the system of criminal intelligence files maintained and operated by the intelligence bureau of the department of public safety, for the regular interagency exchange of information.

8.202(1) *Access.* The commissioner of public safety may authorize a peace officer, criminal justice agency, or state or federal regulatory agency to access ICIS provided that the authorized individual or agency follows approved procedures regarding receipt, maintenance, dissemination, submission and security of information, and related training. Authorization must be received in writing to be effective.

8.202(2) *Termination of authorization.* The commissioner of public safety may terminate authorization for access to ICIS which has been previously approved at any time for good cause. An individual or agency whose authorization to access ICIS has been terminated may appeal the termination in accordance with 661—Chapter 10. Notification of any termination of authorization for access to ICIS shall be provided to all agencies which operate criminal intelligence systems in Iowa.

8.202(3) *Reinstatement.* Any user whose authorization for access to ICIS 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.

8.202(4) *Applications.* To apply for access to ICIS or to obtain further information about ICIS, contact the Intelligence Bureau, Iowa Department of Public Safety, Wallace State Office Building, Des Moines, IA 50319, or by electronic mail via the Internet at intinfo@safe.ia.gov.

8.202(5) *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 ICIS unless such information directly relates to an investigation of criminal conduct or activity and there are reasonable grounds to believe that the subject of the information is, or may be, engaged in criminal conduct or activity.

8.202(6) *Entry of information—conformance with applicable law.* No information which has been obtained in violation of any applicable federal, state, or local law or ordinance, or these rules, may be entered into ICIS.

8.202(7) *Dissemination.* Criminal intelligence files from ICIS may be disseminated only to peace officers, criminal justice agencies, or state or federal regulatory agencies. Criminal intelligence files from ICIS may be disseminated only when there is a right to know and a need to know in the performance of a law enforcement activity. Criminal intelligence files from ICIS shall not be disseminated to any user whose authorization to access ICIS has been terminated and not reinstated.

EXCEPTION: Intelligence data may also be disseminated to any agency, organization, or person for an official purpose and in order to protect a person or property from the threat of imminent serious harm as defined in 8.201(7).

8.202(8) *Redissemination.* An agency, organization, or person receiving intelligence data from the department pursuant to Iowa Code chapter 692 as amended by 2003 Iowa Acts, House File 216, may redisseminate the intelligence data only if authorized by the agency or peace officer who originally provided the data and 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 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 as amended by 2003 Iowa Acts, House File 216, must maintain a list of the agencies, organizations, and persons receiving the intelligence data and the purpose of the redissemination.

661—8.203(692) Criminal intelligence systems.

8.203(1) *Notification.* Any agency which establishes a criminal intelligence system shall provide written notification of its establishment to the intelligence bureau, Iowa department of public safety, indicating the name, address, and telephone number of the agency operating the system and the identity and title of an employee of the agency responsible for the administration of the system.

8.203(2) *Identification of authorized users.* Any agency operating a criminal intelligence system shall establish policies and procedures for identifying authorized users of the system and for termination of such authorization for cause. Authorized users may be peace officers, criminal justice agencies, or state or federal regulatory agencies.

8.203(3) *Termination of authorization—notification of department.* Any agency operating a criminal intelligence system which terminates the authorization for access to that system of any user for cause shall notify the intelligence bureau of the Iowa department of public safety of the termination, including the identity of the user whose authorization has been terminated and the reasons for the termination.

8.203(4) *Restrictions on information entered.* Information about the political, religious, racial, or social views, associations, activities or sexual orientation of any individual shall not be entered into a criminal intelligence file unless such information directly relates to an investigation of criminal conduct or activity and there are reasonable grounds to believe that the subject of the information is, or may be, engaged in criminal conduct or activity.

8.203(5) *Information entered—conformance with applicable laws.* No information which has been obtained in violation of any applicable federal, state, or local law or ordinance, or these rules, may be entered into criminal intelligence files in any criminal intelligence system in Iowa.

8.203(6) *Dissemination.* Criminal intelligence files may be disseminated only to peace officers, criminal justice agencies, or state or federal regulatory agencies. Criminal intelligence files may be disseminated only when there is a right to know and a need to know in the performance of a law enforcement activity. Criminal intelligence files may not be disseminated from any criminal intelligence system in Iowa to any user whose authorization to access ICIS has been terminated and not reinstated, nor may any criminal intelligence system disseminate criminal intelligence files to any user whose authorization to access that system has been terminated and not reinstated.

EXCEPTION: Intelligence data may also be disseminated to any agency, organization, or person for an official purpose and in order to protect a person or property from the threat of imminent serious harm as defined in subrule 8.201(7).

8.203(7) *Redissemination.* An agency, organization, or person receiving intelligence data from a criminal or juvenile justice agency, state or federal regulatory agency, or peace officer pursuant to Iowa Code chapter 692 as amended by 2003 Iowa Acts, House File 216, may redisseminate the intelligence data only if authorized by the agency or peace officer who originally provided the data and the data is for an official purpose in connection with the prescribed duties of the recipient. If the agency, organization, or person receiving the data 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. A criminal or juvenile justice agency, state or federal regulatory agency, or peace officer 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 as amended by 2003 Iowa Acts, House File 216, must maintain a list of the agencies, organizations, and persons receiving the intelligence data and the purpose of the redissemination.

661—8.204(692) Criminal intelligence file security. The intelligence bureau of the department of public safety, other agencies operating criminal intelligence systems, and recipients of criminal intelligence files from criminal intelligence systems shall adopt administrative, technical, and physical safeguards, including audit trails, to ensure against unauthorized access and against intentional or unintentional damage. These safeguards shall include, but are not limited to, the following:

8.204(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.

8.204(2) Criminal intelligence files shall be labeled to indicate security level and identities of submitting agencies and submitting individual.

8.204(3) Where appropriate, effective and technologically advanced computer software and hardware designs shall be implemented to prevent unauthorized access.

8.204(4) Any access to criminal intelligence files and computing facilities in which they are stored shall be restricted to authorized personnel.

8.204(5) Criminal intelligence files shall be stored in such a manner that they cannot be modified, destroyed, accessed, purged, or overlaid in any fashion by unauthorized personnel.

8.204(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.

8.204(7) Access to any information required to gain authorized access to criminal intelligence files, including access codes and passwords, shall be restricted to only those personnel authorized to access these files. Agencies shall ensure that criminal intelligence files remain confidential when entering into specific agreements with individuals or organizations who provide computer or programming support to the agency.

8.204(8) Procedures shall be adopted to protect criminal intelligence files from unauthorized access, theft, sabotage, fire, flood, wind, or other natural or man-made disasters.

8.204(9) Procedures shall be adopted which establish the right of the agency receiving or having in its possession criminal intelligence files, to screen and, if appropriate, reject for employment any personnel who would, if hired, have access to criminal intelligence files.

8.204(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.

8.204(11) Any compromise, or suspected compromise, of information that would allow unauthorized access into criminal intelligence files shall be reported within 24 hours, excluding weekends and holidays, to the intelligence bureau of the department of public safety.

8.204(12) Any compromise, or suspected compromise, of information contained in criminal intelligence files shall be reported within 24 hours, excluding weekends and holidays, to the intelligence bureau of the department of public safety.

661—8.205(692) Review of criminal intelligence files—purge.

8.205(1) The intelligence bureau of the department of public safety, other agencies operating criminal intelligence systems, and recipients of criminal intelligence files from criminal intelligence systems shall regularly review the information in the criminal intelligence files for reclassification or purge. Decisions to retain, reclassify, or purge criminal intelligence files shall:

a. Ensure 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.

8.205(2) Information that is misleading, unreliable, or is no longer useful shall be purged or reclassified when necessary within 24 hours of the discovery that it is misleading, unreliable, or is no longer useful. Any person or agency to whom the criminal intelligence file was disseminated shall be notified of the reclassification or purge.

8.205(3) All information shall be reviewed within a five-year period of its submission to ensure compliance with subrule 8.205(1).

8.205(4) All information retained as a result of a review shall reflect the name of the reviewer, date of review, and explanation of decision to retain.

8.205(5) Information that is not retained in the criminal intelligence file after a review shall be destroyed by shredding, mulching, or burning.

661—8.206(692) Prohibition on surveillance data. No surveillance data shall be placed in files or manual or automated data storage systems maintained by any peace officer or criminal justice agency.

661—8.207(692) Subpoenas and court orders. Any agency or individual shall notify the department of public safety in writing within 24 hours, excluding weekends and holidays, 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.

661—8.208 to **8.300** Reserved.

These rules are intended to implement Iowa Code sections 692.8, 692.10, and 692.19.

DIVISION III
IOWA SEX OFFENDER REGISTRY
Rescinded IAB 2/16/05, effective 4/1/05; see 661—Ch 83

[Filed June 30, 1975]
[Filed 6/7/79, Notice 5/2/79—published 6/27/79, effective 8/2/79]
[Filed 1/10/86, Notice 11/20/85—published 1/29/86, effective 3/6/86]
[Filed 4/1/88, Notice 9/23/87—published 4/20/88, effective 5/25/88]
[Filed emergency 9/27/94—published 10/26/94, effective 10/1/94]
[Filed emergency 6/29/95—published 7/19/95, effective 7/1/95]
[Filed 7/26/95, Notice 3/1/95—published 8/16/95, effective 10/1/95]
[Filed 10/30/97, Notice 7/2/97—published 11/19/97, effective 1/1/98]
[Filed emergency 6/26/98—published 7/15/98, effective 7/1/98]
[Filed emergency 6/30/99—published 7/28/99, effective 7/1/99]
[Filed emergency 6/29/00—published 7/26/00, effective 7/1/00]
[Filed 2/22/01, Notice 7/26/00—published 3/21/01, effective 5/1/01]
[Filed emergency 4/30/01—published 5/30/01, effective 5/1/01]
[Filed emergency 6/5/02—published 6/26/02, effective 7/1/02]
[Filed emergency 4/24/03—published 5/14/03, effective 5/1/03]
[Filed emergency 7/13/04—published 8/4/04, effective 7/15/04]
[Filed 1/26/05, Notice 9/29/04—published 2/16/05, effective 4/1/05]