Red Tape Review Rule Report
(Due: September 1, 2026)

Department Name:	Public Safety	**Date:**	9/11/2025	**Total Rule Count:**	5
IAC #:	661	**Chapter/ SubChapter/ Rule(s):**	81	**Iowa Code Section Authorizing Rule:**	692.10
Contact Name:	Josie Wagler	**Email:**	wagler@dps.state.ia.us	**Phone:**	515-725-6185

PLEASE NOTE, THE BOXES BELOW WILL EXPAND AS YOU TYPE

What is the intended benefit of the rule?

The intended benefit of the rule is to ensure the security and confidentiality of all systems established for the exchange of intelligence data between criminal or juvenile justice agencies and provides for the authorization of officers or employees to access a system in which criminal intelligence information is stored.

Is the benefit being achieved? Please provide evidence.

Yes, the processes and procedures put in place pursuant to this rule ensure the security and confidentiality of all systems which house intelligence data. This rule also provides the method of authorization for certain individuals to be able to access this sensitive information. The Department has adopted several administrative, technical, and physical safeguards, including audit trails, to ensure against unauthorized access and against intentional or unintentional damage to the information system.

What are the costs incurred by the public to comply with the rule?

There are no costs to the public or to any law enforcement agency to comply with this rule.

What are the costs to the agency or any other agency to implement/enforce the rule?

There are no costs to the Department or any other agency to implement or enforce this rule.

Do the costs justify the benefits achieved? Please explain.

Yes, this chapter ensures security and confidentiality of sensitive criminal intelligence information is preserved and handled appropriately/in accordance with Iowa Code chapter 692.

Are there less restrictive alternatives to accomplish the benefit? ☐ YES ☒ NO

If YES, please list alternative(s) and provide analysis of less restrictive alternatives from other states, if applicable. If NO, please explain.

The Department has determined this to be the least restrictive method to accomplish the intended benefit of the rule.

Does this chapter/rule(s) contain language that is obsolete, outdated, inconsistent, redundant, or un-necessary language, including instances where rule language is duplicative of statutory language? [list chapter/rule number(s) that fall under any of the above categories]

PLEASE NOTE, THE BOXES BELOW WILL EXPAND AS YOU TYPE

81.2(10) was absorbed into 81.2(9).

RULES PROPOSED FOR REPEAL (list rule number[s]):

81.2(10)

RULES PROPOSED FOR RE-PROMULGATION (list rule number[s] or include rule text if available):

CHAPTER 81
CRIMINAL INTELLIGENCE INFORMATION

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

"Commissioner" means the commissioner of the department of public safety of their designee.

"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" is defined in Iowa Code 692.1(16). 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 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 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 may contact the Intelligence Bureau, Iowa Department of Public Safety, State Public Safety Headquarters Building, 215 East 7th Street, Des Moines, Iowa 50319, or by

email 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 will 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 will 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 and intelligence assessment.* An agency, organization, or person receiving intelligence data or an intelligence assessment from the department pursuant to Iowa Code chapter 692 may redisseminate the intelligence data or intelligence assessment only if authorized by the agency or peace officer who originally provided the data or assessment and if the data or assessment 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 or intelligence assessment. Any agency, organization, or person who redisseminates intelligence data or an intelligent assessment pursuant to Iowa Code chapter 692 must maintain a list of the agencies, organizations, and persons receiving the intelligence data or intelligence assessment and the purpose of the redissemination. Intelligence data and intelligence assessments must be maintained separately from and should not be included in any form in any investigative or prosecutorial files. 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 adopts 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 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 will be maintained until the information has been purged.

81.3(2) Criminal intelligence files will 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 will be implemented to prevent unauthorized access.

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

81.3(5) Criminal intelligence files will 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 will 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, will be restricted only to personnel authorized to access these files. The intelligence division will 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 will be adopted to protect criminal intelligence files from unauthorized access, theft, sabotage, fire, flood, wind, and natural or other disasters.

81.3(9) Procedures will be adopted establishing the right of the intelligence division to screen and reject for employment any personnel who would, if hired, have access to criminal intelligence files.

81.3(10) Procedures will be established allowing 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 will be reported without delay and, in any event, by the end of the next business day, to a supervisor within the intelligence division of the department of public safety.

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

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

81.4(1) The intelligence division regularly reviews the information in criminal intelligence files for reclassification or purging. Decisions to retain, reclassify, or purge criminal intelligence files will:

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 will be purged or reclassified, when necessary, without delay. Any person or agency to which the criminal intelligence file was disseminated will be notified of the reclassification or purge.

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

81.4(4) All information retained after a review will 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 will be deleted from the LEIN information system.

661—81.5(692) Subpoenas and court orders. Any agency or individual will notify the department 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.

For rules being re-promulgated with changes, you may attach a document with suggested changes.

METRICS

Total number of rules repealed:	**1**
Proposed word count reduction after repeal and/or re-promulgation	**184**
Proposed number of restrictive terms eliminated after repeal and/or re-promulgation	**26**

ARE THERE ANY STATUTORY CHANGES YOU WOULD RECOMMEND INCLUDING CODIFYING ANY RULES?

No.