☒ Division Order ☐ Special Order Order No.: **19-01** --- ☒ Procedure ☐ Plan ☒ Rule	**Iowa Department of Public Safety** **Division of Intelligence**	
	TITLE/SUBJECT: Intelligence Policy on Privacy, Civil Rights and Civil Liberties	**IDENTIFIER: 48-03.08**
	TO: All Division of Intelligence and Fusion Center (DOI/FC)	**CC:**
	RELATED DIRECTIVES/FORMS: DOM 04-03.03, *Information Sharing Guiding Principles*; DOM 23-01.03, *Criminal Intelligence*; DOM 23-01.04, *Intelligence Policy on Privacy, Civil Rights & Civil Liberties* (General Order)	
	APPLICABLE CALEA STANDARD(S): 42.1.6	
	EFFECTIVE DATE: 5-13-19	**REVISION #: 2**
	INSTRUCTIONS: A change has been made in section IV.A.1.h.	
	APPROVED BY: Kevin A. Winker	**DATE:** **April 29, 2019**

Table of Contents

I. Purpose

The purpose of this policy is to establish and maintain a criminal intelligence system within the Department to further the following purposes:

A. Increase public safety and improve national security;

B. Minimize the threat and risk of injury to specific individuals;

C. Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety or health;

D. Minimize the threat and risk of damage to real or personal property;

E. Protect individual privacy, civil rights, civil liberties, and other protected interests;

F. Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

G. Minimize reluctance of individuals or groups to use or cooperate with the justice system;

H. Support the role of the justice system in society;

I. Promote governmental legitimacy and accountability;

J. Not unduly burden the ongoing business of the justice system; and

K. Make the most effective use of public resources allocated to justice agencies.

II. Policy

A. This policy applies to all DPS personnel assigned to the Division of Intelligence and Fusion Center (DOI/FC).

B. All members of the Iowa Department of Public Safety, including the DOI/FC, and all participating agencies, employees and users will comply with all laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. In sharing or disclosing information, personnel will take reasonable measures to ensure that sources and methods of information gathering are adequately protected. Notice of pertinent written policies will be provided to Department and non-Department personnel who provide services. The existence of this policy will be a public record and information about the protection of privacy, civil rights, and civil liberties will be made available to the public on request and through any public Web site providing information about the system. The DOI/FC will maintain internal operating policies that ensure accountability and require personnel and authorized users to report violations or suspected violations of this policy to the Division's privacy officer. The Division will require compliance with all applicable laws protecting privacy, civil rights, and civil liberties, in the compliance with applicable laws in the collection, use, analysis, retention, destruction, sharing and disclosure of information in the system. All participating Division of Intelligence and Fusion Center personnel, personnel providing information technology services to the agency, private contractors, and users will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. This includes, but is not limited to, *Iowa Code* Chapters 22 and 692, and 28 C.F.R. Part 23. All internal policies governing the DOI/FC shall be consistent with these statutes, as well as the state and federal constitutions.

III. Definitions

A. *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, as provided in *Iowa Administrative Code* section 661-81.1.

B. *Criminal investigative data* - information collected in the course of an investigation where there are reasonable grounds to suspect that specific criminal acts have been committed by a person, as provided in *Iowa Code* section 692.1(6).

C. *Department* – the Iowa Department of Public Safety.

D. *Information* - includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.

E. *Intelligence assessment* - an analysis of information based in whole or in part upon intelligence data, as provided in *Iowa Code* section 692.1(13).

F. *Intelligence data* - information on identifiable individuals and associated criminal organizations, compiled in an effort to anticipate, prevent, or monitor possible criminal activity, as provided in *Iowa Code* section 692.1(14).

G. *LEIN information system* - means the Iowa Law Enforcement Intelligence Network. The (LEIN) information system is the statewide interjurisdictional intelligence system maintained and operated by the DOI/FC of the Department of Public Safety, for the regular interagency exchange of criminal intelligence files in compliance with 28 C.F.R. Part 23. Criminal intelligence files contained in the LEIN information system may be disseminated or redisseminated by the DOI/FCof the Department of Public Safety, as provided in *Iowa Code* chapter 692.

H. *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, as provided in *Iowa Administrative Code* section 661-81.1.

I. *Noncriminal identifying information* - means information about the characteristics and associations of an identifiable person suspected of being involved in criminal activity, as provided in *Iowa Administrative Code* section 661-81.1.

J. *Public* –

1. Includes:
    a) Any person and any for-profit or non-profit entity, organization or association;
    b) Any governmental entity for which there is no existing specific law or policy authorizing access to the Department's information;
    c) Media organizations; and
    d) Entities that seek or receive or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to nature or extent of those requesting information from the Department.
2. Does not include:
    a) Employees of the Department;

b) People or entities, private or governmental, who assist the Department in the operation of the justice information system; and

c) Public agencies whose authority to access information gathered and retained by the Department is specified in law.

d) Public or private entities of any type, whether for-profit or nonprofit, that are authorized by law and obtain requisite permission to receive information in bulk from the agency.

K. *Purge* - to remove or reclassify a record from an intelligence information system, either because the information is incorrect, inaccurate or incomplete, or because it has been provided by another agency and five years has passed since the information was updated.

L. *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 , as provided in *Iowa Administrative Code* section 661-81.1.

M. *Right to know* - is established when a recipient of criminal intelligence information is legally permitted to receive intelligence data or an intelligence assessment, as provided in *Iowa Administrative Code* section 661-81.1.

N. *Surveillance data* - 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, as provided in *Iowa Code* section 692.1(16) and *Iowa Administrative Code* section 661-81.1.

O. *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, as provided in *Iowa Administrative Code* section 661-81.1.

IV. Procedure

A. Overview of Division of Intelligence and Fusion Center

1. Information Systems

a) The DOI/FC is solely responsible and serves as custodian of record for the multi-jurisdictional criminal intelligence information system, which contains intelligence data. It also maintains a criminal intelligence system that is accessible only to authorized law enforcement personnel assigned to the DOI/FC to other authorized personnel employed in the Department. Information systems within the DOI/FC identify the user, and require acknowledgement of an information security policy before access is granted, and continued compliance with the policy when access is granted. A log is maintained to identify what information is accessed and disseminated, and an audit trail is maintained. Access to the system is denied when an employee separates from employment.

b) Chapter 661 of the *Iowa Administrative Code*, Section 81 sets out the standards governing the Department's criminal intelligence system. The administrative rules address collection, retention, dissemination, destruction and audit requirements that comply with the standards set out in 28 C.F.R. Part 23. The intelligence information

systems located within the DOI/FC are subject to continuous audit procedures, including automatic purging after 5 years and periodic audits that occur at least monthly. Policies and procedures within the DOI/FC specify requirements for physical security and personnel screening and require separation of duties; identification and authentication of users; authorization and access control procedure that is primarily Role-Based Access Control; data integrity measures designed to ensure continuous access to the system; and specification of firewalls, virtual private network access, and antivirus software. The information systems provide intrusion detection systems and security auditing, and are supplemented by personal audits that are documented. A disaster recovery and business continuity plan is in place. Guidelines have been set regarding data security, including removal of data from the physical premises of the DOI/FC, and access to Internet resources or other computer systems outside of the DOI/FC network.

c) Intelligence data kept in the intelligence information systems, by law and by policy, must have an articulated criminal or terrorism nexus. Access to intelligence data is, by law, limited to persons who are legally authorized to have the information and have an actual need to know. Individual access to the criminal intelligence system is limited to duly authorized personnel in the DOI/FC who have received a thorough background investigation and who have complied with policies and procedures established by the Department and the DOI/FC. Remote secure access to some portions of the criminal intelligence system is permitted to law enforcement personnel. All intelligence data contained in the multi-jurisdictional intelligence system complies with the provisions of 28 C.F.R. Part 23. The criminal intelligence system is designed so that a person who is authorized to access the system will only see those types of information to which the person is authorized to have access.

d) The criminal intelligence system within the DOI/FC was created and designed so that only information that satisfies designated criteria may be accepted and entered into the system, and so that activity related to the system is subject to various audit procedures. In addition, manual and computerized audit procedures are established to monitor compliance with legal and policy requirements and to review information contained within the system.

e) Authorized personnel within the DOI/FC also have access to other law enforcement sensitive information maintained by the Department, including the Iowa Online Warrants and Articles system, the Sex Offender Registry database, and certain investigative files maintained by Divisions within the Department. In addition, in conducting their duties, personnel within the Division of Intelligence and Fusion Center may be granted authority to access other information systems that are provided by other government or non-government agencies or organizations. Some of the sources are available to the public and some are available only to authorized law enforcement personnel. The collection and storage of information related to criminal investigation or criminal intelligence, regardless of the source, is in the criminal intelligence information system. The DOI/FC's criminal intelligence information system is designed to ensure that the sources and types of information are identified, the reliability and validity of the information is specified, the criminal nexus is articulated, and any restrictions regarding access or dissemination are specified.

f) Personnel within the DOI/FC also may access Uniform Crime Report data, which is maintained by the Program Services section of the Division of Administrative Services in the Department. This data is analyzed and published in a public-record document each year. Data from the Uniform Crime Report system is shared with other agencies or individuals who are authorized by law and policy to receive such information. Analysis of the UCR data may be provided to individual requesters, and fees may be charged, consistent with the provisions of Chapter 22, for complex analysis.

g) All personnel within the Division of Intelligence and Fusion Center who may have access to law enforcement sensitive or criminal intelligence information must successfully complete a thorough background investigation, similar to the background investigation for sworn law enforcement personnel. Personnel who have appropriate federal clearances are permitted access to secure information and secure areas, consistent with governing policies and procedures.

h) Breaches of security policy or breaches of restrictions on access to information may result in disciplinary action against employees who violate policy; restrictions on access to information or to physical space for non-employees who violate policy; and criminal prosecution for any person who violates standards regarding the dissemination or access to criminal intelligence information. Procedures are established for employees of the DOI/FC to report breaches of physical security to the Security Officer, or to report breaches of information security to the Systems Manager. Notifications provided to individuals who are the subject of a breach may be limited by state law if the data is classified as intelligence data, which is confidential by law except in very limited circumstances. To the extent that it is lawful, the Systems Manager will work with the Director and the Public Information Officer of the Department of Public Safety to ensure that individuals are notified regarding the breach, consistent with the processes established by the State of Iowa Department of Administrative Services. The State of Iowa standards established by the Iowa Department of Administrative Services are available online at http://secureonline.iowa.gov/links/index.html. If the originator or current custodian of the information is another agency, the System Manager will contact the other agency within 24 hours of the discovery of the breach.

2. Physical Space and Access

a) Physical access to the DOI/FC headquarters offices is restricted and includes physical security measures specific to the DOI/FC. Physical security includes electronic access that identifies the user, and policy restrictions regarding the use of personal identification to access the DOI/FC. Personnel who are granted unaccompanied physical access to the law enforcement portion of the DOI/FC must be authorized via background investigation equivalent to the requirements for sworn personnel within the Department. Authorized access into the Center requires an electronic access card that individually identifies the person, in addition to a biometric access system. Authorized access is limited to DOI/FC personnel and high level supervisors within the Department. After-hours access is restricted to DOI/FC personnel. Access to those portions of the offices in which intelligence and investigative analysis is conducted is restricted to law enforcement personnel, unless the visitor is escorted. Non-law-enforcement personnel who are housed in the DOI/FC are not granted

access, without an escort, to those areas in which intelligence and investigative analysis is conducted. Sections of the offices that house federally classified information are under the direction and control of authorized federal and state employees and are accessible only by authorized personnel, according to security policies and procedures established by the DOI/FC in conjunction with the federal agency.

b) The DOI/FC includes a physical area for non-law-enforcement partners. The non-law-enforcement personnel are not authorized to enter the law-enforcement areas of the DOI/FC without an escort, and non-law-enforcement personnel are not authorized to access the criminal intelligence systems operated and maintained by the DOI/FC. The non-law-enforcement personnel maintain a computer network separate from the computer network accessible to law enforcement personnel.

c) Federal partners who are co-located within the Division of Intelligence and Fusion Center access and maintain certain classified and unclassified information systems operated by their federal agencies. Only duly authorized DOI/FC personnel are permitted access to those systems. Only personnel with the required clearances are permitted to have access to classified information.

d) Secure space for the processing of classified information is located within the restricted-access portion of the DOI/FC. The secure area is monitored and all individuals who have access to the space, for any length of time, must comply with policies that ensure security and that protect the privacy of sensitive information.

3. Information Sharing

a) The DOI/FC is legally authorized to disseminate an intelligence assessment to non-law-enforcement personnel who have a genuine need to know. It is the policy of the DOI/FC that, in sharing information in an intelligence assessment, personal identifying information will be minimized to the extent possible, and law enforcement and intelligence sources and methods will be protected. In addition, instructions regarding the handling, storage and redissemination of an intelligence assessment will be provided as part of that intelligence assessment. The dissemination of criminal intelligence data and criminal investigative data will occur, to the extent feasible, using secure communication systems rather than open-Internet communication. The dissemination of federally classified information must comply with the standards applicable to the classification of such information.

b) The DOI/FC has adopted a Centralized Information Repository Model for the majority of information sharing among law enforcement agencies. In limited circumstances, a Joint Task Force Model or a Peer Group Model may be used, so long as the information is shared in a secure environment that fulfills the minimum requirements of the DOI/FC's information sharing policies. The DOI/FC participates in the Justice Interconnection Services Model as a member of the National Law Enforcement Telecommunications System and the Regional Information Sharing System, which meet the minimum requirements for information sharing by the DOI/FC.

c) The Division of Intelligence and Fusion Center coordinates and facilitates information sharing by governmental and non-governmental agencies and organizations, to the extent that such activities enhance the efforts to meet or avert

current, emerging and future public safety and homeland security threats. The coordination and facilitation does not necessarily require reliance on intelligence information systems, and intelligence data will be shared only in circumstances in which the recipient has a legal right to know and an actual need to know. The dissemination of intelligence assessments will occur, to the extent feasible, using secure communication systems rather than open-Internet communication.

d) Information collected or retained by the DOI/FC is not characterized based on citizenship, alienage, or residence status of the subjects of the information. Characterizations of information are based on distinctions between criminal intelligence data, criminal investigative data, and surveillance data, as defined under Iowa law. All persons are subject to the same standards with respect to the collection, retention, use and dissemination of criminal intelligence information and criminal investigative information. Surveillance data cannot be retained in any circumstance, regardless of citizenship, alienage or residence status.

e) Consistent with the requirements of the Information Sharing Environment Privacy Guidelines, the DOI/FC will develop, implement, maintain and review polices that enable authorized users of terrorism-related information to determine the nature of the protected information that the DOI/FC is making available in the Information Sharing Environment, so that participants can handle the information in accordance with legal requirements. This includes:

1) Basic descriptive information will be entered and associated with each record, data set or system of records containing personally identifiable information that will be accessed, used and disclosed, including: the name of the originating agency or component; the center system in which the information is maintained; the date the information was collected; and the title and contact information for the person to be contacted regarding the information;

2) The DOI/FC has established policies that require that products shared with others are saved in a Portable Document Format that minimizes metadata. The document itself is accompanied by a cover page that describes handling instructions, intended recipients and restrictions on dissemination or redissemination.

4. Privacy Officer and Privacy Team

a) The Director of the DOI/FC shall designate a trained privacy officer, who will coordinate the activity of the privacy team.

b) The privacy officer shall handle reported s and violation and, in addition, carry out the following duties:

1) Ensure that the DOI/FC's policies, procedures and systems are appropriately designed and executed in compliance with the Information Sharing Environment Privacy Guidelines;

2) Ensure that procedures are in place for regular review of the DOI/FC privacy policy in order to comply with legal requirements and other requirements set out in Information Sharing Environment Privacy Guidelines;

3) Maintain familiarity with the activities of the Division of Intelligence and Fusion

Center as they relate to the Information Sharing Environment;

4) Identify and address privacy and other legal issues arising out of the DOI/FC's participation in the Information Sharing Environment; and

5) Ensure that the appropriate personnel in the Department are trained in the Information Sharing Environment and the requirements of the Information Sharing Environment Privacy Guidelines.

c) The privacy officer shall designate other employees of the DOI/FC to be part of a privacy team, which will be responsible for the development and revision of the privacy policy, and for developing, modifying, and updating the written policies and procedures necessary to ensure compliance with the privacy policy. Privacy team members may be called upon to assist in the development, implementation, training, review and revision of the privacy policy of the DOI/FC. The privacy policy shall be reviewed at least annually to ensure compliance with governing state and federal statutory and constitutional law, and to ensure that other policies governing the operation of the DOI/FC are consistent with the privacy policy. The privacy team will ensure that the policies of the DOI/FC are consistent with the protection of privacy/civil rights/civil liberties interests of the public. The privacy team will be trained regarding Information Sharing Environment expectations, and will ensure that those expectations are reflected in the policies of the DOI/FC. The privacy team will provide input regarding the training of all employees of the Division of Intelligence and Fusion Center, the Department's information technology services employees, and any contractors who may have access to information within the DOI/FC.

d) The privacy officer shall be designated to receive and respond to inquiries or complaints regarding information collected, retained or disseminated by the Division of Intelligence, in coordination with the Public Information Officer in the Iowa Department of Public Safety. The process for seeking access to public and confidential records are set out in *Iowa Administrative Code* section 661-80.3 et seq. Complaints regarding the operation of intelligence data systems should be directed in writing to Director, Division of Intelligence, 215 East 7th Street, Des Moines, IA 50319, or emailed via intinfo@dps.state.ia.us.

B. SEEKING AND RETAINING INFORMATION

1. WHAT INFORMATION MAY BE SOUGHT OR RETAINED

a) The Department, consistent with 28 C.F.R. Part 23, will only seek or retain intelligence data in its LEIN Information System when there is reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity. If information originates from a non-law-enforcement source, it will be vetted by law enforcement personnel to determine the criminal or terrorism nexus of the behavior within 180 days. If a criminal or terrorism nexus is established, the information will be retained in the criminal intelligence system. If no criminal or terrorism nexus is established, the information will not be retained.

b) Surveillance data shall not be collected or retained in any criminal justice information

system maintained by the DOI/FC or the Department. The DOI/FC will not seek or retain information about an individual or organization solely on the basis of religious, political, or social views or activities; participation in a particular organization or event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

c) The DOI/FC will not seek or retain information about the political, religious, or social views; participation in a particular organization or event; or activities of any individual or his or her race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation unless such information is:

1) Relevant to whether an individual or organization has engaged in, is engaging in, or is planning a criminal (including terrorist) activity; or

2) Needed by the DOI/FC:

i) To identify an individual,

ii) In order for the DOI/FC to operate effectively, or

iii) To provide services to the individual or accommodate an individual's religious, ethnic, or cultural requests or obligations.

d) The DOI/DC will keep a record of the source of all information retained by the DOI/FC.

2. METHODS OF SEEKING INFORMATION

a) Information gathering and investigative techniques used by this Department will comply with *Iowa Code* Chapters 80 and 692, as well as accompanying administrative rules, and other state and federal statutory and constitutional laws.

b) Information gathering and investigative techniques used by the Department will be no more intrusive or broad scale than necessary in the particular circumstance to gather information it is authorized to seek or retain.

c) The DOI/FC will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernment information provider, who may or may not receive a fee or benefit for providing the information, if the DOI/FC knows or has reason to believe that:

1) The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the Division of Intelligence and Fusion Center unless such information was provided voluntarily;

2) The individual or information provider used methods for collecting the information that the Division of Intelligence and Fusion Center itself could not legally use if such actions are taken by a private individual on behalf of or as an agent of a peace officer, unless the information was used for impeachment of the accused person who testified;

3) The specific information sought from the individual or information provider could not legally be collected by the DOI/FC; or

4) The DOI/FC has not taken the steps necessary to be authorized to collect the information.

d) The DOI/FC shall not accept the following types of information:

1) Information that is inherently unreliable;

2) Information that was obtained as a result of unlawful or undue duress or coercion;

3) Information that was obtained in violation of the law.

3. CATEGORIZATION OF INFORMATION REGARDING VALIDITY AND RELIABILITY

a) At the time of retention in the system, the information will be categorized regarding its:

1) Content validity;

2) Nature of the source;

3) Source reliability;

4) Verifiability or accuracy;

5) Currency;

6) Completeness.

b) The categorization of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

4. CATEGORIZATION OF INFORMATION REGARDING LIMITATIONS ON ACCESS AND DISCLOSURE

a) At the time a decision is made to retain information it will be categorized pursuant to applicable limitations on access and sensitivity of disclosure in order to:

1) Protect confidential sources and police undercover techniques and methods;

2) Not interfere with or compromise pending criminal investigations;

3) Protect an individual's right of privacy and civil rights and civil liberties; and

4) Provide legally required protection based on the status of an individual as a child sexual abuse victim, a resident of a substance abuse treatment program, a resident of a mental health treatment program, or a resident of a domestic abuse shelter.

b) The categorization of existing information will be reevaluated whenever:

1) New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or

2) There is a change in the use of the information affecting access or disclosure limitations.

c) The access categories will be used to control:

1) What information a class of users can have access to;

2) What information a class of users can add, change, delete, or print; and

3) To whom the information can be disclosed, and under what circumstances.

C. INFORMATION QUALITY

1. The DOI/FC will make every reasonable effort to ensure that it complies with *Iowa Code* Chapter 692 and the applicable administrative rules, which restrict the collection, use, analysis, retention, destruction, sharing and disclosure of information to that information which has a criminal nexus and for which each recipient has both a right to know and a need to know, as well as any other regulations that apply to multijurisdictional intelligence databases, including 28 C.F.R. Part 23. The criminal intelligence system is designed so that submissions that fail to meet minimum standards will not be accepted for submission.
2. The DOI/FC will advise recipient agencies when information previously provided to them is deleted or changed when the requesting Department has specifically requested to be notified, or when the information has been sealed or deleted.
    a) The DOI/FC will make every reasonable effort to ensure that information sought or retained is:
        1) Derived from dependable and trustworthy sources of information;
        2) Accurate;
        3) Current;
        4) Complete, including the relevant context in which it was sought or received and other related information; and
        5) Merged with other information about the same individual or organization only when the applicable standard in section IV.C.2 has been met.
    b) The DOI/FC will make every reasonable effort to research suspected errors and deficiencies and to correct inaccurate data, and to assist other agencies in correcting inaccurate data that they have provided or that they have received from the DOI/FC.
    c) The DOI/FC will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete information in the system.
    d) The DOI/FC will make every reasonable effort to ensure that information will be deleted from the system when the DOI/FC learns that:
        1) The information is erroneous, misleading, obsolete, or otherwise unreliable;
        2) The source of the information did not have authority to gather the information or to provide the information to the DOI/FC; or
        3) The source of the information used prohibited means to gather the information unless such information was provided voluntarily.

D. COLLATION AND ANALYSIS OF INFORMATION

1. GENERAL PROCEDURE

    a) Information sought or received by the Department or from other sources will only be analyzed:
        1) By qualified individuals,
        2) To provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal or terrorist activities generally; and

3) To further crime (including terrorism) prevention, enforcement, force deployment, or prosecution objectives and priorities established by the Department.

b) Information sought or received by the Department or from other sources will not be analyzed or combined in a manner or for a purpose that violates section IV.A.1.b).

2. MERGING OF INFORMATION FROM DIFFERENT SOURCES

a) Information about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.

b) The set of identifying information sufficient to allow merging will consist of full name and one or more of the following: date of birth, fingerprints, law enforcement or corrections system identification number, usually based on fingerprints; photograph; physical description: height, weight, eye and hair color, race, ethnicity, tattoos, scars, etc.; Social Security Number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The information or characteristics that, in combination, could establish that information from two or more sources is, indeed, about the same organization may include the organization's name, federal or state tax ID number, office address, and telephone number.

c) If the matching requirements are not fully met but there is a strong partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

3. CONTRACTING WITH COMMERCIAL DATABASES

a) The Department will make every reasonable effort to monitor the information gathering techniques of commercial databases, including the commercial entity's practices in gathering personal information based on ruse or other misleading collection techniques, or based on unlawful information collection practices.

b) The Department will make every reasonable effort to contract only with commercial database entities that gather personal identifying information in a way that complies with local, state, tribal, territorial and federal law, and which is not based on misleading information collection practices.

E. SHARING AND DISCLOSURE OF INFORMATION

1. SHARING INFORMATION WITHIN THE DEPARTMENT AND WITH OTHER JUSTICE SYSTEM PARTNERS

a) Access to information gathered and retained by the Department will only be provided to persons within the Department or in other criminal justice or regulatory agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with the law and procedures applicable to the agency for which the information may be lawfully used. Access may be terminated for good cause, as set out in 661 I.A.C. 81.2(2)-(3). The person who received, reviewed, or added information to the system may be authorized to view the information he or she provided regardless of the type of access associated with

the information or the contributor's access authority.

b) The DOI/FC will establish, periodically review and train personnel regarding procedures for dissemination and redissemination of intelligence data and intelligence assessments. Procedures include the inclusion of specific handling instructions, standards for publication of documents and dissemination of information.

c) Access to the departmental intelligence system and to the multijurisdictional intelligence system is strictly limited to those personnel who are individually authorized to access the intelligence data contained in that system.

d) Only those personnel within the Division of Intelligence and Fusion Center who are authorized to access systems maintained by federal agency partners are permitted access, consistent with procedures established by the federal agency. Division of Intelligence and Fusion Center personnel must comply with any information sharing restrictions established by the federal agency, in conjunction with the DOI/FC.

e) The DOI/FC may share intelligence information with non-law-enforcement entities and individuals based only on the actual need to know. The DOI/FC will periodically review and train the DOI/FC personnel and non-law-enforcement partners about the standards established for information sharing. Information sharing may include information about potential criminal activity, or about events or activities that may have an impact on public order, such as public violence, crowd control or traffic control.

f) An audit trail will be kept of access by or dissemination of information to such persons.

2. SHARING INFORMATION WITH THOSE RESPONSIBLE FOR PUBLIC PROTECTION, PUBLIC SAFETY, OR PUBLIC HEALTH

a) Information gathered and retained by the Department may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures, consistent with *Iowa Code* Chapter 692. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.

b) An audit trail will be kept of the access by or dissemination of information to such persons.

3. SHARING INFORMATION FOR SPECIFIC PURPOSES

a) Information gathered and retained by the Department can be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.

b) The Department shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

c) An audit trail will be kept of the request for access and what information is

disseminated to such persons.

4. DISCLOSING INFORMATION TO THE PUBLIC

a) Information gathered and retained by this Department will be disclosed to a member of the public only as provided in *Iowa Code* Chapters 22 and 692.

b) Intelligence data is strictly regulated and remains confidential except in two limited circumstances:

1) intelligence data is disclosed as part of a sentencing hearing, or

2) intelligence data that is disclosed in an intelligence assessment.

c) Requests for information other than intelligence data must be addressed to the agency responsible for retaining and managing that information. Thus, for example, requests for peace officer investigative reports must be addressed to the investigating agency, and requests for criminal history data must be addressed to the Division of Criminal Investigation. Co-location of other agencies within the DOI/FC does not affect information-sharing practices that are restricted by law. If a request for such information is received, the DOI/FC will refer the requestor to the appropriate agency.

d) The Department shall not confirm the existence or nonexistence of intelligence data to any person or agency that would not be eligible to receive the information itself.

e) The DOI/FC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

f) An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

g) Fees may be charged, consistent with *Iowa Code* Chapter 22 and Departmental policies.

5. DISCLOSING INFORMATION TO THE INDIVIDUAL ABOUT WHOM INFORMATION HAS BEEN GATHERED

a) Information gathered and retained by the DOI/FC is intelligence data and dissemination of any intelligence data will comply with *Iowa Code* § 692.8A. Generally, intelligence data is protected from disclosure pursuant to *Iowa Code*, Chapters 22 and 692. If a person who is not authorized to receive intelligence data makes a request for information, the Department will deny the request, pursuant to the state and Departmental policies regarding disclosure of public records, as set out in *Iowa Code* Chapter 22 and Departmental Policy DOM 31-01.01, regarding public records requests. If necessary, the Department will seek a protective order from a court with jurisdiction to prohibit the unauthorized disclosure of intelligence data.

b) Iowa law permits disclosure of intelligence data in the limited circumstance of a sentencing proceeding or juvenile adjudication. The Department will comply with all provisions of *Iowa Code* section 692.8 regarding disputes about the accuracy of such information used in a sentencing proceeding or juvenile adjudication.

c) The Department may obtain information from criminal justice or other agencies that is designed for use in an ongoing investigation. The agency that provides investigative data or other, non-intelligence information is considered the custodian

of record. The submitting agency, rather than the Department, will be viewed as the custodian of the records, and the requester will be referred to the custodian of the record consistent with *Iowa Code* Chapter 22. The DOI/FC will coordinate and assist other agencies in handling complaints and correction requests, as appropriate. Any information that is retained by the DOI/FCis classified as intelligence data, which will be stored in the intelligence system, consistent with intelligence-system security and access policies as set out above.

d) The Department maintains a record of all requests for public information. The DOI/FC will maintain a record of all requests for intelligence data pursuant to *Iowa Code* § 692.8A, including requests for corrections or complaints. If any information is corrected, whether as a result of a complaint or for any other reason, the DOI/FC will notify anyone to whom the incorrect information was disseminated.

e) If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the Information Sharing Environment that (a) is held by the DOI/FC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from disclosure, the DOI/FC will inform the individual of the procedure for submitting (if needed) an resolving complaints or objections. All inquiries and complaints should be addressed to the DOI/FC privacy officer at the following address: Director, DOI/FC 215 East 7th Street, Des Moines, IA 50319, or intinfo@dps.state.ia.us.

f) The DOI/FC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure unless otherwise required by law. If the information did not originate with the DOI/FC, the DOI/FC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies or to verify that the record is accurate. Any personal information originating with the DOI/FC will be reviewed and corrected in or deleted from the DOI/FC data/records if it is determined to be erroneous, including incorrectly merged information, or if it is determined to be out of date. A record will be kept of all complaints or requests for corrections and the resulting action, if any.

g) To delineate protected information shared through the Information Sharing Environment from other data, the Division of Intelligence maintains records of agencies sharing terrorism-related information and audit logs and employs system mechanisms to identify the originating agency when the information is shared.

F. INFORMATION RETENTION AND DESTRUCTION

1. REVIEW OF INFORMATION REGARDING RETENTION

a) Information will be reviewed for purging in accordance with the governing administrative rules, which include provisions for review, retention, reclassification, purging; and documentation regarding review, as set out in 661 *Iowa Administrative Code* §81.4. Policies regarding review, retention, reclassification or purging of data in the multijurisdictional criminal intelligence database will comply with 28 C.F.R. Part 23.

b) When information has no further value or meets the criteria for removal under applicable law, it will be purged, destroyed, deleted, or returned to the submitting

source.

2. DESTRUCTION OF INFORMATION

a) The Department will delete information in accordance with the governing administrative rules, as set out in 661 *Iowa Administrative Code* §81.4.

b) Permission to destroy or return information or records will be obtained in accordance with the governing administrative rules, as set out in 661 *Iowa Administrative Code* §81.3(5) & (6).

c) Notification of proposed destruction or return of records will be provided in accordance with the governing administrative rules, as set out in 661 *Iowa Administrative Code* §81.4(2).

d) A record of what information has been purged or returned or reclassified shall be maintained by the Department.

e) Destruction of physical data requires shredding if it contains or reveals sensitive information. Destruction of electronic data will entail methods that reasonably assure that sensitive electronic data is not recoverable. Policies regarding the destruction of physical and electronic data will be reviewed and updated periodically and DOI/FCpersonnel will be trained on the policies.

f) Standard practices within the DOI/FC are consistent with the requirements set out in the *Iowa Administrative Code*. This includes standard practices regarding the shredding of hard copies of information, the review of proposed deletion of electronic information, and the procedures regarding destruction of electronic data storage media. Personnel within the DOI/FC do not maintain custody of evidence or original copies of investigative data. Copies of investigative data may be provided by the investigative officer to personnel within the DOI/FC for analysis, and those copies will be destroyed by shredding when the completed analysis is provided to the investigator who maintains the originals. Electronic information in the multi-jurisdictional database is automatically archived and made inaccessible 5 years after the reporting date, without notification to the originating agency or to the personnel in the DOI/FC. Other information may be deleted or modified, with review by the Systems Manager, and with appropriate notice to the originating agency or other agencies to which inaccurate information has been provided.

G. ACCOUNTABILITY AND ENFORCEMENT

1. INFORMATION SYSTEM TRANSPARENCY

a) The policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request and through any public web sites providing information about the system.

b) The Director of the DOI/FC will designate an employee of the Department to be responsible for receiving and responding to inquiries and complaints about privacy, civil rights and civil liberties protections in the information system and will provide to the Department's public information officer the contact information of the individual so designated.

c) The Director of the DOI/FC will designate a privacy team, whose duties will include review of DOI/FC policies related to privacy, civil rights and civil liberties. The

team will be trained regarding ISE information. Review of the DOI/FC policy will occur at least annually, and the privacy team will ensure that DOI/FC personnel and others have been trained on a regular basis regarding the DOI/FC policy and related topics.

2. ACCOUNTABILITY FOR ACTIVITIES

a) Primary responsibility for the operation of this justice information system, including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of information; and the enforcement of this policy is assigned to the Director of the DOI/FC.

b) The Department will establish procedures, practices, and system protocols, and use software, information technology tools, and physical security measures that protect information from unauthorized access, modification, theft, or sabotage, whether internal or external, and whether due to natural or human-caused disasters or intrusions. The Director of the DOI/FC will designate a DOI/FC employee to have primary responsibility for physical security. The designated employee will be trained in security procedures, and will ensure that personnel within the DOI/FC are trained. The Director of the DOI/FC will designate a DOI/FC employee to have primary responsibility for information systems security. The designated person will be trained in information-systems security procedures, and will ensure that personnel within the DOI/FC are trained. Information systems within the DOI/FC will operate within a secure electronic environment, and shall be located within a physically secure site that includes a secure building, a secure area within the building, locked doors and an alarm system.

c) Unlawful access, dissemination or redissemination of intelligence data can be prosecuted as a crime, according to *Iowa Code* § 692.8A. If a possible violation comes to the attention of the DOI/FC by any means, the Director of the DOI/FC will ensure that the matter has been referred to a prosecuting attorney, and will ensure that sworn personnel within the DOI/FC are made available to assist in the investigation upon request of the prosecuting attorney or the local law enforcement agency with jurisdiction, consistent with *Iowa Code* Chapter 80 and other state law.

d) If an employee of the Division of Intelligence and Fusion Center violates policy regarding access to intelligence data, that employee may be subject to disciplinary action, up to and including termination of employment, based on the employment provisions of that employee's union contract or State of Iowa administrative rules.

e) If an employee of the Department, who is not an employee of the DOI/FC, violates DOI/FC policy regarding access to intelligence data, that employee may be denied access to the criminal intelligence systems operated by the DOI/FC. The Director of the DOI/FC may refer the matter to the Department's Professional Standards Bureau for further action.

f) If there is reason to believe that an employee of a law enforcement agency has violated or is violating DOI/FC policy regarding the multijurisdictional criminal intelligence system, the Director of the DOI/FC will ensure that the matter is investigated. If it is determined that a violation has occurred, the employee of the law enforcement agency may be prohibited from obtaining access to the multijurisdictional criminal intelligence system. Action against the employing

agency may be taken if the DOI/FC Director determines that such action is warranted.

g) If there is reason to believe that an employee of a non-law-enforcement agency has violated or is violating DOI/FC policy regarding an intelligence assessment, the Director of the DOI/FC will ensure that the matter is investigated. If it is determined that a violation has occurred, the employee of the law enforcement agency may be prohibited from obtaining access to the multijurisdictional criminal intelligence system. Action against the employing agency may be taken if the DOI/FC Director determines that such action is warranted.

h) Other violations will be addressed in the DOI/FC security policy.

i) Complaints against Division of Intelligence and Fusion Center employees that are not related to the criminal intelligence system will be referred to the Professional Standards Bureau of the Department of Public Safety.

j) The Department will store information in a manner such that it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

k) The Department will require individuals authorized to use the system to agree in writing to comply with the provisions of this policy.

l) The Department will periodically conduct audits and inspections of information in the multijurisdictional criminal intelligence system. The audits will be conducted randomly by a designated representative of the Department or designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity and privacy of the Department's information.

m) The Department will review, at least annually, and update the provisions protecting privacy, civil rights, and civil liberties in its policies and make appropriate changes in response to changes in applicable law and public expectations.

3. ENFORCEMENT

Pursuant to Chapter 661 *Iowa Administrative Code* sections 81.2(2)-(3), if a user is suspected or found not to be complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, or disclosure of information, the Department will:

a) Suspend or discontinue access to information by the user;

b) Suspend, demote, transfer or terminate the person as permitted by applicable personnel policies;

c) Apply other sanctions or administrative actions as provided in Department personnel policies;

d) Request the agency, organization, contractor, or service provider employing the user to initiate proceedings to discipline the user or enforce the policy's provisions; or refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy as stated in section IV.A. Pursuant to 661 IAC section 81.2(4), authorization to access information may be reinstated if the problem which led to the termination has been corrected.

H. TRAINING

1. The Department will provide the following individuals training regarding the implementation of and the adherence to the intelligence-related privacy, civil rights, and civil liberties issues conveyed in this policy:

   a) All personnel assigned to the DOI/FC;

   b) Personnel providing information technology services to the Department;

   c) Staff in other public agencies or private contractors providing information technology services to the Department; and

   d) Users who are not employed by the Department or a contractor.

2. The training will cover:

   a) Purposes of the privacy, civil rights, and civil liberties protection policy;

   b) Substance and intent of the provisions of the policy relating to collecting, use, analysis, retention, destruction, sharing and disclosure of information retained by the Department;

   c) The impact of improper activities associated with information accessible within or through the Department; and

   d) The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

   e) The DOI/FC will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:

      1) Its personnel;

      2) Personnel providing information technology services to the agency;

      3) Staff in other public agencies or private contractors providing services to the agency; and

      4) Users who are not employed by the agency or a contractor.

   f) The training program will cover:

      1) Purposes of the privacy, civil rights, and civil liberties protection policy;

      2) Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the agency;

      3) The impact of improper activities associated with information accessible within or through the agency; and

      4) The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

I. PROVISIONS FOR A MULTIAGENCY AGREEMENT FOR AN INFORMATION SHARING SYSTEM

1. The goal of establishing and maintaining a justice information sharing system is to

further the following purposes:

a) Increase public safety and improve national security;

b) Minimize the threat and risk of injury to specific individuals;

c) Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health;

d) Minimize the threat and risk of damage to real or personal property;

e) Protect individual privacy, civil rights, civil liberties, and other protected interests;

f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;

h) Support the role of the justice system in society;

i) Promote governmental legitimacy and accountability;

j) Not unduly burden the ongoing business of the justice system; and

k) Make the most effective use of public resources allocated to justice agencies.

2. The DOI/FC may enter into an agreement with another agency to share information, so long as the policies and procedures permit information sharing in a way that is consistent with Iowa law.

3. The employees and users of the participating agencies and of the agency's information service providers will comply with all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information through the justice information sharing system.

4. Participating agencies will adopt internal policies and procedures requiring the participating agency, its personnel, contractors, and users to:

a) Only seek or retain information that is legally permissible for the agency to seek or retain under laws applicable to the agency;

b) Only use lawful means to seek information;

c) Only seek and retain information that is reliably accurate, current, and complete, including the complete, relevant context;

d) Take appropriate steps when merging information about an individual or organization from two or more sources to ensure that the information is about the same individual or organization;

e) Investigate in a timely manner any alleged errors and correct or delete information found to be erroneous;

f) Retain information sought or received only so long as it is relevant and timely, and delete or return information that is inaccurate, outdated, or otherwise no longer related to known or suspected criminal, including terrorist, activities;

g) Maintain information and systems containing information in a physically and electronically secure environment and protected from natural or man-made disasters

or intrusions;

h) Engage in collation and analysis of information in a manner that conforms to generally accepted practices;

i) Establish procedures that comply with the policies and procedures of the justice information sharing system for accessing information through the participating agency;

j) Only allow authorized users to access the information in the shared system and only for purposes related to the performance of their official duties;

k) Share information with authorized users of other justice system partners based only on a "right-to-know" and a "need-to-know" basis; and

l) Establish and comply with information retention and destruction schedules.

5. A participating agency will make information available in response to a query either by:

   a) Providing the requested information directly;

   b) Responding with the contact information of a person in the responding agency whom the individual making the query can contact;

   c) Having a person in the responding agency contact the individual making the query; or

   d) Indicating that no information is available.

6. The choice of approach as to any particular piece of information will be at the discretion of the agency that has retained the information.

7. A participating agency will not disclose information originating from another agency except as authorized or required by law in the jurisdiction in which the information originated, or provided for in this policy or in the operational policies of the shared information system. If disclosure of information is required, allowed or approved, then the disclosure is permitted.

8. When a participating agency gathers or receives information that suggests that information originating from another agency may be erroneous, may include incorrectly merged information, or lacks relevant context, the alleged error will be communicated in writing to the person designated in the originating agency to receive such alleged errors pursuant to Subsection IV.E.5.f).

9. Participating Agency Accountability and Enforcement

   a) Participating agencies will adopt and comply with internal policies and procedures requiring the agency, its personnel, contractors, and users to:

      1) Have and enforce policies for discovering and responding to violations of agency policies and this memorandum, including taking appropriate action when violations are found;

      2) Provide training to personnel authorized to use the justice information sharing network about the agency's requirements and policies regarding information collection, use, and disclosure;

3) Make available to the public the agency's internal policies and procedures regarding privacy, civil rights, and civil liberties;

4) Cooperate with periodic, random audits by representatives of the justice information sharing system; and

5) Designate an individual within the participating agency to receive reports of alleged errors in the information that originated from the participating agency.

b) If a participating agency fails to comply with the provisions of this agreement or fails to enforce provisions in its local policies and procedures regarding proper collection, use, retention, destruction, sharing, disclosure, or classification of information, the justice information sharing network may:

1) Suspend or discontinue access to shared information by a user in the offending agency who is not complying with the agreement or local policies and procedures;

2) Suspend or discontinue the offending agency's access to the justice information sharing system; or

3) Offer to provide an independent review, evaluation, or technical assistance to the participating agency to establish compliance.