Montana Analysis and Technical Information Center Policies and Procedures

Section:	INTELLIGENCE
Policy Number:	K-1
Policy Name:	MATIC PRIVACY POLICY
Effective Date:	9/23/08
Revised Date:	2010, 2015, 2018, 2019

I. PURPOSE

The mission of the Montana Analysis and Technical Information Center (MATIC) is to collect, store, analyze and disseminate information on public safety issues, including suspected offenses, to the law enforcement community and government officials regarding dangerous drugs, fraud, organized crime, terrorism and other criminal activity for the purposes of decision making, and proactive law enforcement while ensuring the rights and privacy of citizens.

This policy will help ensure that MATIC meets its mission.

II. POLICY APPLICABILITY AND LEGAL COMPLIANCE

A. All agencies and participating personnel will comply with the privacy policy, the Code of Federal Regulations (28 CFR 23), The Bank Secrecy Act (31 USC 5311, 31 CFR 103), the Administrative Rules of Montana (ARM) (23.12.301-23.12.305) and the Montana Code Annotated (MCA) (44-5-101 through 44-5-515), specifically concerning information the MATIC collects, receives, maintains, archives, accesses, or discloses. If an authorized user does not comply with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification or disclosure of information, the MATIC Supervisor will:

- Suspend or discontinue user access to the information;
- Suspend, demote, transfer or terminate the person, as permitted by applicable personnel policies;
- Apply administrative actions or sanctions as provided by the ARM or as provided in agency personnel policies;
- If the user is from an agency external to the center, request that the relevant agency, organization, contractor or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or

- Refer the matter to appropriate authorities for criminal prosecution, as applicable.

- Participating employees of the MATIC who perform an act forbidden by law may be charged with official misconduct, under MCA ~ 45-7-401.

B. The MATIC will provide training regarding the policy as part of new employee training and to participating personnel as part of the new intelligence system user training. This training will include implementation of and adherence to the privacy, civil rights and civil liberties policy. This training will be required for:

- All personnel assigned to the MATIC;

- Personnel providing information technology services to the MATIC;

- Staff in other public agencies and private contractors providing services to the agency;

- Users who apply for access to MATIC information.

The MATIC will provide training regarding the center's requirements and policies for the collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

C. The Policy will be posted on the MATIC web-portal and inserted into the Montana Division of Criminal Investigation Policy and Procedures Manual. Individuals with access to information maintained by MATIC will sign a Statement of Understanding. Agencies with access to information maintained by MATIC will sign a Memorandum of Understanding.

D. MATIC reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the center's privacy policy.

III. GOVERNANCE AND OVERSIGHT

A. The Montana Department of Justice, Division of Criminal Investigation has the primary responsibility for the operation of the MATIC, including:

- Coordination of personnel;

- The collection, receipt, retention and evaluation of information;

- The analysis, destruction, sharing or disclosure of such information.

B. Pursuant to the MCA ~ 44-5-501, the Attorney General will appoint an advisory council. The Attorney General, in conjunction with the Department of Justice and after

considering recommendations of the advisory council, shall adopt standards and procedures for the operation of the section. The standards and procedures must ensure compliance with this part by the section and must include safeguards of individual privacy rights. (MCA ~ 44-5-504)

- The advisory council will recommend the approval or denial of an agency to the Attorney General for participation in the MATIC. The advisory council will recommend the suspension of a participant agency for due cause and recommend, if appropriate, the reinstatement of a suspended participant agency. (MCA ~ 44-5-511)

- The advisory council will review and evaluate the implementation of safeguards of individual privacy rights. The council will also periodically inspect records relating to dissemination of information to determine whether they are in compliance with this part and with standards and procedures adopted by the section. The advisory council shall make an annual report to the attorney general.

IV. INFORMATION SECURITY AND SAFEGUARDS

A. The MATIC will operate in a secure facility protecting the facility from external intrusion. The MATIC will utilize secure internal and external safeguards against network intrusions. Access to MATIC databases from outside the facility will only be allowed over secure networks.

    - The MATIC 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.

    - Direct access to center's information will only be granted to center personnel whose positions and job duties require such access and who have successfully completed background checks and appropriate security clearances, if applicable, and have been selected, approved, and trained accordingly.

    - The MATIC will utilize watch logs to maintain records of requested and disseminated information.

B. In order to prevent inadvertent public disclosure, risk and vulnerability assessments will not be stored with publicly available data.

C. The MATIC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens the physical well-being, reputation, or finances of the person. The notice will be made promptly and without unreasonable delay following discovery of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the

integrity of any information system affected by this release, or the MATIC will follow the guidance set for the in OMB Memorandum M 07-16 (May 2007).

D. The MATIC Supervisor shall be designated and trained to serve as the MATIC Security Officer. The MATIC Supervisor may designate another employee to serve as Security Officer. The designee must receive Security Officer training prior to serving in this position.

V. INFORMATION GATHERING AND ACQUISITION

A. The MATIC and affiliated agencies will adhere to the following regulations and guidelines (in addition to those listed in paragraph II) when gathering information:

- The Organization for Economic Co-operation and Development's (OECD) Fair Information Practices (http://www.cdt.org/privacy/guide/basic/oecdguidelines.html.) Under certain circumstances, there may be exceptions to the Fair Information Practices, based, for example, on authorities provided in the Federal Privacy Act; state, local, and tribal laws; or agency policy;
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) national Criminal Intelligence Sharing Plan (NCISP).

B. The MATIC will only seek, retain, and share information to further the mission of the center. The MATIC will only utilize information that it is legally entitled to, including but not limited to criminal justice information (MCA ~ 44-5-13), public records and information available to the general public.

C. The MATIC will use the least intrusive techniques possible in the particular circumstance to gather information it is authorized to seek or retain.

D. Agencies participating in the MATIC or providing information to the center are subject to the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

E. The MATIC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

F. The MATIC will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernmental information provider who may or may not receive a fee or benefit for providing the information if the center knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information; or a source that used prohibited means to gather the information.

G. The MATIC will not collect or maintain information about the political, religious or social views, associations, or on the basis of race, ethnicity, citizenship, place of origin, age disability, gender, or sexual orientation or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

H. The MATIC will maintain a record of what information is sought, collected and disseminated from the center.

I. The information and intelligence collection practices of the MATIC are open to the public. The MATIC's privacy policy shall be available upon request.

J. The MATIC Supervisor or designee shall be the designated Privacy Officer for all matters and shall receive appropriate training. Acting in the role of the Privacy Officer the MATIC Supervisor will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights and civil liberties protections in the information system(s). The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies.

K. In the event an individual has a complaint the Privacy Officer can be contacted at: **Montana Analysis and Technical Information Center, PO Box 201417, Helena, MT 59620-1417** or **(406) 444-1330**.

L. All MATIC staff will adhere to the provisions outlined in the Privacy Policy. It will be the Privacy Officer's role to ensure the center follows the provisions.

VI. INFORMATION QUALITY ASSURANCE

A. The MATIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; that it is accurate, current, and complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable has been met.

B. At the time of retention in the system, the information will be labeled regarding its level of quality (verifiable and reliable). Information that is inaccurate, incomplete or not current will not be maintained. All information will be labeled to identify if the information has been verified and if the information is reliable. All information

will be reviewed by MATIC staff to ensure that all records retained by MATIC will be complete, accurate and current.

C. The MATIC will investigate, in a timely manner, alleged errors and deficiencies, and correct or delete, and refrain from using, protected information found to be erroneous or deficient.

D. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the center's confidence in the validity or reliability of retained information.

E. The MATIC will make every reasonable effort to ensure that information will be corrected or deleted from the system, and not used, when the center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable.

F. State, local and tribal agencies, including agencies participating in the information sharing environment, are responsible for the quality and accuracy of the data accessed by or shared with the center. Originating agencies providing data remain the owners of the data contributed. The MATIC will advise the appropriate data owner, in writing, if its data is found to be inaccurate, incomplete, out of date, or unverifiable.

G. The MATIC will use written or documented electronic notification to inform recipient agencies when information previously provided by the MATIC is deleted or changed by the center (for example, it is determined to be inaccurate or includes incorrectly merged information).

VII. INFORMATION RETENTION AND DESTRUCTION

A. The MATIC will collect or retain information that:

- Is based upon a criminal predicate or threat to public safety; or

- Is based upon 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, in the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity; or

- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or

- Is useful in a crime analysis or in the administration of criminal justice and public safety (including topical searches); and

- The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

B. Participants in MATIC, when contributing information, will review the information to identify and categorize the criminal activity the information refers to; the nature of the source; and the reliability of the source and the validity of the content.

C. When the information is received, it will be reviewed by MATIC staff for compliance with; Code of Federal Regulations (28 CFR 23); ARM (23.12.301-23.12.305) and MCA (44-5-501 thru 44-5-515). Information that is <u>not</u> compliant with these standards will be purged. If compliant, it will be placed in the central intelligence file (CrimeNTel).

D. All retained information about individuals, and to the extent expressly provided in this policy, to organizational entities, will be labeled by the contributor and reviewed by MATIC staff (by record, data set or system of records) pursuant to applicable limitations on access and sensitivity of disclosure in order to:

- Protect confidential sources, techniques and methods;
- Protect and preserve pending criminal investigations;
- Protect an individual's right to privacy, civil rights and liberties and;
- Provide legally required protection based on the individual's status as a youth, victim of sexual abuse, resident of a substance abuse treatment program, resident of a mental health treatment program or resident of a domestic abuse shelter.

E. All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23 and the ARM 23.12.303.

- When information has no further value or meets criteria for removal according to the MATIC's retention and destruction policy or according to applicable law, it will be purged and destroyed, or returned to the submitting source.
- The MATIC will delete information or return it to the source, unless it is validated, every five (5) years, as provided in 28 CFR Part 23 and the ARM 23.12.303.
- Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period.
- Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information and any agreement with the providing agency.

- A record of information to be reviewed for retention will be maintained by the MATIC, and for appropriate system(s).

F. The classification of existing information will be reevaluated whenever new information is added that affects access or disclosure limitations or there is a change in the use of the information affecting access or disclosure limitations.

G. MATIC requires certain basic descriptive information to be entered and electronically associated with data (or content) that is to be accessed, used, and disclosed, including:

- The name of the originating department, component, and subcomponent;
- The date the information was collected and the date its accuracy was last verified;
- The title and contact information for the person to who questions regarding the information should be directed.

H. The MATIC will label all information that will be accessed and disseminated to notify the accessing authorized user that the information is subject to state and federal laws restricting access, use or disclosure. The MATIC will apply specific labels and descriptive metadata to clearly indicate all legal restrictions on information sharing based on information sensitivity or classification.

I. Records 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. Information is not merged based on partial matches.

VIII. COLLATION AND ANALYSIS

A. In compliance with MCA ~ 44-5-503 the MATIC will provide both tactical and strategic intelligence reports. These reports will be completed by MATIC analytical staff. All staff members will have successfully completed a background check and a security clearance appropriate for the information they are dealing with at the center.

B. All analytical staff will receive baseline analytical training and ongoing professional education to ensure a quality analytical product.

C. MATIC staff will utilize all legal sources of information when completing an analytical product. Legal sources include but are not limited to those listed in Section VII, Part A. All products will be reviewed by the MATIC Supervisor or designee to ensure to protection of civil rights and civil liberties and the quality of the product.

D. The purpose of the products produced by the MATIC is to support the mission of the center.

IX. INFORMATION SHARING AND DISCLOSURE

A. Access to or disclosure of records retained by the MATIC will only be provided to persons within the MATIC or in other governmental agencies who are authorized to have access and have a legitimate law enforcement, public protection, public prosecution, public health or justice purpose. Additionally, such disclosure or access shall only be granted for the performance of official duties in accordance with law procedures applicable to the agency for which the person is employed. Records will be kept of access by or dissemination to such persons.

B. Information gathered and records retained by the MATIC will not be:

- Sold, published, exchanged, or disclosed for commercial purposes;
- Disclosed or published without prior notice and/or permission of the contributing agency;
- Disseminated to unauthorized persons.

C. Participating agencies may not disseminate information received from MATIC without approval from the originator of the information.

D. Information gathered and records retained by the MATIC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access, and only for purposes specified by law.

E. Credentialed secure access will be utilized to control:
- What information a class of user can have access to;
- What information a class of users can add, change, delete, or print; and
- To whom the information can be disclosed and under what circumstances.

F. The MATIC will maintain audit trail regarding access to information and the dissemination of information.

G. Information gathered and records retained by the MATIC may be accessed or disclosed to a member of the public ONLY if the information is defined by law to be public record or otherwise appropriate for release to further the agency mission. Such information may only be disclosed in accordance with applicable law and records will be kept of all requests for information and what information is released to a member of the public.

H. There are several categories of records that will ordinarily not be provided to the public and/or an individual about whom information has been gathered:

- Criminal investigative information and criminal intelligence information. MCA ~ 44-5-303. However certain law enforcement records must be made available for inspection and copying under MCA ~ 44-5-301.

- Information that is constitutionally protected from disclosure i.e., information in which there is an individual privacy interest that clearly exceeds the merits of public disclosure, and matters related to individual or public safety. MCA ~ 2-6-102.

I. Pursuant to MCA ~ 2-6-102 a record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure. This includes:

- A record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism;

- Vulnerability assessments, risk planning documents, needs assessments, and threat assessments;

- Protected federal, state, local, or tribal records, which may include records owned or controlled by another agency.

J. The MATIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive such information.

K. The MATIC will comply with court orders for dissemination issued in compliance with MCA ~ 44-5-303. Records of all such orders and information disclosed shall be kept.

X. COMPLAINTS AND CORRECTIONS

A. If an individual makes a complaint or objection to the accuracy or completeness of information retained about him or her within a system under the MATIC's control, the MATIC will inform the individual of the procedure for submitting complaints or requesting corrections. Upon receipt of a complaint or request for correction regarding information that has been disclosed, the MATIC will consent to the correction, remove the record, or state a basis for the denial of the complaint or request. A record will be kept of all complaints and request for corrections. Complaints will be received by the MATIC's Privacy Officer at: **Montana Analysis and Technical Information Center, PO Box 201417, Helena, MT 59620-1417** or **(406) 444-1330**.

B. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that is exempt from disclosure, (a) Has been or may be shared through the ISE, (b) Is held by the MATIC and (1) Allegedly has resulted in demonstrable (2) harm to the complainant,

The MATIC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the MATIC's Privacy Officer at: **Montana Analysis and Technical Information Center, PO Box 201417, Helena, MT 59620-1417** or **(406) 444-1330**. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the MATIC, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate.

C. All information held by the MATIC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the MATIC will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

D. If an individual makes a complaint or objection regarding the accuracy or completeness of information about him or her that originates with another agency and has been disclosed to the individual, the MATIC Supervisor will notify the originating agency of the complaint or correction request and coordinate with them to ensure that the individual is provided with complaint submission or correction procedures. Upon receipt of a complaint or request for correction, the originating agency will consent to the correction, remove the record, or state a basis for the denial of the complaint or request. A record will be kept of all complaints and correction requests.

E. In the event an individual wants to appeal the decision of the Privacy Officer, the complainant can contact the Administrator of the Division of Criminal Investigation. The Administrator will review the complaint and the suggested action of the Privacy Officer. The Administrator of the Division of Criminal Investigation can be reached at: **Administrator, Montana Division of Criminal Investigation, P.O. Box 201417, Helena, MT 59620-1417.**

F. The sources of all information received by the MATIC are identified to help ensure accountability and accuracy of the information.

XI. SYSTEMS ACCOUNTABILITY

A. Queries made to the MATIC data applications will be logged into the data system identifying to the user initiating the query.

B. The MATIC watch log will be utilized to maintain a record of requested or disseminated information.

C. The MATIC will provide a copy of this policy to all agency and non-agency personnel who provide services and will require written acknowledgement of receipt of this policy and agreement of compliance with the provisions of this policy.

D. The MATIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems. These audits will occur yearly, and a record of the audit will be maintained by the supervisor (or designee) of the center. The results of the audit will be reported to the Attorney General.

E. The MATIC's personnel or other authorized users will report violations or suspected violations of center policies relating to protected information to the MATIC Supervisor.

F. The MATIC Supervisor will periodically review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy and make appropriate modifications in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

Terms and Definitions

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. For data access, access is usually specified as read-only access and read/write access. With regard to the Information Sharing Environment (ISE), access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Center—Center refers to the MATIC and all participating agencies of the MATIC.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Civil Liberties—Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data—Inert symbols, signs, or measures.

Disclosure—The release, transfer, provision of access to, or divulging of personally identifiable information in any other manner—electronic, verbal, or in writing—to an individual, agency, or organization outside of the agency who collected it. Disclosure is a subset of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. The eight FIPs are:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, tips and leads data, and criminal intelligence data.

Information Quality—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Law—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Logs—Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and only authorized individuals are getting access to the data. See also Audit Trail.

MATIC – Montana Analysis and Technical Information Center

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular content. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based upon the type of information and context of use.

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Privacy—Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Protected Information—For the non-intelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to

information privacy or other legal protections under the Constitution and laws of the United States. For state, local, and tribal governments, it would include applicable state and tribal constitutions and State, Local and Tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's information;
- Media organizations; and
- Entities that seek, 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 the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency;
- People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency is specified in law.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress—Internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

Retention—Refer to "Storage."

Right to Privacy—The possible right to be left alone, in the absence of some reasonable public interest in a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

Security—Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.