Arkansas State Fusion Center

Privacy Policy Version 2.1

March 2018

The Arkansas State Fusion Center Privacy Policy, Version 2.1, represents the privacy policy applicable to all ASFC operations and activities.

Table of Contents

A. PURPOSE

1. The mission of the Arkansas State Fusion Center (ASFC) is to provide an integrated, multi-discipline, information sharing network to collect, analyze, and disseminate information regarding criminal and terrorist activity to stakeholders in a timely manner in order to protect the citizens and the critical infrastructure of Arkansas, while following appropriate privacy, civil rights, and civil liberties safeguards as outlined in the principles of the Organization for Economic Co-operation and Development's (OECD) Fair Information Principles to ensure that the information privacy and other legal rights of individuals and organizations are protected (See definitions of "Fair Information Principles" and "Protected Information" in Appendix A, Terms and Definitions, of this policy).

2. The information and intelligence data collected, evaluated, and analyzed will be disseminated by the ASFC to members of the law enforcement, public safety and pertinent first responder communities responsible for the prevention, mitigation, and response to crime, terrorism, natural and manmade disasters.

3. The ASFC recognizes the importance of ensuring the protection of individual, civil liberties, civil rights, and privacy interests throughout the intelligence process and will ensure compliance with this policy and applicable laws and regulations as they apply to the State of Arkansas.

4. The ASFC Operations Manual contains the standards the ASFC will adhere to for the collection, use, and security of intelligence and information, as well as accountability guidelines for the management of such intelligence or information.

B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

1. All ASFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with the ASFC's privacy policy concerning the information the ASFC collects, receives, maintains, archives, accesses, or discloses to agency/ASFC personnel, governmental agencies (including Information Sharing Environment (ISE) participating agencies), and participating justice and public safety agencies, as well as to private contractors and the general public.

2. The ASFC will provide a printed copy of this policy including all applicable updates to all ASFC and non-ASFC personnel who provide services to the ASFC and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

3. All ASFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, agencies that originate information, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to those listed in Appendices B and C.

4. The ASFC has adopted internal operating procedures that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to those listed in Appendices B and C.

C. GOVERNANCE AND OVERSIGHT

1. Primary responsibility for the operation of the ASFC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, or disclosure of information; and the enforcement of this policy is assigned to the Administrator/Director of the ASFC.

2. The ASFC is governed by the ASFC Executive Committee that liaises with the community to ensure that privacy and civil rights are protected as provided in this policy and by the ASFC's information gathering and collection, retention, and dissemination processes and procedures. The committee will approve the ASFC Privacy Policy, will provide oversight to the Policy, and will annually review and update the Policy in response to changes in law and implementation experience, including the results of audits and inspections.

3. The ASFC's privacy compliance is guided by a trained Privacy Officer who is either the Director or an individual appointed by the Director of the ASFC and who receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates compliant resolution under the ASFC's redress policy, and who is the liaison for the ISE, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following: arfusioncenter@asp.arkansas.gov, to the attention of the ASFC Privacy Officer.

4. The Privacy Officer ensures that enforcement procedures and sanctions outlined in Section N.3, Enforcement, are adequate and enforced.

5. The ASFC employees, contract employees and persons on assignment to the ASFC, from other agencies, are responsible for adhering to this policy. Failure to abide by this policy may result in, denied access, disciplinary action up to and including dismissal.

D. DEFINITIONS

The primary terms and definitions used in this privacy policy are set forth in Appendix A-Definitions

E. INFORMATION

1. The ASFC will seek or retain information that:
   - Is based on a criminal predicate or possible threat to public safety; or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that 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 source of the information is reliable and verifiable or limitations on the quality of the information are identified; and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.
   - The ASFC may retain information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in Section E.7.

2. The ASFC will not seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

3. The ASFC applies labels to agency-originated protected information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:
   - The information is "protected information," to include "personal data" on any individual (see Appendix A, Definitions) and, to the extent expressly provided in this policy, includes organizational entities.
   - The information is subject to Federal and Arkansas state laws restricting access, use, or disclosure, including, but not limited to, 18 USC 2721, et seq., A.C.A. § 12-12-1001 *et seq*., A.C.A. § 16-90-903, A.C.A. § 25-19-101 *et seq*.

4. The ASFC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency will assign categories to the information) to reflect the assessment, such as:
   - Whether the information consists of tips and leads data, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, or case progress, etc.;

- The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector);
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:
    - Protect confidential sources and police undercover techniques and methods;
    - Not interfere with or compromise pending criminal investigations;
    - Protect an individual's right of privacy, civil rights, and civil liberties; and
    - Provide legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The classification of existing information will be re-evaluated whenever:
    - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
    - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. ASFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. ASFC personnel will:
    - Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The ASFC will use a standard reporting format and data collection codes for SAR information.
    - Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
    - Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).

- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Information will be retained for three years in accordance with the Arkansas General Records Retention Schedule allowing analysts to work a tip or lead or SAR information to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the agency's/ASFC's physical, administrative, and technical security measures that are in place for the protection and security of tips, leads and SAR information. Tips, leads, and SAR information will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

8. The ASFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil liberties, and civil rights.

9. The ASFC will identify and review protected information that is originated by the ASFC prior to sharing that information in the ISE. Further, the ASFC will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The ASFC requires certain basic descriptive information to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information should include:
    - The name of the originating department, component, and subcomponent.
    - The name of the agency's justice information system from which the information is disseminated.
    - The date the information was collected and, where feasible, the date its accuracy was last verified.
    - The title and contact information for the person to whom questions regarding the information should be directed.

11. The ASFC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

12. The ASFC will keep a record of the source of all information retained by the agency.

F. ACQUIRING AND RECEIVING INFORMATION

1. Information gathering (acquisition and access) and research techniques used by the ASFC and information-originating agencies are in compliance with and will adhere to applicable regulations and guidelines, including, but not limited to:

    - 28 CFR Part 23 regarding criminal intelligence information.
    - Organization for Economic Co-operation and Development's (OECD) *Fair Information Principles* (under certain circumstances, there may be exceptions to the *Fair Information Principles*, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal laws; or agency/ASFC policy).
    - Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
    - Applicable constitutional provisions, A.C.A. § § 12-12-1001 *et seq*. and any applicable administrative rules, as well as any other regulations that apply to multijurisdictional intelligence databases.

2. The ASFC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and ASFC personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The ASFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in behaviors that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights and civil liberties (e.g., race, culture, religion, or political associations) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. Information gathering and research techniques used by the ASFC will (and for originating agencies should) be the least intrusive and lawful means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access and share information with the ASFC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

6. The ASFC 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 collection practices.

7. The ASFC will not directly or indirectly receive, seek, accept, or retain information from:
    - An individual or nongovernmental entity who may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or ASFC policy.; or
    - An individual or information provider that is legally prohibited from obtaining or disclosing the information.

G. INFORMATION QUALITY ASSURANCE

1. The ASFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; 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 standard [Refer to Section I. Merging Records] has been met.

2. At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable).

3. The ASFC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

4. The labeling of retained information will be reevaluated when new information is gathered that has an impact on the confidence (validity and reliability) in previously retained information.

5. The ASFC will conduct periodic data quality reviews of information it originates and will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the ASFC learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the ASFC did not have authority to gather the information or to provide the information to another agency; or the ASFC discovers that prohibited means were used to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

6. Originating agencies external to the ASFC are responsible for the quality and accuracy of the data accessed by or provided to the ASFC. The ASFC will advise the appropriate contact person in the originating agency, in writing, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

7. The ASFC will use written or documented electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the ASFC because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. COLLATION AND ANALYSIS

1. Information acquired or received by the ASFC or accessed from other sources will be analyzed only by qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

2. Information subject to collation and analysis is information as defined and identified in Section E, Information.

3. Information acquired or received by the ASFC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
    - Further crime prevention (including terrorism), enforcement, force deployment, public safety or prosecution objectives and priorities established by the ASFC.
    - 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 (including terrorist) activities.

4. The ASFC requires that all analytical products be reviewed and approved by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the ASFC.

I. MERGING RECORDS

1. The set of identifying information sufficient to allow merging by the ASFC will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

2. If the matching requirements are not fully met but there is an identified 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.

J. SHARING AND DISCLOSURE

1. Credentialed, role-based access criteria will be used, as appropriate, to control:
   - The information to which a particular group or class of users can have access based on the group or class;
   - The information a class of users can add, change, delete, or print; and
   - To whom, individually, the information can be disclosed and under what circumstances.

2. The ASFC will adhere to the current version of the ISE-SAR Functional Standard for the suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process within the ISE that complies with the current version of the ISE-SAR Functional Standard.

3. Access to or disclosure of records retained in ASFC databases will be provided only to persons within the ASFC or in other governmental agencies or private sector entities 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 law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed the information retained by the ASFC and the nature of the information accessed will be kept by the ASFC.

4. Agencies external to the ASFC may not disseminate protected information received from ASFC without approval from the originator of the information. This requirement does not apply to information that was already provided to or disclosed to, or independently acquired by, the ASFC without restrictions from its originating source and disseminated to agencies external to the ASFC by the ASFC.

5. Records retained in ASFC databases may be accessed or disseminated to those responsible for public protection, safety, or public health only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the ASFC and the nature of the information accessed will be kept by the ASFC.

6. Information gathered and records retained by the ASFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail will be kept for a minimum of three (3) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

7. Information gathered and records retained by the ASFC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the ASFC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the laws of the State of Arkansas for this type of information. An audit trail sufficient to allow the identification of each member of the public who accessed or received information retained by the ASFC and the nature of the information accessed will be kept by the ASFC.

8. Information gathered and records retained by the ASFC will not be:
   - Sold, published, exchanged, or disclosed for commercial purposes;
   - Disclosed or published without prior notice to the originating agency that such information is subject to re-disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency; or
   - Disseminated to persons not authorized to access or use the information.

   Records required to be kept confidential by law are exempted from disclosure requirements under the Arkansas Freedom of Information Act, A.C.A. § 25-19-105(b). Undisclosed investigations by law enforcement agencies of suspected criminal activity are exempted from disclosure under A.C.A. § 25-19-105(b)(6).

9. Subject only to the requirement of ASFC to comply with the Arkansas Freedom of Information Act or other applicable law, the ASFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.

K. REDRESS

K.1 Disclosure

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in K.1 (2), below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the ASFC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The ASFC response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

2. Pursuant to the ASFC's lawful discretion, the existence, content, and source of the information will not be made available to an individual unless required under the Arkansas Freedom of Information Act or other law.

K.2 Complaints and Corrections

1. The Arkansas State Fusion Center does not have any legislation specific to complaints and corrections of information. The ASFC will refer all complaints of accuracy to the originating agency of the data. The Privacy Officer will facilitate the request and audit the information housed in ASFC to ensure changes are applied to the ASFC databases as required. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

2. If an individual has complaints or objections to the accuracy or completeness of information about him or her that ***originates with another agency***, including information that is shared through the ISE, the ASFC's privacy officer or designee will notify the originating agency of the complaint or request for correction and coordinate with the originating agency to assist the individual with complaint and corrections procedures. A record will be kept of all such complaints and requests for corrections and the resulting action taken, if any.

3. If an individual has a complaint or objection with regard to the accuracy or completeness of terrorism-related protected information that:
   (a) is exempt from disclosure;
   (b) has been or may be shared through the ISE,
      (1) is held by the ASFC; and
      (2) allegedly resulted in demonstrable harm to the complainant,
   The ASFC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints should be directed to the ASFC Privacy officer at the following e-mail address: arfusioncenter@asp.arkansas.gov, to the attention of the ASFC Privacy Officer. The ASFC 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 ASFC, the ASFC Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct or purge any identified data/record deficiencies, subject to applicable records retention procedures (as discussed in Section M. of this policy), or to verify that the record is accurate. All information held by the ASFC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected or deleted from ASFC data/records according to applicable records retention procedures if it is determined to be erroneous, include incorrectly merged information, or out of date. If there is no resolution within 30 days, the ASFC will not share the information until such time as the complaint has been resolved. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

4. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for correction(s) are denied by the ASFC or originating agency, including ISE participating agencies. The individual will also be informed of the procedure for appeal when the ASFC or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

5. To delineate protected information shared through the ISE from other data, the ASFC 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.

L. SECURITY SAFEGUARDS

1. The ASFC Administrator/Director is the assigned, designated and trained ASFC Security Officer.

2. The ASFC will operate in a secure facility protecting the facility from external intrusion. The ASFC will utilize secure internal and external safeguards against network intrusions. Access to ASFC databases from outside the facility will be allowed only over secure networks.
3. The ASFC will secure tips, leads, and SAR information in a separate repository system that is the same as or similar to the system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

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

5. The ASFC will utilize watch logs to maintain audit trails of requested and disseminated information.

6. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

7. The ASFC 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.

8. Access to ASFC information will be granted only to ASFC personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

9. The ASFC 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 physical, reputation, or financial harm to the person in accordance with Ark. Code Ann. § 4-110-101 *et seq*. The notice will be made promptly and without unreasonable delay following discovery or notification 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.

M. INFORMATION RETENTION AND DESTRUCTION

1. 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.

2. When information has no further value or meets the criteria for removal according to the ASFC's retention and destruction policy or according to A.C.A. § 25-18-601 *et seq*., it will be purged, destroyed, and deleted or returned to the submitting source.

3. The ASFC will delete information or return it to the source once its retention period has expired unless it is validated, as specified in 28 CFR Part 23.

4. The procedure contained in the Arkansas General Records Retention Schedule or any other rule promulgated by the Department of Finance and Administration with respect to records retention will be followed for notification of appropriate parties before information is destroyed or returned.

5. Notification of proposed destruction or return of records may or may not be provided to the source agency, depending on the relevance of the information and any agreement with the providing agency.

6. A record of information to be reviewed for retention will be maintained by the ASFC and, for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

N. ACCOUNTABILITY AND ENFORCEMENT

N.1 Information System Transparency

The ASFC will be open with the public in regard to information and intelligence collection practices. The ASFC privacy policy will be provided to the public for review, made available upon request made to the following e-mail address: arfusioncenter@asp.arkansas.gov, to the attention of the ASFC Privacy Officer and posted online at: http://www.nfcausa.org

1. The designated Privacy Officer 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 can be contacted at the following email address: arfusioncenter@asp.arkansas.gov, to the attention of the ASFC Privacy Officer.

N.2 Accountability

1. The audit log of queries made to the ASFC will identify the user initiating the query.

2. The ASFC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of three (3) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

3. The ASFC 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, so as to not establish a pattern of the audits. These audits will be mandated at least quarterly, and a record of the audits will be maintained by the ASFC Administrator/Director.

4. ASFC personnel, or other authorized users, shall report errors and suspected or confirmed violations of agency/ASFC policies relating to protected information to the ASFC Privacy Officer (as described in Section C. 3).

5. The ASFC will annually conduct an audit and inspection of the information contained in its criminal intelligence system. The audit will be conducted by a designated independent panel. This independent panel has the option of conducting a random audit, without announcement, at any time and without prior notice to the ASFC. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the agency's/ASFC's criminal intelligence system.

6. The ASFC Executive Committee, guided by an appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

N.3 Enforcement

1. If an authorized user is found to be in noncompliance with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the Administrator/Director of the ASFC will:
    - Suspend or discontinue access to information by the user;
    - Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
    - Apply administrative actions or sanctions as provided by state police rules and regulations or as provided in agency/ASFC personnel policies;
    - If the user is from an agency external to the agency, 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 necessary, to effectuate the purposes of the policy.
    - The ASFC reserves the right to restrict the qualifications and number of personnel having access to ASFC information and to suspend or withhold service personnel that are found in violation of the privacy policy. The ASFC reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of the ASFC'S privacy policy.

O. TRAINING

1. The ASFC will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:
    - All assigned personnel of the ASFC;
    - Personnel providing information technology services to the ASFC;
    - Staff in other public agencies or private contractors providing services to the agency; and,
    - Associated users who are not employed by the ASFC or a contractor.
    - Person(s) that are participating with the ASFC as part of the Homeland Security Liaison Officer (HSLO) program.

2. The ASFC will provide special training to personnel authorized to share protected information through the ISE regarding the ASFC requirements and policies for collection, use, and disclosure of protected information.

3. The ASFC privacy policy training program will cover:
    - Purposes of the privacy, civil rights, and civil liberties protection policy;
    - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the ASFC;
    - How to implement the policy in the day-to-day work of the user, whether a paper or systems user;

- The impact of improper activities associated with infractions within or through the agency;
- Mechanisms for reporting violations of agency/ASFC privacy-protection policies; and the nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.
- Originating and participating agency responsibilities and obligations under applicable policies or memorandums of understanding (MOU).

APPENDIX A -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. Data access is usually specified as read-only and read/write access.

With regard to the 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.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition - The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports, or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency -Agency refers to the Arkansas State Fusion Center and all agencies that access, contribute, and share information in the Arkansas State Fusion Center's information system.

ASFC Personnel - ASFC personnel may include state employees, state agency contractors or subcontractors, and federal, state or local agency person(s) assigned to the ASFC.

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 (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication - Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords.

Authorization - The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through Authentication. See Authentication.

Biometrics - Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center - Center refers to the Arkansas State Fusion Center.

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.

Civil Rights - The term "civil rights" refers to governments' role in ensuring that 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 on 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.

Computer Security—The protection of information assets through the use of technology, processes, and training.

Confidentiality - Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials - Information that includes identification and proof of identification that is used to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates.

Criminal Intelligence Information—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 activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

Data - Elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure - The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disc optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

Fair Information Principles -The Fair Information Principles (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows or 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 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

Firewall—A security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations, such as computer-aided dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information may be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Fusion Center - A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing their ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

Homeland Security Information - As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Homeland Security Liaison Officer (HSLO) - is a specially trained individual within his respective discipline to be responsible for coordinating the all-crimes/all-hazards approach from his local agency to ASFC.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

Individual Responsibility—Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

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 may be categorized in general areas, including, but not limited to, general data, tips and leads data, suspicious activity reports, criminal intelligence information, intelligence information, or investigatory records.

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.

Information sharing Environment (ISE) Suspicious Activity Report-SAR (ISE-SAR) - A suspicious activity report (SAR) that has been determined, pursuant to a two-step process, established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to 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.

Law Enforcement Information - For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident— A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

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

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and nonelectronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. 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 on the type of information and the context of use.

Need to Know—As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Nonrepudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR (and when Authorized, ISE-SAR) information that is collected by a fusion center.

Participating Agency—An organizational entity that is authorized to access or receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Data – Personal Data refers to any information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personal Information - Information which can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

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, 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, biometrics information such as fingerprints, DNA, and retinal scans).
- A unique set of numbers of 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 Systems [AIFIS] 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.).

Persons - Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency concerned to b e permanent resident aliens, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

Privacy - Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the right 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 Fields - Data fields in ISE-SAR IEPD's that contains personal information.

Privacy Policy - A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personal 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, disclosure, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center 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 maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information - Protected information includes Personal Data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Arkansas constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; and applicable state and local law. Protection may also be extended to organizations by center policy or state and local law.

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/center'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/center in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.

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 ASFC'S control.

Repudiation—The ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention - Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about 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 a person's privacy.

Role-Based Access - A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security - Security refers to the range of administrative, technical, and physical business practices and 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.

Shared Space - A networked data and information repository that is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

Sharing - Refers to the act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

Source Agency - Source agency refers to the agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Storage - In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

- Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
- In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.
- Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.
- With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Submitting Agency - Submitting agency refers to the agency or entity providing ISE-SAR information to the shared space)

Suspicious Activity - Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR) - Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional agency. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information - Consistent with Section 1016(a)(4) of IRTPA, all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (c) communications of or by such groups or individuals, or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information - In accordance with IRTPA, as amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also Information Sharing Environment Implementation Plan (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information:" (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

Tips and Leads Information or Data – Generally, uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or Computer Aided Dispatch (CAD) data.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

User —An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

APPENDIX B

Federal Laws, Regulations and References:

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations,
Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272

APPENDIX C

State Laws, Regulations and References:

Arkansas Homeland Security Advisory Group
A.C.A. § 12-75-132

Criminal Intelligence Information
A.C.A. § 12-12-1001

Office of Motor Vehicles Records
A.C.A. § 27-14-401 *et seq*.

Disclosure of Personal Information Contained in Motor Vehicle Records
A.C.A. § 27-14-412

Personal Information Protection Act
A.C.A. § 4-110-101 *et seq*.

Arkansas State Fusion Center
Executive Order 08-11

Arkansas Freedom of Information Act
A.C.A. § 25-19-101 *et seq*.

Arkansas Constitution
Article 2 (Declaration of Rights)

Disclosure of Security Breaches
A.C.A. § 4-110-105

Procedure for sealing of records
A.C.A. § 16-90-904

Release of Medical Information
A.C.A. § 4-110-101 *et seq*. (Personal Information Protection Act)

Release of Social Security Number
A.C.A. § 4-110-104 (Personal Information Protection Act)

APPENDIX D

Receipt of ASFC Privacy Policy By ASFC and Non-ASFC Personnel

My signature below indicates that I have been provided a copy, have read and that I understand the Arkansas State Fusion Center Privacy Policy.

Signature: _____

Printed Name: _____

Agency: _____

Date Signed: _____