Alabama Fusion Center

Privacy Policy

9/25/2012

This Alabama Fusion Center Privacy Policy is applicable to all AFC operations and activities. It supersedes the previous private policy dated 10/8/2010.

"signed"
Joe B. Davis
Director

ALABAMA FUSION CENTER
PRIVACY POLICY

Table of Contents

A. PURPOSE

The mission of the Alabama Fusion Center (AFC) is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal and terrorist activity in the state while following the applicable fair information practices to ensure the rights and privacy of citizens. The purpose of this privacy, civil rights, and civil liberties protection policy is to promote AFC user conduct that complies with applicable federal, state, local, and tribal laws for AFC employees and its users with regard to:

- Increasing public safety and improving national security,
- Minimizing the threat and risk of injury to specific individuals,
- Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health,
- Minimizing the threat and risk of damage to real or personal property, and
- Protecting individual privacy, civil rights, civil liberties, and other protected interests.

B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

1. All AFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with the AFC's privacy policy concerning the information the agency/center collects, receives, maintains, archives, accesses, or discloses to agency/center 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 AFC will provide a printed or electronic copy of this policy to all AFC and non-AFC personnel who provide services to the AFC and will require a written or electronic acknowledgement of receipt of this policy and a written or electronic agreement to comply with this policy and the provisions it contains.

3. All AFC 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 Appendix B.

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

C. GOVERNANCE AND OVERSIGHT

1. Primary responsibility for the operation of the AFC, 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 Director, AFC.

2. The Fusion Center Director will serve as the privacy officer. The AFC will also have a trained Privacy Manager, selected by the AFC Director, who is responsible for ensuring that this privacy policy is implemented, and who receives reports regarding alleged errors and violations of the provisions of this policy. The Privacy Manager can be contacted at the following e-mail fusioncenter@alacop.gov.

3. The AFC Executive Steering Committee will provide oversight with regard to this policy and its provisions.

D. DEFINITIONS

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

E. INFORMATION

1. The AFC will keep a record of the source of all information retained by the center.

2. The AFC will seek 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, 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 relevant to planning and response to a natural disaster or other public safety emergency; or
   - Is useful in a crime analysis or in the administration of criminal justice and public safety (including topical searches); and
     - Is derived from a source of the information that is reliable and verifiable or limitations on the quality of the information are identified; and
     - Was collected in a fair and lawful manner, with or without the knowledge and consent of the individual, if appropriate.

3. The AFC 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 information, subject to the policies and procedures.

4. The AFC 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.

5. The AFC will apply labels (either electronically or on paper, depending on the medium) to agency-originated information (or ensure that the originating agency has applied labels) to indicate to the accessing authorized user that the information is protected information as defined by the center to include personal data pertaining to any individual (See Appendix B) and, to the extent expressly provided in this policy, to include organizational entities.

6. The AFC personnel will, upon receipt of information, access the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment. The various categories of information may be stored in the repository in accordance with federal policy supplements and interpretations to 28 CFR Part 23. The intent is to clearly label the various types of information but not to limit the power of information technology by artificially requiring separate storage areas. Labels may include but not limited to:

   - Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, Department of Corrections information, open source, governmental records, or other information category as defined by AFC.

- 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).
- The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

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

   - Protect confidential sources and police undercover techniques and methods;
   - Not interfere with or compromise pending criminal investigations;
   - Indicate that the information is subject to Federal and Alabama laws restricting access, use, or disclosure, including, but not limited to, 18 USC § 2721 et. seq., Ala. Code § 41-13-6, and Ala. Code § 41-9-642
   - 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.

8. 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 new 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.

9. AFC 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. AFC 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 AFC 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).
   - 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.

   - Retain information for 180 days in order 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 that

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 center's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads 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.

10. The AFC will incorporate 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 constitutional rights, including personal privacy and other civil liberties, and civil rights.

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

12. The AFC will require 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. 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 who questions regarding the information should be directed.

13. The AFC 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.

F. ACQUIRING AND RECEIVING INFORMATION

1. Information gathering (acquisition and access) and investigative techniques used by the AFC 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 *Fair information Practices* (under certain circumstances, there may be exceptions to the *Fair Information Practices*, e.g., based on authorities paralleling those provided in the Federal Privacy Act; state, local, and tribal laws; or center policy).
- Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
- Applicable constitutional provisions and any applicable administrative rules, as well as any other regulations that apply to multijurisdictional intelligence databases, as cited in Appendix B.

2. The AFC'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 criminal or terrorism nexus. Law enforcement officers and AFC personnel will be trained to recognize those behaviors and incidents that are indicative of criminal activity.

3. The AFC'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 investigative techniques used by the AFC will (and for originating agencies should) be the least intrusive 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 AFC are governed by the laws and rules governing those individual agencies, as well as by applicable federal and state laws.

6. The AFC will contract only with governmental 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 AFC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who or nongovernmental entity except as expressly authorized by law or center policy.
- An individual or information provider that is legally prohibited from obtaining or disclosing the information.

G. INFORMATION QUALITY ASSURANCE

1. The AFC 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 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 AFC Privacy Manager will investigate, 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 AFC managers will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the agency/center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the agency; or the source used prohibited means 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 AFC are responsible for the quality and accuracy of the data accessed by or provided to the AFC. The AFC will advise the appropriate contact person in the originating agency in writing if its data is suspected or found to be inaccurate, incomplete, out of date, or unverifiable.

7. The AFC 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 AFC. For example, when 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 AFC 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.

3. Information acquired or received by the AFC 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, or prosecution objectives and priorities established by the AFC: or
- 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.

I. MERGING RECORDS

1. The set of identifying information sufficient to allow merging 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 info 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 AFC will adhere to national standards 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 by the AFC will be provided only to persons within 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 will be kept of access by or dissemination of information to such persons.

4. Agencies external to the AFC may not disseminate AFC information received from AFC 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 AFC without restrictions from its originating source and disseminated to agencies external to the AFC by the AFC. The external agencies may be required to obtain approval from the AFC to disseminate the information received from the AFC as needed.

5. Records retained by the AFC 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 will be kept of access by or dissemination of information to such persons.

6. Information gathered and records retained by the AFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those users 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. Select intelligence analysts from local law enforcement and other law enforcement agencies may be granted access to the AFC intelligence repository and will serve as field intelligence analysts for the AFC. This select group of analysts will access and input to the system in the same fashion as AFC intelligence analysts. MOUs will be developed by AFC and signed by both organizations before access is granted.

7. Information gathered and records retained by the AFC 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 AFC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the laws of the State of Alabama for this type of information. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

8. Information gathered and records retained by the AFC 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.

9. There are several categories of records that will ordinarily not be provided to the public:

- Law enforcement investigative reports and related investigative material (Ala. Code § 12-21-3.1). Records concerning security plans, procedures, assessments, measures, or systems, and any other records relating to, or having an impact upon, the security or safety of persons, structures, facilities, or other infrastructures, including without limitation information concerning critical infrastructure (as defined at 42 U.S.C. § 5195c(e) as amended) and critical energy infrastructure information (as defined at

18 C.F.R. § 388.113(c)(1) as amended) the public disclosure of which could reasonably be expected to be detrimental to the public safety or welfare, and records the disclosure of which would otherwise be detrimental to the best interests of the public (Ala. Code 36-12-40).

- Information that meets the definition of ―classified information‖ as that term is defined in the National Security Act, Public law 235, Section 606 and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission, unless they are required to be disclosed under the Alabama Law (Ala Code 41-9-642).
- Records in violation of an authorized nondisclosure agreement (Ala Code 41-9-642).
- Other records required to be kept confidential by federal or Alabama law.

10. The AFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself, unless otherwise required by law.

K. REDRESS

1. Disclosure

(a) Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified 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 AFC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The AFC's 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.

(b) The existence, content, or source of the info will not be made available to an individual when:

• Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (Ala. Code § 12-21-3.1;
• The information is in a criminal intelligence system (28CFR Part 23);
• Disclosure would endanger the health or safety of an individual, organization, or community (Ala. Code § 36-12-40).

If the information does not originate with the agency, the request will be referred to the originating agency, if appropriate or required, or the agency will notify the source agency of the request and its determination that disclosure by the agency or referral of the request to the source agency was neither required nor appropriate under applicable law.

2. Complaints and Corrections

(a) If an individual has complaints or objections to the accuracy or completeness of information about him or her originating with the agency, including information that may be shared through the ISE, the AFC's Privacy Officer or Privacy Manager will inform the individual of the procedure for submitting complaints or requesting corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

(b) 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 AFC's privacy official 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.

(c) An individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the AFC or originating agency, including ISE participating agencies, and be informed of any existing procedure for appeal. The individual will also be informed of the procedure for appeal when the center or originating agency has cited an exemption for the type of individual to whom the information relates. To delineate protected information shared through the ISE from other data, the AFC 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.

(d) If an individual has a complaint or objection to the accuracy or completeness of terrorism-related information that has been or may be shared through the ISE that: (a) is held by the AFC; (b) allegedly resulted in harm to the complainant; and (c) is exempt from disclosure, the AFC will inform the individual of the procedure for submitting (if needed) and resolving complaints or objections. Complaints should be directed to the AFC Privacy Manager at the following e-mail address: fusioncenter@alacop.gov. The AFC Privacy Manager will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of the information that is exempt from disclosure, as permitted by law. If the information did not originate with the AFC, AFC will notify the originating agency in writing or electronically within 10 business days and, upon request, assist such agency to correct or purge any identified data/record deficiencies, subject to applicable records retention procedures, or to verify that the record is accurate. Any personal information originating with the AFC will be reviewed within 30 days and confirmed or corrected in or deleted from AFC 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 agency 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.

L. SECURITY SAFEGUARDS

1. The AFC Director is designated and trained to serve as the AFC's Security Officer. The Director will be assisted by the Security Manager.

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

3. The AFC will initially process tips, leads, and SAR information in a SAR vetting tool, but ultimately, this information will be appropriately labeled and incorporated into the AFC intelligence repository. The metadata or data field labels will inform authorized users of the AFC system that this information is a tip, lead or SAR and subject to all applicable legal requirements.

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

5. The AFC 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 AFC 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 AFC information will be granted only to AFC 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 AFC 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, reputational, or financial harm to the person. 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 AFC's retention and destruction policy, it will be purged, destroyed, and deleted or returned to the submitting source. Most of the paper records created during the first four years of AFC operation are RFIs that have been converted to electronic records. If a paper record must be destroyed, then it will be shredded using the appropriate cross cut shredders located within AFC. The AFC electronic records maintained within the AFC repository will be purged by a system administrator via a manual purge routine. The system has been configured to provide a listing of documents (based on "creation date") for review by the administrator on a quarterly basis.

3. The AFC delete the information in electronic repositories, and shred paper records (or return them to their source) unless validated as specified in 28 CFR Part 23 and as agreed upon with the originating agency in a memorandum of agreement. For electronic records, the automated system is set up to generate a review based on the "created on" date. Electronic records meeting the criteria will be reviewed by the senior intelligence analyst on a quarterly basis and deletion will be accomplished via a manual purge routine. Paper records meeting the criteria will also be reviewed by the senior intelligence analyst on a quarterly basis and shredding will be accomplished on the approved cross cut security shredders located in the AFC. When appropriate, certain documents may be returned to the originating entity by US registered mail or by AFC courier.

4. No approval will be required from the originating agency before information held by the AFC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a memorandum of understanding or memorandum of agreement.

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 AFC 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

1. Information System Transparency

(a) The AFC will be open with the public in regard to information and intelligence collection practices. The AFC privacy policy will be posted on the AFC Website (http://fusionalabama.gov) and made available upon request made to the following e-mail address: fusioncenter@alacop.gov.

(b) The AFC Privacy Manager will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s). Complaints should be directed to the AFC Privacy Manager at the following e-mail address: fusioncenter@alacop.gov.

2. Accountability

(a) The audit log of queries made to the AFC will identify the user initiating the query.

(b) The AFC 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.

(c) The AFC 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 AFC Director.

(d) The AFC's personnel or other authorized users shall report violations or suspected violations of agency/center policies relating to protected information to the AFC Privacy Manager.

(e) The AFC Privacy Manager and Senior Managers will annually conduct an audit or inspection of the information contained in its criminal intelligence and other systems. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the AFC intelligence system.

(f) The AFC Privacy Officer and Manager, 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.

3. Enforcement

(a) 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 AFC Director 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 center personnel policies;

- If the user is from an agency external to the AFC, 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.

(b) The AFC 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 user who fails to comply with the applicable restrictions and limitations of the AFC's privacy policy.

O. TRAINING

1. The AFC will require the following individuals to participate in privacy training programs and/or briefings (normally annually) regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:

   - All personnel serving on duty within the AFC (local, state, federal or contract)
   - Staff in other public agencies or private contractors providing services to the agency (except ACJIC employees will receive privacy training as directed by Director, ACJIC)
   - Field Intelligence Analysts with access to the AFC Intelligence repository.

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

3. The AFC 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 AFC;
   - How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
   - Mechanisms for reporting violations of agency/center 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 law and policy.
   - The impact of improper activities associated with infractions within or through the agency.

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. For data access, access is usually specified as read-only access and read/write access.

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.

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.

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

General Information or Data—Information that could 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 could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

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 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 compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—A 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).

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.

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.

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.

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.

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 personally identifiable information that relates to an identifiable individual (or data subject).

Persons—Executive Order 12333 defines ―United States persons as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, 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 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.

Protected Information—Protected information is personal data about any individual that is subject to information privacy or other legal protections under the constitution and laws of the State of Alabama or the United States. It includes applicable state and tribal constitutions and State, Local and Tribal laws, ordinances, and codes.

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 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 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.

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:

1. 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.

2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (often 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. Note that 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.

Suspicious Activity—Defined in the ISE-SAR Functional Standard 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. 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 fusion center. 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.

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion. 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 may be based on mere suspicion or on a level of suspicion that is less than ―reasonable suspicion‖ and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

Appendix B: Laws, Regulations and References

Federal:

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

Classified Information, 32 CFR 2003

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

Homeland Security Act of 2002 codified at 6 U.S.C. § 482(f)(1)

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

Intelligence Identities Protection Act, 50 USC 421,

Internal Security Act, 50 USC 783,

IRTPA, as amended by the 9/11 Commission Act Law Enforcement Intelligence Systems,

National Child Protection Act of 1993, Pub. L. 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

Presidential Executive Order 13526 Classified National Security Information

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, Sixth, Thirteenth and Fourteenth Amendments

USA Patriot Act, Public Law No. 107-56 (October 26, 2001), 115 Stat. 272

United States Criminal Laws, including 18 USC 641, 783, 793, 794, 798, 952, 1924

State:

Invasion of Privacy in Relation to Collection/Dissemination of Criminal Data, Ala. Code § 41-9-642

Open Records Act, Ala. Code § 36-12-40

Subpeona of Law Enforcement Officers and Investigative Reports, Ala. Code § 12-21-3.1

Use of Social Security Numbers, Ala. Code § 41-13-6

Appendix C: Receipt of AFC Privacy Policy

To: AFC Policy Manager

My signature below indicates that I have been provided a copy (either paper, electronically or in O drive), and that I have read and understand the Alabama Fusion Center Privacy Policy. I understand that the Privacy Policy applies to me and that a violation of the procedures prescribed may serve as a basis for a disciplinary action, up to and including dismissal.

Signature: _____

Printed Name: _____

Date Signed: _____

Appendix D: Sample Response Letter

Alabama Fusion Center

P.O. Box 304116
Montgomery, AL 36130-4116
334-517-2660

August 1, 2012

John Doe
123 Main Street
Any Town, Alabama 46000

Dear Mr. Doe:

As required by Alabama Code, this letter is a response to your request for access to public records, which was received by this office on MM/DD/YYYY. You specifically requested the following:

–INSERT HERE THE DETAILS OF THE REQUEST.

This office is compiling and reviewing the records and anticipates having a complete response to your request ready to send to you by MM/DD/YYYY.

The copy cost for any records which are responsive to your request will be $1.00 per page. We will notify you of the final copy cost and will then send you the records which may be released upon receipt of payment. If you prefer to pick up the records from the office, please let me know and you may submit payment at that time.

Please do not hesitate to contact us if we can be of further assistance.

Sincerely,

Jane Smith
Director