Alabama Fusion Center Privacy Policy

5/19/2015

This Alabama Fusion Center Privacy Policy is applicable to all AFC operations and activities. It supersedes the previous policy dated 9/25/2012.

Alabama Fusion Center

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 other 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 an electronic copy of this policy to all AFC and non-AFC personnel who provide services to the AFC and will require an 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

The AFC shall have a privacy officer who shall be a licensed Attorney designated by the AFC Director with consultation with the Secretary. The AFC will also have a trained Privacy Manager, selected by the AFC Director, who is responsible for the implementation of this privacy policy.

1. Primary responsibility for the operation of the AFC, its justice systems, operations, and coordination of personnel.
2. The Privacy Manager can be contacted at the following e-mail alabamafusioncenter@alea.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 information retained by the center.

2. The AFC may 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 may have committed a criminal offense or is involved in or is planning criminal (including terrorism) 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 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; 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.

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 retain information about individuals or organizations solely on the basis of lawful actions or beliefs.

5. 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 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.

6. The classification of existing information may be re-evaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of new disclosure of the information.

7. AFC personnel will be responsible for the evaluation and review of applicable suspicious activity information.

8. The AFC will identify and review information prior to sharing that information.

9. The AFC will require certain basic descriptive information to be entered and electronically associated with data. The types of information should include:

- The name of the originating department, component, and subcomponent.
- 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.

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 28 CFR Part 23.
2. The AFC's SAR (suspicious activity reports) 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 or associated with terrorism are documented and shared through the ISE.
4. Information gathering and investigative techniques used by the AFC will be by the least intrusive means necessary in the particular circumstances to gather information it is authorized to 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.

G. INFORMATION QUALITY ASSURANCE

1. The AFC will make every reasonable effort to ensure that information retained is derived from dependable and trustworthy sources of information and will be labeled regarding its level of reliability.
2. The Privacy Manager will in a timely manner, will refer back to originating agency alleged errors or deficiencies before use.
3. The labeling of retained information may be reevaluated when new information is provided that has an impact on reliability in previously retained information.
4. The AFC will conduct data quality reviews of information it generates related to the retention and use policy.
5. 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 if its data is found to be inaccurate, incomplete, out of date, or unverifiable.

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, resource

allocation, or prosecution objectives and priorities established by the AFC: or

- Provide intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorism) activities.

I. MERGING RECORDS

1. The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization or person.
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. 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./or have a need to know.
3. Agencies external to the AFC may not disseminate AFC information received from the AFC without approval from the originator of the information.
4. 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 other law enforcement agencies may be granted access to the AFC intelligence repository and will serve as Field Intelligence Officers (FIO's) for the AFC. MOUs will be signed by both organizations before access is granted.
5. 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. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.
6. 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.
7. 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, 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 accordance 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 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 state law.

K. REDRESS

1. Although the AFC will not confirm the existence or nonexistence of information, if an individual is entitled by court order or other the legal mechanisms AFC may disclose that information.
    - A record will be kept of all requests and of what information is disclosed to an individual.
        - 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 (28 CFR Part 23);
            - Disclosure would endanger the health or safety of an individual, organization, or community (Ala. Code § 36-12-40).
    - If the information did not originate from the AFC 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
    - 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 Privacy Officer at the following e-mail address: alabamafusioncenter@alea.gov. The Privacy Officer 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 within the AFC, AFC will notify the originating agency in writing or electronically 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 within 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, including incorrectly merged information, or out of date information. 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 will designate an AFC Security Officer.
2. The AFC will operate in a secure facility. 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. Queries made to the AFC data applications will be logged into the data system identifying the user initiating the query.
4. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.
5. The AFC will store information in a manner that it cannot be amended, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.
6. When appropriate, 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. The AFC electronic records maintained within the AFC repository will be purged by a system administrator via a manual purge routine.
3. 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.
4. Notification of proposed destruction or return of records may be provided to the source agency, depending on the relevance of the information and any agreement with the providing agency.
5. 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. The AFC privacy policy will be made available via our website or upon request made to the following e-mail address: alabamafusioncenter@alea.gov.
2. Accountability:
    - 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 and what information is disseminated.
    - The AFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems. This will include logging access of these systems and periodic auditing of these systems, so as to not establish a pattern of

the audits. A record of audits will be maintained by the AFC Director.

- 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 Officer.
- The 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 and use of the information systems.

3. Enforcement
    - 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 may take appropriate actions.
    - 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 (annually) regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:
    - All AFC personnel
    - Field Intelligence Officers (FIO's)
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 all appropriate topics related to the proper handling of intelligence information and may include the following:
    - 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

This appendix is not intended to be an exhaustive list of definitions or applicable laws relating to the operation and/or governance of privacy protections and applications. It should be noted that it is the reader's responsibility to research all issues and should not rely solely on definitions or laws provided within this document.

Audit Trail—audit trail is a generic term for recording (logging) a sequence of activities.

Authorization—the process of granting a person, computer process, or device with access to certain information, services, or functionality.

Civil Rights—equal protection under the law and **e**qual opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other rights to personal liberty guaranteed to all United States citizens.

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.

Criminal Intelligence Information—information deemed relevant to the identification of and the criminal activity engaged in by an individual or organization that is reasonably suspected of involvement in criminal acts.

Data— facts and statistics collected together for reference or analysis.

Disclosure— the release, transfer, provision of access to, or divulging information.

Fair Information Practices Principles—Fair Information Practice Principles (FIPP's) are a set of guidelines for information security for federal government department and agencies.

The eight principles 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

Identification—the action or process of identifying someone or something.

Information Sharing Environment (ISE) — broadly refers to the people, projects, systems, and agencies that enable responsible information sharing for national security.

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

Law—includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order.

Logs—an official record of information that is retained.

Metadata—a set of data that describes and gives information about other data.

Need to Know— jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence which is necessary for the conduct of an individual's official duties.

Permissions—Authorization to perform operations associated with a specific shared resource.

Privacy—state of being free from public scrutiny or unsanctioned intrusions.

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.

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.

Record—is information that 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.

Retention—the continued possession, use or control of something.

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.

Security—mechanisms used to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes.

Suspicious Activity—observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

Suspicious Activity Report (SAR)—Official documentation as provided by citizens or law enforcement of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity.

Tips and Leads Information—reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of possible criminal activity.

Appendix B: Laws, Regulations and References

Federal:

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