Alaska Information Analysis Center

Privacy Policy

A. Purpose Statement

The mission of the Alaska Information Analysis Center (AKIAC) is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal and terrorist activity in the State of Alaska while following appropriate privacy and civil liberties safeguards to ensure that information privacy and other legal rights of individuals and organizations are protected. AKIAC specifically seeks to:

- Increase public safety and improve national security.
- Minimize the threat and risk of injury to specific individuals.
- Minimize the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
- Minimize the threat and risk of damage to real or personal property.
- Protect individual privacy, civil rights, civil liberties, and other protected interests.
- Protect the integrity of the criminal investigatory, criminal intelligence, and criminal justice system processes and information.
- Minimize reluctance of individuals or groups to use or cooperate with the criminal justice system.
- Support the role of the criminal justice system in society.
- Promote governmental legitimacy and accountability.
- Make the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

All AKIAC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the center's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, or disseminates to center personnel, governmental agencies (including information sharing environment participating centers and

agencies), participating criminal justice and public safety agencies, private contractors, private entities, and the general public.

AKIAC will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services to the center and to all authorized users of the center.

AKIAC will require all center and non-center personnel who provide services to the center and to all authorized users of the center to execute a written document acknowledging receipt of this policy and agreeing to comply with its terms.

All AKIAC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable law protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S Constitution, the Alaska constitution (Article I, Section 22 Right to Privacy), Alaska Public Records Act, AS 40.25.100 – 40.25.295, and 28 CFR Part 23.

AKIAC has adopted internal operating policies that are in compliance with the applicable law cited above to protect privacy, civil rights, and civil liberties.

Please see Appendix A for definitions of primary terms used in this policy.

C. Governance and Oversight

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

The Director is guided by an Executive Committee and a designated Privacy Officer that is to liaison with the community to ensure that privacy and civil rights are protected as provided in this policy and by the center's information-gathering and collection, retention, and dissemination processes and procedures. The Privacy Officer will annually review and update the policy in response to changes in law and implementation experience, including the results of audits and inspections.

A trained Privacy Officer is to be available to the AKIAC. The Privacy Officer is to receive reports regarding alleged errors and violations of the provisions of this policy, receive and coordinate complaint resolution under the center's redress policy, and serves as the liaison for the Information Sharing Environment ensuring that privacy protections are implemented through efforts such as training, business process changes, and system

designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at john.novak@alaska.gov.

The Privacy Officer will ensure that enforcement procedures and sanctions outlined in this policy are adequate and enforced.

D. Acquiring and Receiving Information

AKIAC will not accept or retain information about individuals or organizations based solely due to religious, political, social views or activities; their participation in non-criminal organizations or lawful events; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

AKIAC will keep a record of the source of all information sought and collected by the center.

AKIAC information acquisition, access efforts and investigative techniques used by AKIAC and information-originating agencies are to adhere to applicable laws and guidance, including:

- 28 CFR Part 23;
- OECD Fair Information Principles; and
- Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP)

AKIAC will contract only with those commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with the law and that the methods they utilize are not based on misleading information gathering practices.

AKIAC may accept and/or retain information that:

- Is based on a possible threat to public safety or the enforcement of the criminal law; 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 criminal justice system

or

- Is useful in crime analysis or in the administration of criminal justice and public safety; 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 center may retain protected 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 this policy.

AKIAC applies labels to agency-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- The information is protected information (as defined by the ISE Privacy Guidelines, to include information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the constitutions and laws of the United States and the State of Alaska. Protection may be extended to other individuals and organizations under Federal or Alaska law or AKIAC policy).

- The information is subject to Federal or Alaska law restricting access, use, or disclosure.

AKIAC will, upon acquisition or receipt of information, assess the information to determine 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, such as:

- Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.

- The nature of the source as it affects veracity, *e.g.*, anonymous tip, informant, peace officer, court record.

- Reliability of the source, *e.g.*, reliable, usually reliable, unreliable, unknown.

- Validity of the content, *e.g.*, confirmed, probable, doubtful, cannot be judged.

At the time a decision is made by AKIAC 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 individual rights of privacy and civil liberties.

- Provide legally required protections 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.

The labels assigned to existing information are to be reevaluated whenever:

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

- There is a change in the use of the information affecting access or disclosure limitations; for example, the information has been disclosed in an open to the public court proceeding.

AKIAC 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. Center 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 center 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 which 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.

- Retain information days in order to work an invalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, 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 center's physical, administrative, and technical security measures to ensure 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 as or similar to the system that secures data that rises to the level of reasonable suspicion.

AKIAC 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 rights, and civil liberties.

AKIAC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center 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.

AKIAC requires certain basic descriptive information (metadata tags or labels) 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 include:

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

- The name of the center'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.

AKIAC 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

The AKIAC'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 appropriate center and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

The AKIAC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities 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 (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

Information-gathering and investigative techniques used by the AKIAC will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

External agencies that access the AKIAC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

AKIAC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.

- An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

E. Information Quality Assurance

AKIAC will undertake reasonable efforts to ensure that information acquired, received, and retained is from trustworthy sources, accurate, current, complete, and in context. Information is to be merged with other information about the same individual or organization only when the applicable standard for merging records set forth in section G. below has been met.

At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence (verifiability and reliability).

AKIAC is to timely investigate alleged errors and deficiencies in acquired or received information that has been retained to correct, delete, or refrain from using or disseminating information found to be erroneous, misleading, or obsolete**.**

The labeling of retained information will be reevaluated by the AKIAC when new information is acquired or received that has an impact on the source reliability or content validity in previously retained information.

AKIAC will conduct periodic data quality reviews of information it originates and undertake reasonable efforts to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, or obsolete; or the center acquired or received the information in violation of the law.

Originating agencies external to AKIAC are to be responsible for reviewing the quality and accuracy of information provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be erroneous, misleading, or obsolete.

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

F. Information Collation and Analysis

Information acquired or received by the AKIAC is analyzed only by qualified individuals who have successfully completed a background evaluation, possess the appropriate security clearances and have been trained.

Information subject to collation and analysis is information as defined and identified in section D, Acquiring and Receiving Information.

Information acquired or received by AKIAC is analyzed in order to:

- Further crime prevention (including terrorism), law enforcement, public safety, and/or prosecution efforts.
- 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.

G. Merging Records

Records about an individual or organization from two or more sources will not be merged by AKIAC unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of match.

If there is not sufficient identifying information to reasonably conclude the information is about the same individual or organization, but there is information to indicate the possibility of the information pertaining to the same individual or organization, the information may be associated by AKIAC if accompanied by a clear statement that it has not been reasonably established that the information relates to the same individual or organization.

H. Sharing and Disclosure

All analytical products created by AKIAC personnel are to be reviewed and approved by the Director or the Privacy Officer to ensure compliance with privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

Credentialed, role-based access criteria will be used by the AKIAC, 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.

- To whom, individually, the information can be disclosed and under what circumstances.

The AKIAC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

Access to or dissemination of information retained by AKAIC is to be provided only to persons within the center, to other governmental agencies, or to private persons or entities in order to facilitate and promote legitimate law enforcement, public protection, prosecution, public health, or criminal justice purposes and only for the performance of official duties. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed is to be kept by the center.

Agencies external to AKIAC are not to disseminate information retained by or analytical products created by the center without approval of the center or other originating agency. .

Information acquired or received and retained by AKIAC may be accessed or disseminated to a member of the public only if the information is a public record not exempt from disclosure under the law or the release of the information is necessary to further the center's mission. AKIAC will not disseminate the following types of information to the public:

- Information from personnel files or other personnel records. See**,** AS 39.25.080).

- Information from records that are required to be kept confidential under federal law, including 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. See**,** AS 40.25.120(a)(4).

- Information from records regarding the investigation or prosecution of a juvenile. See, AS 40.25.120(a)(2).

- Information pertaining to a matter under criminal investigation, subject to potential prosecution, or being prosecuted in the trial or appellate courts. See, AS 40.25.120(a)(6)(A).

- Information disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist. This includes documents prepared to prevent, mitigate, or respond to an act of terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments. See, AS 40.25.120(a)(6)(A).

- Information pertaining to a matter under administrative proceeding investigation, subject to a potential administrative proceeding, or a pending administrative proceeding. See, *NLRB v. Robbins Tire*, 437 U.S. 214 (1978).

- Information that could disclose the identity of a confidential source of information provided to law enforcement. See, AS 40.25.120(a)(6)(A).

- Information that could disclose investigative or prosecution confidential techniques or procedures. See, AS 40.25.120(a)(6)(E).

- Information that would disclose law enforcement or prosecution guidelines, disclosure of which could reasonably be expected to risk circumvention of the law. See, AS 40.25.120(a)(6)(F).

- Information disclosure of which could reasonably be expected to endanger the life or physical safety of a person. See, AS 40.25.120(a)(6)(G).

- Information relating to a pending civil lawsuit in which the State of Alaska or one of its agencies is a party. See, AS 40.25.122.

- Information protected from disclosure by the executive privilege doctrine, attorney client privilege, or deliberative process privilege? See, *Doe v Alaska Superior Court*, 721 P2d 617 (Alaska 1986); *Capital Info. Group v. State*, 923 P2d 29 (Alaska 1996).

- Information as to which the need to protect the state's interest in confidentiality or an individual's reputational interests outweigh the public interest in disclosure. See, *City of Kenai v. Kenai Newspapers*, 642 P2d 1316 (Alaska 1982); *Municipality* of *Anchorage v. Daily News*, 794 P2d 584 (Alaska 1990).

- Information that would unjustifiably fail to protect the personal privacy of a suspect, defendant, victim or witness. See, AS 40.25.120(a)(6)(C).

- Photographs that were part of an application or renewal of a driving license, application or renewal of an identification card, or photograph taken in connection with a law enforcement contact or arrest unless it is apparent that the person depicted would authorize the release if he could be asked. See, *1994 Public Release of Police Records Attorney General Opinion* at p. 28-9.

- Information reflecting the residence address, business address, and/or telephone number(s) for the victim or witness to any crime. See, AS 12.61.110; 11.41.470(7).

- Information reflecting the name(s) of a victim to kidnapping for purposes of sexual assault, first degree sexual assault, second degree sexual assault, third degree sexual assault, first degree sexual assault of a minor, second degree sexual assault of a minor, third degree sexual assault of a minor, fourth degree sexual assault of a minor, incest, unlawful exploitation of minor, or indecent exposure that is the subject of the requested records. See, AS 12.61.140; 11.41.470(7).

- Information reflecting any social security numbers, APSIN numbers, NCIC numbers, ID/OL numbers, passport numbers, and/or financial account/code numbers.

- The information is in a criminal intelligence information system (See, 28 CFR § 23.20(e)) subject to the need to know and right to know requirements of the regulation (see Definitions).

An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed or disseminated be kept by the center.

AKIAC is not to confirm or deny the existence of information to any person or entity that would not be eligible to receive the information unless otherwise required by law.

Information gathered or collected and records retained by the AKIAC 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 disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.

- Disseminated to persons not authorized to access or use the information...

I. Redress

(a) Disclosure

As a general matter, an individual does not have any greater right to know the existence of or review information about himself or herself than a member of the public generally.

All requests for information from an individual or entity outside the center or another governmental agency authorized to have access and seeking the information for legitimate law enforcement, public protection, prosecution, public health, or criminal justice purposes are to be treated as public record requests. See, AS 40.25. The types of information not to be disclosed pursuant to pubic records requests are identified in section H. above. AKIAC personnel also should use the September 30, 2009 Department of Public Safety Public Records Decision Key in responding to public records requests.

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

AKIAC is to timely respond to public records requests. When public record requests are denied in whole or in part, the requestor is to be notified of the denial basis in writing as well as appeal rights. A record is to be kept of all public records requests and what, if any, information is disclosed.

The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the AKIAC or the originating agency. 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 information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

(b) Corrections

If an individual or organization requests correction of information that directly was acquired by or contained in a document created by AKIAC, the center's Privacy Officer is to inform the individual or organization of the procedure for requesting and considering corrections. A record will be kept of all requests for corrections and the resulting action.

If an individual has a complaint 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 AKIAC and

(2) Allegedly has resulted in demonstrable harm to the complainant,

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at john.novak@alaska.gov. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

To delineate protected information shared through the ISE from other data, the AKIAC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

J. Security Safeguards

AKIAC has a trained person to serve as the center's Security Officer.

AKIAC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.

AKIAC will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same

as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

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

Access to AKIAC information will be granted only to AKIAC personnel whose positions and jobs duties required such access; who will be required to successfully complete a background check and appropriate security clearance, if applicable, and who have been trained to assure that information acquired by or received and retained by the center remains secure.

Inquires to AKIAC are to be logged into the data system identifying the user initiating the query.

AKIAC will utilize watch logs to maintain audit trails of requested and disseminated information.

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

AKIAC 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 following discovery of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by the release.

K. Information Retention and Destruction

All applicable information will be reviewed for record retention (validation or purge) , based on a record kept by AKIAC of dates when information is to be removed (purged) if not validated, by AKIAC at least every five (5) years, as provided by 28 CFR Part 23.

When information has no further value or meets the criteria for removal according to AKIAC's retention and destruction policy, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

AKIAC will delete information or return it to the originating agency once its retention period has expired as provided by this policy. AKIAC will not give any advance notice to any information originating agency of its intent

to delete information unless required by a participation or membership agreement.

L. Accountability and Enforcement

(a) Information System Transparency

AKIAC will be open with the public regarding its information and intelligence collection practices. A written copy of the center's privacy policy will be provided upon request and will be posted on the AKIAC Web site upon its establishment.

AKIAC's Privacy Officer is to be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections regarding the center. The Privacy Officer can be contacted at john.novak@alaska.gov.

(b) Accountability

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

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

AKIAC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to 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 annually and a record of the audits will be maintained by the center Director.

AKIAC personnel or other authorized users shall report errors and suspected or confirmed violations of this privacy policy to the center's Privacy Officer.

AKIAC is to annually conduct an audit and inspection of the information and intelligence contained in its information system. Audits will be conducted by the center's designated auditor. The auditor has the option of conducting random audits, without announcement, at any time and without prior notice to center staff. Audits will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

AKIAC's Privacy Officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, purpose and use of the AKIAC information systems, and public expectations.

M. Enforcement

If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the acquisition, receipt, use, retention, destruction, sharing, classification, or dissemination of information, the Director of AKIAC will:

- Take appropriate administrative personnel action, up and including dismissal.
- If the authorized user is from an agency external to the AKIAC, request that the relevant agency, organization, contractor, or service provider employing the user take appropriate administrative personnel action, up and including dismissal.
- Refer the matter to appropriate authorities for criminal prosecution, as appropriate, to effectuate the purposes of this privacy policy and AKIAC's mission.

AKIAC reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel that may violate the center's privacy policy.

N. Training

AKIAC will require the following individuals to participate in training regarding implementation of and adherence to this privacy policy:

- All AKIAC personnel.
- All authorized AKIAC users of governmental agencies outside AKIAC and private contractors providing services to the center.

- Personnel providing information technology services to the center.

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

The AKIAC 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 acquisition, use, analysis, retention, dissemination, destruction, of information.
- Originating and participating agency responsibilities and obligations.
- How to implement the policy in the day-to-day work of the user.
- The potential impact on AKIAC's mission of privacy policy violations.
- Mechanism for reporting violations of center privacy protection policy.
- The nature and possible consequences to individual employees/users that may flow from privacy policy violations.

Dated this ____ day of February, 2012 at Anchorage, Alaska

_____
John J. Novak
Privacy Officer
Alaska Information Analysis Center

Dated this ____ day of February, 2012 at Anchorage, Alaska

_____
Lieutenant Rex Leath
Director
Alaska Information Analysis Center

APPENDIX A – PRIMARY 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.

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 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—The Alaska Information Analysis Center (AKIAC) and all agencies that access, contribute, and share information in the AKIAC's justice information system.

Audit Trail—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.

Authentication—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.

Center—Refers to the AKIAC and all participating state agencies of the AKIAC.

Civil Liberties—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" is used to imply that the state has a 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—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—Inert symbols, signs, descriptions, or measures; 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.

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.

Fair Information Principles—The Fair Information Principles (FIPs) are contained within the Organisation 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:

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

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. It includes 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.

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.

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.

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 four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information.

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 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).

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

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

Logs—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 data. See also Audit Trail.

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.

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.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information.

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

Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans);

A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Integrated Automated Fingerprint Identification System [IAFIS] 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); or

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 be 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—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 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 printed 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, dissemination, and access. The purpose of the privacy policy is to articulate that the center will adhere to those legal requirements and 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 center, the individual, and the public; and promotes public trust.

Protected Information—Refers to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States and the State of Alaska. Protection may also be extended to other individuals and organizations by AKIAC policy or regulation.

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 center's information.
- Media organizations.
- 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 center or participating agency.

Public does not include:

- Employees of the center or participating agency.
- People or entities, private or governmental, which assist the center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the center 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—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the center's

control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

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 authorization that uses roles to determine access rights and privileges. A role is a symbolic category of users that share the same security privilege.

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.

Source Agency—Source agency refers to the agency or organizational 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 is probably the most common meaning in the IT industry.

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—including 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.

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 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.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (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 the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (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 the 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 may include 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 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.

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.