2010

Nebraska Information Analysis Center

Privacy Policy

NIAC
Nebraska State Patrol
10/22/2010

Nebraska Information Analysis Center

Privacy Policy

October 22, 2010

A. Purpose Statement

The Nebraska Information Analysis Center (NIAC) was formed to detect, prevent, investigate, and respond to criminal and terrorist activity. The mission of the NIAC is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal and terrorist activity to federal, state, local, and tribal law enforcement agencies; other Fusion Centers; and to the public and private entities as appropriate, while following the *Fair Information Practices* to ensure the rights and privacy of citizens.

The purpose of NIAC's Privacy Policy is to ensure that NIAC personnel, partners and participating agencies with direct access to NIAC information comply with federal, state, local, and tribal laws; NIAC's policies and procedures; and assists its authorized users in:

- Increasing public safety and improving national security
- Minimizing the threat and risk of injury to specific individuals
- Minimizing the threat and risk of 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
- Protection individual privacy, civil rights, and civil liberties under applicable Federal and State law
- Protecting the integrity of criminal investigations, criminal intelligence, and justice system processes and information

- Minimizing reluctance of individuals or groups to use, or cooperate with, the justice system
- Supporting the role of the justice system in society
- Promoting governmental legitimacy and accountability
- Not unduly burdening the ongoing business of the justice system
- Making the most effective use of public resources allocated to public safety agencies

B. Policy Applicability and Legal Compliance

All NSP and NIAC 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 and the NIAC has adopted internal operating policies that are in compliance with applicable law protecting privacy, civil rights, and civil liberties, including but not limited to Constitution of the United States of America; applicable Civil Rights Acts; 28 CFR Parts 20, 22, and 23; the Electronic Communications Privacy Act of 1986; the Constitution of the State of Nebraska; as well as applicable portions of Nebraska State Statute 84-712.

The NIAC will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services and to participating agencies and individual users and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

C. Governance and Oversight

NIAC was created to provide strategic direction and ensure that objectives are achieved, risks are managed appropriately, and resources are used responsibly. A Governing Board representing the NSP, the Omaha Police Department (OPD), and the Lincoln Police Department (LPD), and Federal Bureau of Investigation (FBI) was established and meets regularly to provide input due to the collaborative nature of the NIAC. Primary responsibility for the operation of the NIAC, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, and evaluation of information; information quality, analysis, destruction, sharing, or disclosure; and the enforcement of this policy is tasked to the Investigative Services Captain (hereinafter referred to as the "Director") assigned to the NIAC.

The Governing Board directed the NIAC to develop a Privacy Policy. The Governing Board ensures that the NIAC's privacy and civil rights are protected within the provisions of this policy and within the NIAC's information collection, retention, and dissemination processes and

procedures. The Governing Board has mandated that the policy be reviewed and updated as appropriate.

The NIAC's privacy committee is guided by a trained Privacy Officer who is the Investigative Services Lieutenant assigned to the NIAC, and who is appointed by the Director of the center. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, ensures that enforcement procedures and sanctions outlined in Section N.3 are adequate and enforced, 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 the following address: 3800 NW 12th Street, Lincoln, NE 68521.

D. Definitions

Primary terms and definitions used in the NIAC Privacy Policy are located in Appendix A., page 16.

E. Information

The NIAC's Watch Center serves as the focal point for the receipt and dissemination of criminal and terrorism activity information. NIAC's information is received from, and disseminated to, local, state, federal, and tribal law enforcement; other Fusion Centers; the public; and to private entities, as appropriate. The Watch Center also supports emergency operations centers which coordinate Nebraska's response to significant man-made and natural disaster incidents. All requests for information are noted in the Watch Center's Request for Information Database.

The NIAC will seek, view and/or retain information that:

- Is based on a criminal predicate or threat to public safety; or
- Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in, and/or planning, criminal (including terrorist) conduct or activity that presents a threat to any individual, community, or the nation, and that the information is relevant to the criminal (including terrorist) conduct or activity; or
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, and sentences; or the prevention of crime; or

- Is useful in crime analysis, or in the administration of criminal justice and public safety (including topical searches); and
- The source of the information is reliable and verifiable, and/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.

All NIAC information will be sought, retained, shared, or disclosed under the appropriate policy provisions.

The NIAC may retain information that is based on a level of suspicion that is less than "reasonable suspicion", such as tips and leads, and information that is reasonably indicative of preoperational planning related to terrorism or other criminal activity, such as Suspicious Activity Report (SAR) or Information Sharing Environment (ISE) SAR (ISE-SAR) information.

The NIAC will not seek or retain 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 race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

The NIAC 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 center, to include personal data on any individual (see definitions of "protected information" and "personal data" in Appendix A of policy), and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to local, state or federal law restricting access, use, or disclosure.

Upon the receipt of information, the NIAC personnel will evaluate the information to determine its nature, usability, and quality. Personnel will assess information to ensure proper segregation, such as:

- Whether the information is based upon a standard of reasonable suspicion of criminal activity;
- Whether the information consists of tips and leads, data, or suspicious activity reports;

- The nature of the source of the information as it affects its veracity (for example, whether from an anonymous tip, trained interviewer or investigator, public record, private sector);
- The reliability of the source (for example, reliable, usually reliable, unreliable, unknown); and
- The validity of the content (for example, verified, partially verified, unverified, or unable to verify).
- What level of protection is to be afforded the information based upon the type of information received (e.g. information about U.S. citizens or lawful permanent residents) and to what extent it may be shared through the ISE.

At the time a decision is made by the NIAC 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 law enforcement undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy or his or her civil rights 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 will be reevaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
- There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

NIAC 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 for a period of up to five years in order to work an unvalidated 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.

NIAC personnel, partners and participating agencies will be required to adhere to specific practices and procedures for the receipt, collection, assessment, marking, storage, access, dissemination, retention, and security of tips and leads, and SARs information.

The NIAC 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.

For purposes of sharing information in the Information Sharing Environment, the NIAC 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.

The NIAC will track assessment and dissemination and apply 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, nature of protected information, or classification.

The NIAC 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 whom questions regarding the information should be directed.

The NIAC will record the sources of all information that is retained.

F. Acquiring and Receiving Information

Information gathering and investigative techniques used by the NIAC and participating agencies are in compliance with, and will adhere to, regulations and guidelines including, but not limited to:

- Nebraska Statute 84-712 defines public records, establishes the process for requesting disclosure, and makes statutory exceptions to disclosure.
- 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*, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local and tribal laws; or NIAC policy
- Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP)

The NIAC'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.

Additionally, it provides for the following "human" vetting process upon receiving a suspicious activity report:

- Analyst initially reviews the newly reported information to insure that the information was legally obtained.
- Analyst review to identify behaviors and incidents indicative of terrorist activity.
- Analyst review to compare reported information to established priority information needs (PINs) or standing information needs (SINs).
- Analysts review the input against all available knowledge and information for linkages to other suspicious or criminal activity.
- Based on this review, the analyst will apply his or her professional judgment to determine whether or not the information has a potential nexus to terrorism.
- If the analyst cannot make this explicit determination, the report will not be accessible by the ISE, although it may be retained in the NIAC's files, in accordance with its established retention policies and business rules.

- If the analyst can determine that a SAR has a direct connection to possible terrorism-related criminal activity, the information will be considered an ISE-SAR, and the analyst will provide the information to the local JTTF for use as the basis for an assessment or investigation

Information gathering and investigative techniques used by the NIAC will consist of the least intrusive means necessary, in each particular circumstance, to gather the information it is authorized to seek or retain.

External agencies that receive and share information with the NIAC are governed by the laws and rules governing those individual agencies as well as by applicable federal and state laws.

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

The NIAC 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.

G. Information Quality Assurance

The NIAC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; is accurate, current, and complete, including the relevant context in which it was sought or received; and that the information about the same individual or organization is merged only after utilizing the applicable standards.

At the time of retention in the system, the information will be assessed and labeled with regards to its level of quality (current, verifiable, and reliable).

The NIAC investigates, in a timely manner, alleged errors and deficiencies, and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

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

The NIAC 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 center identifies information that 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.

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

The NIAC will use a written or documented electronic means of notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the NIAC; 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 individual may be affected

H. Collation and Analysis

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

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

Information acquired or received by the NIAC, or accessed from other sources, is analyzed according to priorities and needs only to:

- Further crime prevention (including terrorism), law enforcement, force deployment, or prosecution objectives and priorities established by the NIAC, and
- 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 or terrorist activities.

I. Merging Records

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

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, marks or scars; social security number; driver's license number; or other biometrics such as DNA, retinal scan, or facial recognition. Identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the organization's name, federal or state tax ID number, office address, and telephone number.

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

Access to NIAC information:

- The Investigative Services Captain assigned to the NIAC shall establish requirements and record all personnel as to their access authority and permission to access NIAC's information;
- Permissions regarding viewing, adding, editing, and printing of NIAC information is controlled by NIAC's administrator(s);
- All NIAC personnel, with approval from the Investigative Services Captain assigned to the NIAC, may disclose NIAC information pursuant to applicable policy;
- An audit trail shall be maintained regarding access to, and disclosure of, NIAC information

The NIAC will adhere to the national standards for the SARs process. This will include the use of a standard reporting format, commonly accepted data collection codes, and a sharing process that complies with the Information Sharing Environment Functional Standard SAR.

Access to, or disclosure of, records retained by the NIAC will be provided only to persons within the NIAC or in other governmental agencies who are authorized to have access, and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes, and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center.

Agencies external to the NIAC may not disseminate NIAC information received from NIAC without prior approval from the originator of the information.

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

Information gathered and records retained by the NIAC 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 sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center.

Information gathered and records retained by the NIAC may be accessed or disclosed to a member of the public only if the information is appropriate for release to further the NIAC mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the NIAC for this type of information or when there is a legitimate need. Requests of this nature are recorded in the Watch Center's Request for Information Database.

Information gathered and records retained by the NIAC 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.

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

- Protected federal, state, local, or tribal records, which may include records originating with and controlled by, another agency that cannot be shared without permission.
- 84-712.05 which enumerates all records which may be withheld from the public.
- 28-722 which states that the Department of Health and Human Services shall not release data that would be harmful, detrimental, or would reveal the identity of a reporter of child abuse or neglect.
- 29-4009 lists certain information that the Sex Offender registry shall not release, such as personal information or victim's name.
- 60-484.02 is the DMV section on digital signatures and images. They cannot be disclosed to anyone outside of law enforcement.
- 60-2905 Prohibits disclosure of personal information obtained from DMV without written consent of the person to whom the information pertains.
- A violation of the above statutes would result in civil or criminal penalties as defined in each of the statutes listed above.

The NIAC 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

K. 1 Disclosure

Requests for disclosure of NIAC records by the public will be referred to the NSP Legal Division. By law, the public records act, on public records requests, legal only retains denial responses. The NIAC'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.

The existence, content, and source of the information will not be made available to an individual when:

- Disclosure to the individual is exempt or prohibited by applicable U.S. Code, Nebraska State Statute, or administrative rule.
- The NIAC did not originate or does not have a right to disclose the information. In this instance, the NIAC will refer the request to the agency originating the information.

K. 2 Complaints and Corrections

If an individual has complaints or objections to the accuracy or completeness of information about him or her originating from NIAC information, the NIAC will inform the individual of the procedure for submitting complaints or objections (if not properly communicated), or to request corrections. If an individual's complaint or objection cannot be resolved after review at the NIAC, the individual may request a review of that decision by the Governing Board of the NIAC. A record will be kept of all complaints and requests for corrections as well as the resulting actions, if any.

If an individual has complaints or objections to the accuracy or completeness of information about him or her that originates with another agency, the NIAC will notify the source agency of the complaint or request for correction in writing or electronically within 10 days and, upon request will coordinate with the source agency to assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate, and to ensure that the individual is provided with applicable complaint submission or corrections procedures. 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 or 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 such complaints and requests for corrections as well as resulting actions, if any.

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 NIAC 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.

K. 3 Redress

If an individual has complaints or objections to the accuracy or completeness of NIAC /ISE-SAR information allegedly held by NIAC, and that has resulted in specific, demonstrable harm to such individual, NIAC will inform the individual of the procedure for submitting complaints or requesting corrections (if not properly communicated). Complaints will be received by the center's Privacy Officer at the following address: 3800 NW 12th Street, Lincoln, NE 68521. The Privacy Officer will acknowledge the receipt of the complaint and state that it will be reviewed, but will not confirm the existence or nonexistence of any NIAC/ISE-SAR information in privacy

fields that identifies the individual unless otherwise required by law. Any personal information will be reviewed and corrected in, or deleted from; NIAC /ISE-SAR shared space if the information is determined to be erroneous, includes incorrectly merged information, or is out of date. A record will be kept of all complaints and requests for corrections as well as the resulting actions, if any.

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

L. Security Safeguards

The NIAC's Investigative Lieutenant is designated and trained to serve as the center's security officer.

The NIAC is located in a secure facility within the Headquarters Troop area of the NSP, protected from external intrusion. The NIAC's office space is only accessible to NIAC personnel, partners, and participating agencies, and other authorized NSP personnel that have been issued an access card for the NIAC. The NIAC will utilize secure internal and external safeguards against network intrusions. Access to NIAC's system from outside the facility will be allowed only over secure networks. The NIAC's information system is an NSP system, and thus, is maintained by that agency. All NSP systems, including the NIAC system, are required to complete an annual security risk assessment. The purpose of this annual assessment is to identify vulnerabilities. All NSP information systems are required to be compliant with ISO/IEC 17799 standards, National Institute of Standards and Technology Special Publications 800-30 standards, and PCI DSS standards.

The NIAC will secure tips, leads, and SAR information, in a repository system using security procedures and policies that are the same as, or similar to, the system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

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

Direct access to NIAC's information will be granted only to NIAC personnel, partners, and participating agencies, whose positions and job duties require such access; who have successfully completed a background check and retain appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

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

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

To prevent public records disclosure, risk and vulnerability assessments are stored in a separate system, the Automated Critical Asset Management System (ACAMS) database, and will not be stored with publicly available data.

The NIAC will notify an individual whose personal information was, or is, reasonably believed to have been breached or obtained by an unauthorized person, and for whom such unauthorized access may result in physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of unauthorized access to the information, and consistent with the legitimate needs of law enforcement to investigate 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

All NIAC-generated applicable information and/or information furnished to NIAC, some of which may be for dissemination, will be reviewed for record retention (validation or purge) at least every five years, as provided by 28 CFR Part 23.

When information has no further value or meets the criteria for removal according to the NIAC's retention and destruction policy it will be purged, destroyed, and deleted or returned to the submitting (originating) agency. A record of information to be reviewed for retention will be maintained by the NIAC, notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

The NIAC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

No approval will be required from the originating agency before information held by the NIAC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

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

N. Accountability and Enforcement

N. 1 Information System Transparency

The NIAC will be open with the public with regard to information and intelligence collection practices. The NIAC's Privacy Policy will be provided to the public upon request and posted on the center's publicly available Website (https://niac.nebraska.gov/).

The NIAC's Privacy Officer will be responsible for receiving inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s). The privacy officer can be contacted at the following address: 3800 NW 12th Street, Lincoln, NE 68521. The NIAC's Privacy Officer will report all inquiries and complaints to the NSP's Legal Department. The Legal Department will direct the handling and response to inquiries and complaints.

N. 2 Accountability

The Watch Center's Request for Information Database will record queries and other pertinent information. Accessing the Watch Center's Request for Information Database identifies the user in the NIAC's audit system.

The Watch Center's Request for Information Database will be kept to identify who requested information. All dissemination will be denoted on the original document submitted to NIAC. The NIAC's audit system records access to Watch Center's Request for Information database. A record will be kept for a minimum of two years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

The NIAC will provide a copy of this policy to all NIAC personnel, partners, and participating agencies.

The NIAC's Privacy Officer will periodically conduct audits to ensure and evaluate the compliance of users. The Privacy Officer will conduct an annual audit and inspection of the Watch Center's information. Random audits of information and compliance will be performed as deemed appropriate by the Privacy Officer.

The NIAC's personnel, or other personnel participating with the NIAC, shall report violations or suspected violations of NIAC policies relating to protected information to the NIAC's Privacy Officer and/or the Governing Board.

The NIAC's Governing Board, guided by the trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy at least annually and will make appropriate changes in response to changes in applicable law, technology, purpose and use of the information systems, and public expectations.

The NIAC will notify an individual about whom sensitive personally-identifiable 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 individual. The notice will be made promptly and without unreasonable delay, following discovery or notification of the access to the information; in a manner 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.

N. 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 Privacy Officer will:

- Notify, in writing, the chief executive of the employing agency of the noncompliance of his or her employee of the violation.
- Initiate an investigation, criminal, if appropriate.

In addition:

- As the NIAC is a multi-agency effort, the Investigative Services Captain assigned to the NIAC will work with each agency regarding their personnel policies for appropriate sanctions that do not rise to a criminal matter.
- Agencies must take action to correct such violations and provide an assurance in writing, to the Director of the NIAC that corrective action has been taken.
- The failure to remedy violations may result in suspension or termination of access for the employee to NIAC information.
- The NIAC reserves the right to restrict the qualifications and number of personnel having direct access to NIAC information, and to suspend or withhold service to any participating agency user who fails to comply with the applicable restrictions and limitations of the NIAC's privacy policy.

O. Training

The NIAC 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 NIAC will require annual training for the following individuals regarding implementation of and adherence to the privacy policy:

- Any person that is granted direct access to NIAC information
- Personnel authorized to share protected information through the Information Sharing Environment.

The NIAC's 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 NIAC;
- How to implement the policy in the day-to-day work of the user, whether a paper or systems user;
- The impact of improper activities associated with infractions within, or through, the agency;
- Mechanisms for reporting violations of NIAC 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.

Appendix A - Definitions

The following are the primary terms and definitions used in this privacy policy document:

Access—Data access refers to the ability to get to (usually having permission to use) particular data on a computer. Web access refers to 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 or read/write access.

With regard to the Information Sharing Environment, access refers to the business rules, means, and processes by, and through which, Information Sharing Environment participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another Information Sharing Environment participant.

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

Acquisition—The means by which an Information Sharing Environment 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 Information Sharing Environment participants, for example, through news reports or by obtaining information from another Information Sharing Environment participant who originally acquired the information.

Agency—Agency refers to the NIAC and all agencies that access, contribute, and share information in the NIAC'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 and are 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 provides adequate credentials that prove identity. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. *See Biometrics.*

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

Authorized User—A person that is granted direct access to NIAC information.

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

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; therefore civil rights are 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.

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.

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

Confidentiality—Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately

once it has been disclosed to them. One observes rules of confidentiality out of respect for, and to protect and preserve, the privacy of others. *See Privacy*.

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

Criminal Intelligence Information or Data—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. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information.

Data—Inert symbols, signs, descriptions, or measures.

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

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

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

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

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. These were developed around commercial transactions and the trans-border exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles. They 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

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

General Information or Data—Information that may include records, documents, or files pertaining to law enforcement operations such as computer-aided dispatch (CAD) data, incident data, and management information; and 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.

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

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, tips and leads data, suspicious activity reports, and criminal intelligence information.

Information Quality—Information quality refers to various aspects of the information such as 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.

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

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

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

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

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

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

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

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

Need to Know – As a result of jurisdictional, organization, 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.

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

NIAC Call Center—The location within the NSP Headquarters Troop area where information is received, assessed, disseminated and retained.

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

Personal Data—Personal data refers to any information that relates to an identifiable individual. *See also Personally Identifiable Information*.

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

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

Persons—Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency considered 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—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 privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of

information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—Protected information is information about any individual that is subject to information privacy or other legal protections under the Constitution and laws of the United States and the State of Nebraska.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information;
- Media organizations; and
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

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

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

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

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

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

Request for Information Sheet —The input form used by NIAC personnel in the NIAC Call Center to record information received and disseminated.

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 counter-terrorism 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 Authorization—A type of 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—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.

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. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices

such as the processor's L1 cache; and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor, or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the Information Sharing Environment, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland, by both the originator of the information and any recipient of the information.

Suspicious Activity—Suspicious activity is defined as "reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports—The observation and documentation of a suspicious activity. At the federal level, there are two types of SARs: 1) Information Sharing Environment SARs that pertain to terrorism information; and 2) Banking Secrecy Act SARs that pertain to suspicious banking activity and are required to be completed by financial institutions. Suspicious activity reports offer a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR data analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center. SARs are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

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

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

Tips and Leads Information or Data—uncorroborated reports or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data. Tips and leads information is 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 has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.