Missouri State Highway Patrol

Missouri Information Analysis Center

Policies for Privacy, Civil Rights, Civil Liberties and Missouri Statewide Police Intelligence Network

Revised February 10, 2025

Table of Contents

Privacy, Civil Rights and Civil Liberties

Missouri Statewide Police Intelligence Network

Appendices

I. Mission/Purpose

a. The mission of the Missouri Information Analysis Center (MIAC) is to receive, gather, analyze, and disseminate information and intelligence data regarding criminal and terrorist activity to appropriate agencies and individuals, and respond to natural and man-made disasters in a way that enhances public safety. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that the information privacy and other legal rights of individuals and organizations are protected.

b. Toward that end, the MIAC administers the Missouri Statewide Police Intelligence Network (MoSPIN) and facilitates the flow of information through a network of in-house analysts. Although MIAC administers MoSPIN, it is important to note that MIAC and MoSPIN are not one and the same. The MIAC is a division of the Missouri State Highway Patrol (MSHP) charged with the administration of MoSPIN. MoSPIN is a web-enabled database that allows law enforcement to minimize the threat and risk of injury to those responsible for public protection. MoSPIN also allows law enforcement to share intelligence information.

c. The purpose of this privacy, civil rights, and civil liberties (P/CRCL) protection policy is to promote MIAC and user conduct that complies with applicable federal, state, local, tribal, and territorial law. The policy will assist the MIAC and its users in:

   i. Increasing public safety and improving national security.
   ii. Minimizing the threat and risk of injury to specific individuals.
   iii. Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.
   iv. Minimizing the threat and risk of damage to real or personal property.
   v. Protecting individual privacy, civil rights, civil liberties, and other protected interests.
   vi. Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.
   vii. Minimizing the reluctance of individuals or groups to use or cooperate with the justice system.
   viii. Supporting the role of the justice system in society.
   ix. Promoting governmental legitimacy and accountability.
   x. Not unduly burdening the ongoing business of the justice system.
   xi. Making the most effective use of public resources allocated to public safety agencies.

II. Policy Applicability and Legal Compliance

a. All MIAC personnel, participating agency personnel, personnel providing information technology services to the center, staff members in other public agencies, private contractors providing services to the MIAC, and other authorized users who are not employed by the MIAC or a contractor will be trained in and comply with the MIAC's P/CRCL policy. This policy applies to information the MIAC gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information Sharing Environment [ISE] participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

b. The MIAC will provide a printed or electronic copy of this policy to all center personnel. The policy will be posted on the MIAC website for review by participating agencies, individual users, and interested parties, public or private.

c. All MIAC personnel, participating agency personnel, personnel providing information technology services to the MIAC, private contractors, agencies from which center information originates, and other authorized users will comply with all federal and state privacy laws, including but not limited to those cited in the appendix to this policy. Applicable laws protecting civil rights, liberties and privacy include:

    i. Federal Regulations: 28 CFR Part 23, State Statutes: Sections 610.010, 610.021 through 610.025, 610.027 through 610.030, 610.032, 610.035, 610.100, 610.105, 610.106, 610.110, 610.115, 610.120, 610.150, 610.200; 109.180 and 109.190 and Section 407.1500 RSMo.

d. The MIAC has adopted internal operating policies that follow applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to:

    i. Federal Regulations: 28 CFR Part 23, State Statutes: Sections 610.010, 610.021 through 610.025, 610.027 through 610.030, 610.032, 610.035, 610.100, 610.105, 610.106, 610.110, 610.115, 610.120, 610.150, 610.200; 109.180, 109.190 and Section 407.1500 RSMo.

III. Governance and Oversight

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

b. The MIAC is guided by a designated privacy oversight committee that is made up of MIAC assistant Directors, Supervisory Analysts, and the designated Privacy Officer. The committee will annually review and update the privacy policy in response to changes in law, in response to any changes to MSHP General Orders, and implementation experience, including the results of audits and inspections. The Privacy Committee may institute changes in the MIAC Privacy Policy upon the advice of legal counsel. The privacy policy will also be reviewed by MSHP legal counsel on odd years.

c. The MIAC's privacy committee is guided by a trained Privacy Officer, who is appointed by the MIAC Director. 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, and serves as the liaison for the center (and for the Information Sharing Environment), ensuring that privacy, civil rights, and civil liberties 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: miac@mshp.dps.mo.gov or by telephone - 866-362-6422.

d. MIAC employees will follow specified ISE* Guidelines as established in Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 and Section 1 of Executive Order 1388. The ISE Privacy Guidelines are attached and listed as Appendix B to this Privacy Policy. The Privacy Officer's duties will include training assurance, reception and evaluation of errors

and violations of this policy, act as a repository for complaints from the general public regarding this policy, and ensure the MIAC adheres to the provisions of the ISE Privacy Guidelines.

e. The MIAC Director, Privacy Officer, or authorized designee will comply with the enforcement standards outlined in section XIII of this policy. This Privacy Policy is not designed to override the responsibilities of the Superintendent of the MSHP and in no way encroaches on the Superintendent's authority. This policy enhances and is in addition to the already established General Orders of the MSHP.

IV. Information

a. The MIAC is not an investigative division, however in fulfilling its public safety role, the MIAC will seek or retain information (including "protected attributes") subject to conditions articulated in Section IV.B, that:

   i. Is based on a possible threat to public safety or the enforcement of criminal law, or
   ii. 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 the information is relevant to the criminal (including terrorist) conduct or activity, or
   iii. Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
   iv. Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
   v. The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   vi. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

   MIAC may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads (including suspicious activity report [SAR] information) subject to the policies and procedures specified in this policy.

b. In accordance with applicable laws, guidance, and regulations, the MIAC will not seek or retain and will inform information-originating agencies not to submit information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, national origin, ages, disabilities, genders, gender identities, or sexual orientations.

   When documenting a SAR or an ISE-SAR in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI), race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity must not be considered as factors creating suspicion. However, those attributes may be documented in specific suspect descriptions for identification purposes.

c. MIAC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:

i. Whether the information consists of tips and leads (including SAR data), criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
ii. The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
iii. The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
iv. The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

d. At the time a decision is made by the MIAC 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:

i. Protect confidential sources and police undercover techniques and methods.
ii. Not interfere with or compromise pending criminal investigations.
iii. Protect an individual's right of privacy and his or her civil rights and civil liberties.
iv. 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.

e. The labels assigned to existing information under (see Section IV.d above) will be reevaluated whenever:

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

f. MIAC 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 (including SAR information). MIAC personnel will:

i. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place, the information has been assessed for sensitivity and confidence 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 MIAC will use a standard reporting format and data collection codes for SAR information.
ii. Store the information using the same or similar storage method used for data which 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.
iii. 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 PII).
iv. After reviewing a SAR, tip, or lead, assigned personnel will assign a "disposition" label (for example, information only, closed, under investigation by law enforcement, or not

enough information to disseminate) so that a subsequently authorized user knows the status.

v. Adhere to and follow the MIAC'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.

vi. Criminal intelligence will be disseminated to appropriate agencies and entry made into the MoSPIN if criteria are met. This information may include the source of the information, the credibility, if known, the accuracy, if known, validity of the content, if known, and known completeness.

g. The MIAC 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.

h. The MIAC 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, to enable ISE authorized users the ability to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

i. The MIAC 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:

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

ii. The name of the center's justice information system from which the information is disseminated.

iii. The date the information was collected and, when feasible, the date its accuracy was last verified.

iv. The title and contact information for the person to whom questions regarding the information should be directed.

j. The MIAC will attach (or ensure 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.

k. Information received, analyzed, and disseminated at the MIAC will include, at a minimum, indicators for type of criminal investigation, tips and leads (including Suspicious Activity Reporting), source information, requestor identification, reliability of the source, accuracy and validity of the content, currency, sensitivity, completeness, juvenile information, and protected status information. Information may be reclassified whenever new information is added that would increase/decrease the sensitivity of disclosure or impact the validity and reliability of the

information. The MIAC will comply with and adhere to all applicable laws, including the following regulations and guidelines:

i. 28 CFR Part 23, regarding criminal intelligence information
ii. Missouri state statutes Chapters 610 and 407 RSMo
iii. MSHP General Orders and MIAC Division policy
iv. ISE Privacy Guidelines as outlined in Appendix B.

V. Acquiring and Receiving Information

a. Information-gathering (acquisition), access and investigative techniques used by the MIAC and information-originating agencies will remain in compliance and adhere to applicable laws and guidance, including, but not limited to:

   i. 28 CFR Part 23 regarding "criminal intelligence information," as applicable.
   ii. The FIPPs; see [refer to Appendix C, "Fair Information Practice Principles"] but note under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy).
   iii. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP) (Ver. 2).
   iv. Constitutional provisions, administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

b. The MIAC's SAR process provides for human review and vetting to ensure that information is both gathered in an authorized and lawful manner and, when applicable, determined to have a potential terrorism nexus. Law enforcement officers and appropriate center and participating agency staff members will be trained to recognize those behaviors and incidents that are indicative of criminal activity associated with terrorism.

c. The MIAC'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, ethnicity, national origin, religion, etc.) and civil liberties (speech, assembly, association, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

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

e. The MIAC will not directly or indirectly receive, seek, accept, or retain information not already in the public domain from:

   i. An individual or nongovernmental entity that may receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
   ii. An individual or information provider that is legally prohibited from obtaining or disclosing the information.

VI. Data Quality Assurance

a. The MIAC contracts with reputable commercial databases that provide an assurance that their methods for gathering personal information is in compliance with all applicable laws, and whose methods are not based on misleading or questionable collection practices. The MIAC will make every reasonable effort to ensure information is derived from dependable and trustworthy sources, is accurate, reasonably up-to-date, and complete, including the relevant context in which it was sought or received and other related information.

b. The MIAC will put in place a process for additional fact development during the vetting process where a SAR includes Personal Identifiable Information (PII) and is based on behaviors that are not inherently criminal. The MIAC will articulate additional facts or circumstances to support the determination that the behavior observed is not innocent but rather reasonably indicative of preoperational planning associated with terrorism.

c. 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 credibility]).

d. MIAC personnel will investigate suspected errors and deficiencies to the best of their ability (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient. Hard files containing deficient/incorrect information will be redacted, and data storage files purged of such information.

e. The labeling of retained information will be reevaluated by the MIAC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content credibility) in previously retained information.

f. Originating agencies external to the MIAC are responsible for reviewing the quality and accuracy of the data provided to the center. The MIAC 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, electronically, or verbally, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

g. The MIAC 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 information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

VII. Collation and Analysis

a. All MIAC employees have successfully passed an employment background check, may possess an appropriate security clearance, and have been selected, approved, trained according to MIAC and MSHP standards, and are authorized to seek, accept, retain, and disseminate appropriate Criminal/Public Safety-related information.

b. Only MIAC analysts and vetted embedded personnel have direct access to and the right to disseminate MIAC information. This information undergoes analysis in order to enhance public

safety, assist in investigations and prosecutions, and provide tactical and strategic intelligence services to authorized recipients.

c. Information acquired or received by the MIAC or accessed from other sources will be analyzed only to:

   i. Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
   ii. 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.

d. The MIAC requires that all strategic analytical products be reviewed [and approved] by the Privacy Officer and the MIAC Director to ensure they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

VIII. Merging Records

a. Information will be merged only by qualified MIAC analysts who have successfully completed a background check and possess the appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.

b. Records about an individual or an organization from two or more sources will not be merged by the MIAC unless there is sufficient identifying information to clearly establish 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.

IX. Sharing and Disclosure

a. Credentialed, role-based access criteria will be used by the MIAC, as appropriate, to control:

   i. The information to which a particular group or class of users can have access based on the group or class.
   ii. The information a class of users can add, change, delete, or print.
   iii. To whom, individually, the information can be disclosed and under what circumstances.

b. Agencies external to the MIAC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

c. Access to or disclosure of records retained by the MIAC will be provided only to persons within the center 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.

d. Information gathered or collected, and records retained by the MIAC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested or received information retained by the

center; the nature of the information requested or received; and the specific purpose will be kept for a maximum of five (5) years by the MIAC.

e. Information that is considered open-source or public record, may be released outside the public safety community if such disclosure will further the MIAC mission and the recipient has a valid need or lawful right to the information. In addition, MIAC personnel will not disclose the existence or non-existence of information to any entity if such disclosure would violate 28 CFR Part 23, Chapter 610 RSMo (State Sunshine Laws), Chapter 32 (State Revenue Laws) or any other applicable record confidentiality law. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information and the nature of the information accessed will be retained by the center.

f. Information gathered or collected, and records retained by the MIAC will not be:

   i. Sold, published, exchanged, or disclosed for commercial purposes.
   ii. 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 or specifically authorized by the originating agency.
   iii. Disseminated to persons not authorized to access or use the information.

g. There are several categories of records that will ordinarily not be provided to the public unless otherwise required by applicable law:

   i. Records required to be kept confidential by law are exempted from disclosure requirements under Chapter 610 RSMO.
   ii. Information determined by the federal government to meet the definition of "classified information" as defined in the National Security Act, Public Law 235, Section 606, and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
   iii. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under [Chapter 610 RSMo]. However, certain law enforcement records must be made available for inspection and copying under [Chapter 610 RSMo].
   iv. A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under [Chapter 610 RSMo]. By way of example, this may include a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under [Chapter 610 RSMo] or an act of agricultural terrorism under [Chapter 610 RSMo], vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
   v. Protected federal, state, local, tribal, or territorial records, which may include records originated and controlled by another agency that cannot, under [Chapter 610 RSMo], be shared without permission.
   vi. A record, or part of a record that constitutes trade secrets or information that is commercial, financial, or otherwise subject to a nondisclosure agreement that was obtained from a person and is privileged and confidential [Chapter 610 RSMo].
   vii. Certain records specified in MSHP General Order 82-01.

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

X. Redress

a. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in X.b., below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the MIAC. The individual may obtain a copy of the information for the purpose of challenging the accuracy or completeness of the information. The MIAC's response to the request for information will be made within a reasonable time and in writing.

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

   i. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
   ii. Disclosure would endanger the health or safety of an individual, organization, or community.
   iii. The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)].
   iv. Such a disclosure violates Missouri state law.
   v. The information source does not reside with the center.
   vi. The center did not originate and does not have a right to disclose the information.
   vii. Other authorized basis for denial.

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

c. These inquiries should be directed to the MIAC Director via email at miac@mshp.dps.mo.gov. The individual at issue may obtain a copy of the text related to them for the purpose of challenging its accuracy.

d. Access to the text will be provided by the MIAC Director or their designee. Appeals to correct or remove text related to that individual will be directed to the MIAC Director. The MIAC Director will make the final decision on any request appeal to correct or remove text with the assistance of the MSHP legal counsel. However, requests for access to the text that concerns an individual will not be honored if disclosure would compromise an ongoing investigation, compromise a source of information, constitute a release of criminal intelligence, the information does not reside within MIAC, or if such disclosure would violate 28 CFR Part 23 or state law.

e. If an individual at issue in the MIAC information requests correction of information originating with the MIAC that has been disclosed, the MIAC Director will inform the individual of the procedure for requesting and considering requested corrections. If that information originated with another agency, the MIAC Director or their designee will notify the originating agency, including ISE sources and coordinate complaint/corrections inquires by forwarding any requests

for alteration, correction, or removal to the originating agency. The MIAC Director will defer to the final decision made by the originating agency. To delineate protected information shared through the ISE from other data, the MIAC maintains records of the ISE participating agencies to which the center has access, as well as audit logs, and employs system mechanisms whereby the source (or originating agency, including ISE participating agencies) is identified within the information. If the information has been provided to the complainant, the originating agency must decide to correct the information, remove the record, or assert a basis for denial.

f. 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 MIAC or the originating agency.

XI. Security Safeguards

a. A MIAC analyst will be designated and trained as the MIAC's security officer and will ensure the center operates in a secure manner free from facility and network intrusion.

b. The MIAC will comply with generally accepted industry or other applicable standards for security, in accordance with [MIAC so15]. Security safeguards will cover any type of medium (printed and electronic) or technology (e.g., physical servers, virtual machines, and mobile devices) used in a work-related MIAC activity. The MIAC 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.

c. The MIAC will store information in such a way that it cannot be accessed, modified, destroyed, or purged by unauthorized personnel as provided for in Chapters 32, 407 or 610 RSMo. The MIAC does not store risk and vulnerability statements.

d. MIAC employees will secure tips, leads, and SAR information in a separate repository system that is the same as or similar to the system that secures data rising to the level of reasonable suspicion.

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

f. Queries made to the MIAC's data applications will be logged into the data system identifying the user initiating the query.

g. The MIAC will utilize audit logs to maintain audit trails of requested and disseminated information.

h. All individuals with access to MIAC's information or information systems will report a suspected or confirmed breach to the Privacy Officer as soon as possible and without unreasonable delay, consistent with applicable laws, regulations, policies, and procedures. This includes a breach in any medium or form, including paper, oral, and electronic.

i. If an individual's personal information retained by the MIAC is compromised, the MIAC will comply with Section 407.1500 RSMo regarding this breach of data provided that notification does not compromise an ongoing investigation. If this occurs the MIAC Director will notify the Criminal Investigation Bureau Commander who may request the Division of Drug and Crime Control (DDCC) provide investigative assistance to identify the source of the leaked information. If the security breach was directed toward MIAC databases, Criminal Justice Information Services Division (CJIS) personnel will be notified in addition to the Criminal Investigation Bureau Commander.

j. Individual MIAC analysts are required to secure ongoing work products within their workspaces at the end of any shift. Wall postings that could possibly compromise the integrity of any investigation or inadvertently reveal personal information should be secured. Visitors through the MIAC must provide adequate identification and a valid need to visit, and any maintenance or custodial personnel must be escorted.

XII. Information Retention and Destruction

a. The Missouri Statewide Police Intelligence Network (MoSPIN) is the official and sole intelligence database utilized by MIAC personnel and administered by the MIAC. MoSPIN maintains its own retention and purge mechanism in compliance with 28 CFR, Part 23. The MoSPIN privacy policy is part of the MIAC privacy policy. The MoSPIN privacy policy begins on page 17. Purge dates are electronically set by the MoSPIN system on an ongoing five-year basis with purge notification provided to the MoSPIN analyst. The MoSPIN system provides an automatic notification within the system of upcoming purge dates for each intelligence entry based on the original entry date.

b. The MIAC website maintains its own retention and purge mechanism. Criminal incidents posted on the MIAC website that have no further investigative or research value will be purged one (1) year from the date of entry. MIAC alerts will purge 60 days after the date of entry.

c. The MIAC's Suspicious Activity Reporting database will retain tips submitted into the system for one (1) year.

d. The MIAC's Courage2Report reporting database will retain tips submitted into the system for five (5) years.

e. Information that has no further investigative or research value or is found to be in error will be destroyed, purged, or returned to the owner. This task will be accomplished at least every five (5) years unless the information is re-validated. Information requiring further analysis, even though not validated, is retained in the audit database for statistical and administrative purposes only up to five (5) years. Information which is validated is made available to the MoSPIN system.

f. Such information will be purged electronically from files and destruction and/or redaction of that information will be implemented in hard file backup systems if applicable. All MIAC analysts are trained in compliance with 28 CFR Part 23 and may be tasked with such destruction. MIAC analysts need no prior approval for the destruction, redaction, and purge of information. Once purged, no record is maintained of its prior existence and no notification is given prior to its

removal unless reasonable suspicion or exigent circumstances lead a MIAC analyst to seek further updates to warrant its retention.

XIII. Accountability and Enforcement

a. The MIAC will remain open and accountable to the public regarding information collection practices. The MIAC Privacy Policy is posted to its public website. Written documentation of the MIAC Privacy Policy is available to those who do not have Internet access.

b. The MIAC Director or Privacy Officer, with guidance from the MSHP legal counsel or Missouri Attorney General's Office, is responsible for responding to inquiries and complaints about privacy, civil rights, and civil liberties within the center. The MIAC undergoes independent audits by both the MSHP's CJIS and the Research and Development Division (RDD) in their Staff Inspections. MoSPIN audits are conducted on a random basis and audit database audits also occur randomly.

c. The MIAC will maintain an audit log of accessed, requested, or disseminated information. An audit log will be kept for a minimum of five (5) years for information requests and the information that was disseminated to each person in response.

d. If any MIAC personnel are found to be non-compliant with the provisions of the MIAC Privacy Policy, the MIAC Director will be notified immediately and will notify the Criminal Investigation Bureau Commander. The personnel's access to MIAC databases will be suspended, pending a thorough investigation. Further punitive actions will be taken in accordance with MSHP General Orders, MIAC Special Orders, or other administrative rules.

e. If MIAC users are found to be non-compliant with the provisions of the MIAC Privacy Policy, the MIAC Director or Assistant Director(s) will request the employer of that user to initiate proceedings to discipline the user, enforce policy provisions, and ensure the integrity of future MIAC usage. Certain cases of abuse may require the MIAC to refer the matter to appropriate law enforcement authorities for investigation and possible criminal prosecution.

f. The MIAC reserves the right to limit personnel having electronic access to MoSPIN, and to withhold or suspend service to any agency or individual violating the MIAC Privacy Policy. MoSPIN operating policies will ensure user identification and identify the information accessed. All users who access MoSPIN information agree to abide by the MoSPIN Privacy Policy. The MIAC does not provide electronic access to any database. The MIAC Director will have periodic audits of the MoSPIN system to assess and evaluate user compliance with MoSPIN policy. Violations of the MoSPIN policy may result in denial of further access.

g. On a quarterly basis, MIAC supervisors will conduct a random audit and inspection of three requests for information contained in its information system(s) of each subordinate under their direct supervision. MIAC supervisors will document the review in the MIAC's records management software.

The audit will be conducted by the MIAC's privacy committee. The privacy committee has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

XIV. Training

a. The MIAC will require all employees, including full-time, part-time, and employees assigned to the MIAC from other participating agencies to participate in training regarding the implementation of this policy. Additional training may be provided by the MSHP staff legal counsel, Missouri Attorney General's Office, United States Department of Homeland Security, and the United States Attorney's Office as to applicable state and federal privacy laws. The MIAC Privacy Policy training will include, but not be limited to the following:

   i. Purposes of the P/CRCL protection policy
   ii. The intent of all provisions of the policy
   iii. The application of policy in day-to-day work
   iv. The potential impact of user abuse of information systems
   v. Training on 28 CFR Part 23

b. MIAC employees will be familiar with reporting mechanisms regarding violations of the policy, and repercussions, including the potential for dismissal, criminal, and individual civil liability. MIAC analysts, authorized to share protected information within the ISE, will receive specialized training in the requirements, policies for collection, use and dissemination of protected information.

XV. Scope and Compliance

All MoSPIN users, personnel providing information technology services, private contractors and other authorized users will comply with the MoSPIN Privacy Policy concerning the information that is collected in the system. The MoSPIN database will be in compliance with the Privacy Policy concerning the information it collects, receives, maintains, archives, accesses, or discloses to law enforcement agencies. This is a written agreement containing the provisions of MoSPIN and ensuring their employees comply with the provisions of this Privacy Policy. All MoSPIN users will sign an Individual User Agreement, attached to this document, and listed as Appendix D. By signing this form, users agree with the provisions of MoSPIN and this Privacy Policy.

XVI. Governance and Oversight

The MIAC Director, MIAC Assistant Directors, the MoSPIN Administrative Analysts, and Privacy Officer have overall responsibility for MoSPIN operations and compliance with this Privacy Policy. The MIAC Assistant Directors have the responsibility to review all entries made into MoSPIN. The MIAC Director has the responsibility to randomly audit MoSPIN entries for compliance with this privacy policy. The primary goal in the operation of MoSPIN is to enhance the operational capabilities, coordination of personnel, and to streamline the intelligence process for all participating agencies. The MIAC Administrative Analysts are also responsible for training personnel on the MoSPIN system.

XVII. Information

a. The MoSPIN database shall collect and maintain criminal intelligence information concerning an individual/business/gang only if there is reasonable suspicion that the individual/business/gang is involved in criminal conduct or activity, and the information is relevant to that criminal conduct or activity.

b. The MoSPIN database shall not collect or maintain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, national origin, age, disability, gender, gender identity, or sexual orientation.

c. Reasonable suspicion or criminal predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual/business/gang is involved in a definable criminal activity or enterprise.

d. The MoSPIN database shall not include any criminal intelligence information that has been obtained by the MIAC in violation of any applicable Federal or State law.

e. MIAC analysts disseminate criminal intelligence information only where there is a “need to know and a right to know” the information in the performance of a law enforcement activity, unless otherwise required by law.

f. MIAC analysts disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination within the guidelines of this Privacy Policy.

g. The MoSPIN database, which maintains criminal intelligence information, ensures that administrative, technical, and physical safeguards (including audit trails) are adopted to ensure against unauthorized access and against intentional or unintentional damage. MoSPIN maintains a record indicating the date each viewing of the record(s) occurred and by which user.

h. The MIAC Director, Assistant Directors or MIAC analysts are responsible for establishing the existence of an inquirer's "need to know and right to know" the information being requested either through inquiry or by delegation of this responsibility to a properly trained analyst.

i. The MoSPIN database documents the source of the information, credibility, and validity of the content, if known.

j. The MoSPIN database requires that intelligence information provided by each agency is to be shared with other law enforcement agencies.

k. The MIAC Director and Assistant Directors assure the following security requirements are implemented:

   i. MoSPIN has adopted effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system
   ii. MoSPIN stores information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization
   iii. MoSPIN has instituted procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or man-made disaster
   iv. MoSPIN rules and regulations are based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and
   v. MoSPIN has adopted procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures provide for the periodic review of information and the destruction of any information which is misleading, obsolete, or otherwise unreliable and requires that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer and date of review. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years submission to the system and supports compliance with project entry criteria.

l. The MoSPIN database complies with and adheres to the following regulations and guidelines:

   i. 28 CFR, Part 23 regarding criminal intelligence information
   ii. Criminal Justice Guidelines established by the Department of Justice
   iii. Missouri state statutes, MSHP General Orders and MIAC Special Orders

m. In providing information, MoSPIN contributors are governed by the laws and rules of their individual agencies as well as by applicable state and federal laws and are notified through an

attached statement that the information is subject to state and federal laws restricting access, use, or disclosure.

XVIII. Acquiring and Receiving Information

Information gathering and investigative techniques used to populate the MoSPIN database will comply with and adhere to all applicable laws, including the following regulations and guidelines: MoSPIN will follow 28 CFR, Part 23 with regard to criminal intelligence information.

XIX. Data Quality Assurance

a. MoSPIN users will make every reasonable effort to ensure that information is derived from reputable sources, is accurate, reasonably up-to-date, and complete, given the circumstances. MoSPIN users will investigate suspected errors and deficiencies to the best of their ability and if authorized, correct deficient information. Under no circumstances will a MoSPIN user use information known to be erroneous, misleading, or unreliable. MIAC analysts will re-evaluate new information that is received into the database. Originating agencies providing data to be entered into MoSPIN remain the owners of the data contributed.

b. MIAC analysts will advise the appropriate data owner if its data is found to be inaccurate, incomplete, or unverifiable.

XX. Collation and Analysis

All MIAC analysts are authorized to seek, accept, retain, and disseminate appropriate information. The information in MoSPIN undergoes analysis in order to enhance public safety, assist in investigations and prosecutions, and provide tactical and strategic intelligence services to authorized recipients.

XXI. Merging Records

a. If, during analysis, information from disparate sources regarding an individual or organization is determined to be of such validity and quantity to lead a reasonable person to conclude that the individuals or organizations are one in the same, the MoSPIN user should contact the MIAC Director, Assistant Directors, or one of the MoSPIN Administrative Analysts to merge the information.

b. 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 match.

XXII. Sharing and Disclosure

Two different groups are established in MoSPIN. The Administrative Group will have access to modify all records and view hidden fields within MoSPIN records. The Administrative Group will consist of the MIAC Director, Assistant Directors, and Administrative Analysts. The

Administrative Analysts will consist of MIAC Intelligence Analysts and MIAC 1000-hour Analysts, who will have access to modify all records. The User Group will consist of the MSHP users of MoSPIN. The User Group will have access to all records but will only be allowed to edit their own data. Information inside of MoSPIN will only be verbally disseminated. If information is disseminated, the date, person receiving the information, and the reason for dissemination will be documented within MoSPIN.

XXIII. Security Safeguards

a. Access to the MoSPIN database from outside the facility will only be allowed over secure networks. MoSPIN will store information in such a way that it cannot be accessed, modified, destroyed, or purged by unauthorized personnel.

b. If an individual's personal information retained by MoSPIN is compromised, the MIAC will notify that individual without delay, provided that notification does not compromise an ongoing investigation. The MIAC Director will notify the Criminal Investigation Bureau Commander and request assistance from the Director of the DDCC to provide investigative assistance to ascertain the source of the release of compromised information. If the security breach was directed toward the MoSPIN database, CJIS personnel will be notified in addition to Criminal Investigation Bureau Commander and the DDCC Director.

XXIV. Information Retention and Destruction

MoSPIN retains its own retention and purge mechanism in compliance with 28 CFR, Part 23. Information that has no further investigative, or research value will be destroyed or purged. This task will be accomplished at least every five (5) years unless the information is re-validated.

XXV. Accountability and Enforcement

a. MoSPIN could potentially undergo an independent audit by the Department of Justice.

b. The MIAC's designated privacy oversight committee and Administrative Analysts will annually review and update the provisions of this policy and make appropriate changes in response to changes in the laws, technology, and use of the informational systems.

c. If any MoSPIN personnel or users are found to be non-compliant with the provisions of the MoSPIN Privacy Policy, their access to MoSPIN will be removed.

d. MIAC personnel reserve the right to limit users having access to MoSPIN, and to withhold or suspend service to any user violating the MoSPIN Privacy Policy.

XXVI. Training

MIAC will require all users who have access to MoSPIN, be trained in using MoSPIN, 28 CFR Part 23, and sign the individual user agreement.

Terms and Definitions

The following is a list of primary terms and definitions used throughout this Privacy Policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

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

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

Agency—Agency refers to the Missouri State Highway Patrol and all agencies that access, contribute, and share information in the Missouri State Highway Patrol's justice information system.

Analysis (law enforcement)—The review of information and its comparison to other information to determine the meaning of the data in reference to a criminal investigation or assessment.

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

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

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.

Biometrics—A general term used alternatively to describe a characteristic or a process. (1) As a characteristic: a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. (2) As a process: automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics.

Center—Center refers to the Missouri Information Analysis Center (MIAC) and all participating state agencies of the Missouri Information Analysis Center.

Civil Liberties—Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government

action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring that all individuals 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.

Collect—For purposes of this document, "gather" and "collect" mean the same thing.

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 usernames, 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 loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses or potentially accesses PII for a purpose other than the authorized purpose. The center's response to a data breach may be addressed in state law or agency policy. 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 Internet.
- Unauthorized employee access to certain information.
- Moving such information to computer otherwise accessible from the Internet without proper information security precautions.
- Intentional or unintentional 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. • Transfer of such information to the information systems of a possibly hostile agency or an 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.

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.

Fusion Center—Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[a] collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the State and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners.

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

General Orders- Those orders promulgated by the superintendent of the Missouri State Highway Patrol under the authority of Section 43.120.1 RSMo.

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—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 Sharing Environment (ISE)—In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of SLTT agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration.

Information Quality—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and

context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

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

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

Invasion of Privacy—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 constitution, statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

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

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

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

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

MIAC- The Missouri Information Analysis Center.

Missouri State Highway Patrol- the law enforcement agency established by Chapter 43 RSMo.

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.

Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)—The NSI establishes standardized processes and policies that provide the capability for federal, SLTT, campus, and railroad law enforcement and homeland security agencies to share timely, relevant ISE-SARs through a distributed information sharing system that protects privacy, civil rights, and civil liberties.

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.

Non validated Information—A tips or lead (including a SAR) received by the center that has been determined to be false or inaccurate or otherwise determined to not warrant additional action and/or maintenance.

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

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

Personal Information—Information which 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—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 piece of information is linked or linkable to a specific individual.

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—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 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

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—For the nonintelligence community, protected information is 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. While not within the definition established by the ISE Privacy Guidelines, protection may be extended to other individuals and organizations by internal federal agency policy or regulation.

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

For state, local, and tribal governments, protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution, applicable federal statutes and regulations, such as civil rights laws and 28 CFR, Part 23, applicable state and tribal constitutions, and applicable state, local, and tribal laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion center or other state, local, or tribal agency policy or regulation.

Public—Public includes:

- Any individual 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:

- Any employees of the center or participating entity.
- People or entities, private or governmental, who 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.

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—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 that is under the agency's/center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

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.

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:

- 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, 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.

Superintendent-The person appointed or acting, under the authority of Section 43.030 RSMo, in command of the Missouri State Highway Patrol.

Suspicious Activity—Suspicious activity is 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 pre-operational 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 are they designed to support interagency calls for service. SAR, as used in this policy, shall only be used in conformity with the definition of SAR in Section 610.021 (18)(c), RSMo.

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.

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 sub-category 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.

Unvalidated information—A tip or lead (including a SAR) received by the center that has not yet been reviewed to determine further action or maintenance.

Validated Information—A tip or lead (including a SAR) that has been reviewed and, when appropriate, combined with other information or further vetted and is determined to warrant additional action, such as investigation or dissemination, and/or maintenance as per the applicable record retention policy.

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.

Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans are Protected in the Development and Use of the Information Sharing Environment ISE*

I. Background and Applicability.

a. Background. Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE). Section 1 of Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, provides that, "[t]o the maximum extent consistent with applicable law, agencies shall … give the highest priority to … the interchange of terrorism information among agencies … [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities …." These Guidelines implement the requirements under the IRTPA and EO 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.

b. Applicability. These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

c. **Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act**—This act broadly affects U.S. terrorism law and applies directly to the federal government. It establishes the Director of National Intelligence, the National Counterterrorism Center, and the Privacy and Civil Liberties Oversight Board. Of importance to SLTT agencies, IRTPA establishes the Information Sharing Environment (ISE) (see Appendix A, Glossary of Terms and Definitions) for the sharing of terrorism-related information at all levels of government, with private agencies, and with foreign partners.

II. Compliance with Laws.

a. General. In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.

b. Rules Assessment. Each agency shall implement an ongoing process for identifying and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

i. only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and
ii. ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.

c. Changes. If, as part of its rule's assessment process, an agency:
i. identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate, develop policies and procedures to provide protections that address that issue;

ii. identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction;

iii. identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect information privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review.

III. Purpose Specification

Protected information should be shared through the ISE only if it is terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below). Each agency shall adopt internal policies and procedures requiring it to ensure that the agency's access to and use of protected information available through the ISE is consistent with the authorized purpose of the ISE.

IV. Identification of Protected Information to be Shared through the ISE.

a. Identification and Prior Review. In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance with Laws) and Section 3 (Purpose Specification), each agency shall identify its data holdings that contain protected information to be shared through the ISE, and shall put in place such mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to these Guidelines before it is made available to the ISE.

b. Notice Mechanisms. Consistent with guidance and standards to be issued for the ISE, each agency shall put in place a mechanism for enabling ISE participants to determine the nature of the protected information that the agency is making available to the ISE, so that such participants can handle the information in accordance with applicable legal requirements. Specifically, such a mechanism will, to the extent reasonably feasible and consistent with the agency's legal authorities and mission requirements, allow for ISE participants to determine whether:

i. the information pertains to a United States citizen or lawful permanent resident;
ii. the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and
iii. there are limitations on the reliability or accuracy of the information.

V. Data Quality.

a. Accuracy. Each agency shall adopt and implement procedures, as appropriate, to facilitate the prevention, identification, and correction of any errors in protected information with the objective of ensuring that such information is accurate and has not erroneously been shared through the ISE.

b. Notice of Errors. Each agency, consistent with its legal authorities and mission requirements, shall ensure that when it determines that protected information originating from another agency may be erroneous, includes incorrectly merged information, or lacks adequate context such that the rights of the individual may be affected, the potential error or deficiency will be communicated in writing to the other agency's ISE privacy official (the ISE privacy officials are described in section 12 below).

c. Procedures. Each agency, consistent with its legal authorities and mission requirements, shall adopt and implement policies and procedures with respect to the ISE requiring the agency to:

i. take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;
ii. investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and

iii. retain protected information only so long as it is relevant and timely for appropriate use by the agency, and update, delete, or refrain from using protected information that is outdated or otherwise irrelevant for such use.

VI. Data Security

Each agency shall use appropriate physical, technical, and administrative measures to safeguard protected information shared through the ISE from unauthorized access, disclosure, modification, use, or destruction.

VII. Accountability, Enforcement and Audit.

a. Procedures. Each agency shall modify existing policies and procedures or adopt new ones as appropriate, requiring the agency to:

   i. have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;
   ii. provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies;
   iii. cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and
   iv. designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

b. Audit. Each agency shall implement adequate review and audit mechanisms to enable the agency's ISE privacy official and other authorized officials to verify that the agency and its personnel are complying with these Guidelines in the development and use of the ISE.

VIII. Redress

To the extent consistent with its legal authorities and mission requirements, each agency shall, with respect to its participation in the development and use of the ISE, put in place internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

IX. Execution, Training, and Technology.

a. Execution. The ISE privacy official shall be responsible for ensuring that protections are implemented as appropriate through efforts such as training, business process changes, and system designs.

b. Training. Each agency shall develop an ongoing training program in the implementation of these Guidelines and shall provide such training to agency personnel participating in the development and use of the ISE.

c. Technology. Where reasonably feasible, and consistent with standards and procedures established for the ISE, each agency shall consider and implement, as appropriate, privacy enhancing technologies including, but not limited to, permissioning systems, hashing, data anonymization, immutable audit logs, and authentication.

X. Awareness

Each agency shall take steps to facilitate appropriate public awareness of its policies and procedures for implementing these Guidelines.

XI. Non-Federal Entities

Consistent with any standards and procedures that may be issued to govern participation in the ISE by State, tribal, and local governments and private sector entities, the agencies and the PM-ISE will work with non-Federal entities seeking to access protected information through the ISE to ensure that such non-Federal entities develop and implement appropriate policies and procedures that provide protections that are at least as comprehensive as those contained in these Guidelines.

XII. Governance.

a. ISE Privacy Officials. Each agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or executive order, or as otherwise identified in response to OMB Memorandum M-05-08 dated February 11, 2005), shall directly oversee the agency's implementation of and compliance with these Guidelines (the "ISE privacy official"). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency. The ISE privacy official role may be delegated to separate components within an agency, such that there could be multiple ISE privacy officials within one executive department. The ISE privacy official shall be responsible for ensuring that:

   i. the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these Guidelines, and
   ii. changes are made as necessary. The ISE privacy official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's senior ISE official.

b. ISE Privacy Guidelines Committee. All agencies will abide by these Guidelines in their participation in the ISE. The PM shall establish a standing "ISE Privacy Guidelines Committee" to provide ongoing guidance on the implementation of these Guidelines, so that, among other things, agencies follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an inter-agency basis. The ISE Privacy Guidelines Committee is not intended to replace legal or policy guidance mechanisms established by law, executive order, or as part of the ISE, and will as appropriate work through or in consultation with such other mechanisms. The ISE Privacy Guidelines Committee shall be chaired by the PM or a senior official designated by the PM and will consist of the ISE privacy officials of each member of the Information Sharing Council. If an issue cannot be resolved by the ISE Privacy Guidelines Committee, the PM will address the issue through the established ISE governance

process. The ISE Privacy Guidelines Committee should request legal or policy guidance on questions relating to the implementation of these Guidelines from those agencies having responsibility or authorities for issuing guidance on such questions; any such requested guidance shall be provided promptly by the appropriate agencies. As the ISE governance process evolves, if a different entity is established or identified that could more effectively perform the functions of the ISE Privacy Guidelines Committee, the ISE Privacy Guidelines Committee structure shall be modified by the PM through such consultation and coordination as may be required by the ISE governance process, to ensure the functions and responsibilities of the ISE Privacy Guidelines Committee remain priorities fully integrated into the overall ISE governance process.

c. Privacy and Civil Liberties Oversight Board. The Privacy and Civil Liberties Oversight Board (PCLOB) should be consulted for ongoing advice regarding the protection of privacy and civil liberties in agencies' development and use of the ISE. To facilitate the performance of the PCLOB's duties, the ISE Privacy Guidelines Committee will serve as a mechanism for the PCLOB to obtain information from agencies and to provide advice and guidance consistent with the PCLOB's statutory responsibilities. Accordingly, the ISE Privacy Guidelines Committee should work in consultation with the PCLOB, whose members may attend Committee meetings, provide advice, and review and comment on guidance as appropriate.

d. ISE Privacy Protection Policy. Each agency shall develop and implement a written ISE privacy protection policy that sets forth the mechanisms, policies, and procedures its personnel will follow in implementing these Guidelines. Agencies should consult with the ISE Privacy Guidelines Committee as appropriate in the development and implementation of such policy.

XIII. General Provisions.

a. Definitions.

i. The term "agency" has the meaning set forth for the term "executive agency" in section 105 of title 5, United States Code, but includes the Postal Rate Commission and the United States Postal Service and excludes the Government Accountability Office.
ii. The term "protected information" has the meaning set forth for such term in paragraph 1(b) of these Guidelines.
iii. The terms "terrorism information," "homeland security information," and "law enforcement information" are defined as follows:

Terrorism information," consistent with section 1016(a)(4) of IRTPA means all relating to:

1. the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism,

2. threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations,
3. communications of or by such groups or individuals, or
4. groups or individuals reasonably believed to be assisting or associated with such groups or individuals. "Homeland security information," as derived from section 482(f)(1) of the Homeland Security Act of 2002, means any information possessed by a Federal, State, local, or tribal agency that relates to:

    a. a threat of terrorist activity,
    b. the ability to prevent, interdict, or disrupt terrorist activity,
    c. the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization, or
    d. a planned or actual response to a terrorist act. "Law enforcement information" for the purposes of the ISE means any information obtained by or of interest to a law enforcement agency or official that is:

        i. related to terrorism or the security of our homeland and
        ii. 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.

b. The treatment of information as "protected information" under these Guidelines does not by itself establish that the individual or entity to which such information pertains does in fact have information privacy or other legal rights with respect to such information.

c. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide the cooperation, assistance, and information necessary for the implementation of these Guidelines.

d. These Guidelines:

i. shall be implemented in a manner consistent with applicable laws and executive orders, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;
ii. shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;
iii. shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and
iv. are intended only to improve the internal management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies.

Fair Information Practice Principles

I. **Fair Information Practice Principles (FIPPs)** are a set of internationally recognized principles that inform information privacy policies within both government and the private sector.

a. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into data privacy laws, policies, and governance documents around the world. For example, the core elements of the FIPPs can be found:

i. At the heart of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.16
ii. Mirrored in many states' laws and in fusion centers' privacy policies.
iii. In the ISO/IEC 29100 Privacy Framework, which has been adopted by numerous foreign countries and international organizations.

b. The following formulation of the FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).17 Note, however, that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy.

II. **Purpose Specification**—Agencies should specifically articulate the authority that permits the collection of PII. The purpose(s) for which PII is collected should be specified at the time of data collection. Subsequent use of this data should be limited to the original purpose for which the PII was collected (or other purposes compatible with the original collection purpose).

Implementing the Purpose Specification Principle—Agencies are bound by specific constitutional and statutory authorities that circumscribe their ability to collect PII. The following are examples of ways agencies may implement this principle:

i. Ensure that a valid lawful purpose exists and is documented for all collection of PII.
ii. Include the source and authority for the data so that access restrictions can be applied.
iii. Upon receipt of data containing PII from third parties, if possible, identify the purpose for which it was collected initially, and limit agency use to only those uses compatible with the original purpose supporting collection.
iv. Ensure that metadata or other tags are associated with the data as it is shared.
v. Institute a two-individual review and approval process to consider any Privacy Act or other legal or policy limitation before permitting use or sharing of data for purposes other than that for which it was collected.

III. **Data Quality/Integrity**—PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date. Implementing the Data Quality/Integrity Principle—One important way to minimize potential downstream P/CRCL concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:

a. Properly labeling PII. 16 5 U.S.C. § 552a. 17 6 U.S.C. § 142. Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0 55
b. Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with PII on U.S. individuals and others, regardless of nationality).
c. Instituting a source verification procedure to ensure reporting is based only on authorized data.
d. Reconciling and updating PII whenever new relevant information is collected.

e. Developing a protocol for ensuring data corrections are passed to those entities with which information has been shared.
f. Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate or has been expunged.

IV. **Collection Limitation/Data Minimization**—PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose. Implementing the Collection Limitation/Data Minimization Principle—Collection limitation may be implemented by:

a. Designing a data storage system to pull data for review and then, if appropriate, automatically purging data after the specified retention period has been reached.
b. Limiting data field elements to only those that are relevant.
c. Ensuring that all distributed reports and products contain only that PII that is relevant and necessary (nothing extraneous or superfluous).
d. Ensuring that all shared information with PII meets required thresholds for sharing, such as reasonable suspicion.

V. **Use Limitation**—PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law. Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles such as "authorized access." Use limitation may be implemented by:

a. Limiting users of data to those with credential-based access.
b. Requiring that justifications be entered, and logs maintained for all queries with sensitive PII and that an internal review process of those logs takes place at specified intervals.
c. Requiring senior analysts to review all reports that use PII before dissemination to ensure (a) that PII is relevant and necessary and (b) that the recipient is authorized to receive the information in the performance of an authorized activity.
d. Prior to sharing information, verify that partners have a lawful purpose for requesting information.
e. Creating multiple use-based distribution lists and restricting distribution to those authorized to receive the information.

VI. **Security/Safeguards**—Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure. Implementing the Security/Safeguards Principle—This principle can be implemented by:

a. Maintaining up-to-date technology for network security.
b. Ensuring that access to data systems requires that users meet certain training and/or vetting standards and that such access is documented and auditable.
c. Ensuring that physical security measures are in place, such as requiring an identification card, credentials, and/or passcode for data access; disabling computers' USB ports; and implementing firewalls to prevent access to commercial e-mail or messaging services.
d. Implementing a protocol with technical and manual safeguards to ensure the accuracy and completeness of data system purges when records are deleted at the end of their retention period.
e. Ensuring that data system purge protocols include complete record deletion on all backup systems.
f. Transitioning older repositories into more modern systems to improve access controls. Fusion
g. Masking data so that it is viewable only to authorized users.
h. Maintaining an audit log to record when information is accessed and by whom for review by senior staff at specified intervals.

i. Requiring authorized users to sign nondisclosure agreements.

VII. **Accountability/Audit**—Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII. Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

a. Ensuring that upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
b. Conducting effective orientation and periodic refresher training, including P/CRCL protections, for all individuals handling PII.
c. Tailoring training to specific job functions, database access, or data source/storage requirements.
d. Conducting regular audits of all systems in which records are kept ensuring compliance with the P/CRCL policies and all legal requirements.
e. Following a privacy incident handling procedure for any data breaches or policy violations.
f. Denying database access to individuals until they have completed mandatory systems access training (including training for handling of PII), show a mission need for access, and have any necessary clearances.
g. Developing targeted and consistent corrective actions whenever noncompliance is found.

VIII. **Openness/Transparency**—To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the P/CRCL policy, and contact information for data corrections and complaints. Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:

a. Providing reports to an internal or external oversight body concerned with P/CRCL issues, including P/CRCL audit results.
b. Publishing the P/CRCL policy and redress procedures.
c. Meeting with community groups through initiatives or through other opportunities to explain the agency's mission and P/CRCL protections.
d. Responding in the fullest way possible to freedom of information and/or sunshine requests and fully explaining any denial of information requests from the public.
e. Conducting and publishing Privacy Impact Assessments (PIAs) in advance of implementing any new technologies that affect PII, thereby demonstrating that P/CRCL issues have been considered and addressed.

IX. **Individual Participation**—To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII. Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:

a. Collecting information directly from the individual, to the extent possible and practical.
b. Providing the individual with the ability to find out whether an agency maintains a record relating to him or her and, if not (i.e., access and/or correction is denied), then providing the individual with notice as to why the denial was made and how to challenge such a denial.
c. Putting in place a mechanism by which an individual is able to prevent information about him or her that was obtained for one purpose from being used for other purposes without his or her knowledge.

INDIVIDUAL USER AGREEMENT

The Missouri State Highway Patrol (MSHP) authorizes:

(Name of User, Troop)

herein referred to as User, access to the Missouri Statewide Police Intelligence Network (MoSPIN) database.

1. This agreement will also verify that the user agrees to and understands that intelligence information provided by the user can be shared with other law enforcement agencies.

2. The user agrees that their information can be used to participate in any national intelligence sharing project deemed appropriate by the Missouri State Highway Patrol. Such projects include the National Virtual Pointer System (NVPS). This target deconfliction information sharing initiative was developed jointly by the High Intensity Drug Trafficking Area (HIDTA), the National Law Enforcement Telecommunication System (NLETS), the Regional Information Sharing System (RISS), the Drug Enforcement Administration (DEA), and the Missouri Statewide Police Intelligence Network (MoSPIN). The NVPS connectivity enables a single entry from NDPIX, HIDTA, MoSPIN or RISS to access all participating pointer deconfliction databases.

3. This agreement will also verify that the user is complying with 28 Code of Federal Regulations (CFR), Part 23. The purpose of 28 CFR Part 23 is to ensure that all federally funded criminal intelligence systems are utilized in conformance with the protection of the privacy and rights of individuals. (See enclosed 28 CFR, Part 23 guidelines).

4.The user agrees to comply with the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 E.S.C. 2510-2520, 2701-2709, and 3121-3125.

5. In addition, this agreement will verify that the user is complying with the MoSPIN Privacy, Civil Liberties, and Civil Rights Policy. This policy ensures the privacy and constitutional rights of individuals are maintained. (See enclosed MoSPIN Privacy, Civil Liberties, and Civil Rights Policy).

Signature of User: _____

Date: _____