# Missouri Information Analysis Center (MIAC)

# Privacy, Civil Liberties, and Civil Rights Policy

Approved November 29, 2010
Revised June 22, 2012

# Missouri Information Analysis Center
# MIAC
**Approved November 29, 2010, Revised June 22, 2012**
# Privacy, Civil Liberties, and Civil Rights Policy

## Table of Contents:

## 1. Mission/Purpose

The Missouri Information Analysis Center (MIAC) is tasked with the collection, collation, analysis, and dissemination of information to appropriate agencies and individuals, in an effort to mitigate criminal and terrorist activities and respond to natural and man-made disasters in a way that enhances public safety.

Equally important is our mission to safeguard the privacy, civil rights, and civil liberties of any individual.

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 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 law enforcement and others responsible for public protection. MoSPIN also allows law enforcement to share intelligence information.

The end result is enhancement of the public safety effort and the safeguarding of individual privacy, civil liberties, and civil rights. This detailed policy documents those efforts.

## 2. Scope and Compliance

All MIAC employees, whether full, part-time, or temporarily assigned, will receive, be trained in, and comply with this policy. Internal MIAC and Missouri State Highway Patrol operating policies govern operation and comply with all applicable laws. Agencies and individual users of MIAC work products will comply with applicable sections of this policy and be notified of that requirement as an attachment to the individual work products.

All MIAC users, personnel providing information technology services, and private contractors will be directed to the MIAC website for review of this policy and will comply with all federal and state privacy laws cited in the appendix to this policy.

MIAC will post a copy of this policy for public review and make additional copies available to any interested party, public or private. Applicable laws protecting civil rights, liberties and privacy are as follows:

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.

## 3. Oversight

The MIAC Division Director, or his/her designee, has overall responsibility for MIAC operations and its compliance with this policy.

A MIAC Assistant Director, Senior Analyst or an attorney at law is designated as a “Privacy Officer” and is trained in Privacy Policy standards as outlined by the DHS and ISE* Privacy Guidelines.

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.

The MIAC Division Director, Privacy Officer, or authorized designee will comply with the enforcement standards outlined in section 10 of this policy.

This Privacy Policy is not designed to override the responsibilities of the Superintendent of the Missouri State Highway Patrol 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 Missouri State Highway Patrol.

The MIAC Division Director, Assistant Directors and Privacy Officer act as the agency's Privacy Committee, and are responsible for the development and further modification of this policy, and when necessary, interact with privacy advocacy groups to address issues with MIAC's information collection, retention, and dissemination processes. The Privacy Committee may institute changes in MIAC Privacy Policy upon the advice of the legal counsel and in response to any changes in Missouri State or federal privacy laws, or MSHP General Order.

**4. Information**

MIAC is not an investigative (operational) agency, however in fulfilling its public safety role, MIAC may actively seek, analyze, disseminate and retain information that is based on criminal predicate, reasonably suspected terrorism nexus, or that which negatively impacts public safety.

Such information is sought in the least intrusive way and must be relevant to investigation, prosecution, and/or mitigation of genuine public safety incidents.
In order to provide law enforcement, public safety and other affected agencies with useable strategic intelligence, MIAC may also engage in research toward that end.

Missouri State Highway Patrol Information Systems equipment identifies the user during the log-in process using unique passwords and assigned personal computers.
All MIAC employees will ensure that information is verifiable, collected in a lawful manner, and lawfully disseminated. The limitations on the quality of the information will be noted if a source is of doubtful credibility. MIAC may retain preliminary information such as tips and leads, and suspicious activity, providing the information is arguably of public safety interest. Such information will be disseminated as soon as practical to agencies with a vested public safety/enforcement interest for further investigation.

MIAC will not seek or retain information about individuals or organizations based solely on religious, political, or social views and/or activities. This prohibition also applies to information based solely on race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

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: the name of the originating center, department or agency, component, and subcomponent; the name of the center's justice information system from which the information is disseminated; the date the information was collected and, where feasible, the date its accuracy was last verified; and the title and contact information for the person to whom questions regarding the information should be directed.

Information received by MIAC will be categorized as to its nature, such as whether the information is of general public safety interest, tips and leads, or criminal intelligence.
General public safety information will be routed to the appropriate authorities and may be disseminated to the general public if such disclosure does not compromise an ongoing investigation.

Tips and leads are received through a variety of sources, entered into the audit database for storage, and assessed as to credibility and validity. Those Tips and Leads, if deemed credible, will be routed to the appropriate investigative agencies for further investigation.

Criminal intelligence will be disseminated to appropriate agencies and entry made into the Missouri Statewide Police Intelligence Network (MoSPIN) if MoSPIN 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. All information sought, collected, and disseminated, regarding public safety and criminal (including terrorism) activities is entered into the audit database which provides a log of inquiries and an audit trail. This information may also be entered into MoSPIN if MoSPIN Privacy Policy and 28 CFR Part 23 criteria is met. Upon entry into the audit database, analysts are required to make indication as to the type of investigation/incident, the protection of sources of information, status and sensitivity of an ongoing investigation, and privacy protection legally required due to the individual's status as a child, a sex abuse victim, a resident of a substance abuse/mental health treatment program or a resident of a domestic abuse shelter for ISE*authorized users.

Dissemination of any type of information will be based on a "need/right to know."

In the event information pertains to particular classes of citizens or protected persons MIAC will indicate to the recipient that privacy protection is legally required due to the individual's status as a child, a sexual abuse victim, a resident of a substance abuse/mental health treatment program, or a resident of a domestic abuse shelter. MIAC will identify and review protected information prior to sharing that information through the ISE*. MIAC will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

During receipt, storage, or dissemination of information, MIAC personnel will assess the information for sensitivity, evaluate to determine its credibility/validity, accuracy and completeness, label the information as either unsubstantiated/uncorroborated if the validation or reliability is uncertain, and document the information received/disseminated.

As vetted employees of the Missouri State Highway Patrol, MIAC analysts are credentialed to access law enforcement sensitive information. Disclosure of law enforcement sensitive information will only be made to those agencies/individuals employed by other law enforcement agencies, or those with a responsibility for criminal investigations. Tips and Leads information will be clearly labeled as such and be retained long enough to validate the source and reliability of the information. Tips and Leads information will be afforded the same level of physical and technical security as that given to information containing reasonable suspicion.

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. MIAC will comply with and adhere to the following regulations and guidelines:

1. 28 CFR Part 23, regarding criminal intelligence information;

2. Missouri state statutes Chapters 610 and 407 RSMo;

3. Missouri State Highway Patrol General Orders and MIAC Division policy;

4. ISE Privacy Guidelines as outlined in Appendix B.

In providing information, MIAC 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.

MIAC users are required to review the MIAC Privacy Policy online, and additional written non-disclosure agreements are required on a case-by-case basis. MIAC analysts are required to acknowledge receipt of and understanding of the MIAC Privacy Policy in writing.

MIAC analysts will not knowingly seek, receive, accept, disseminate, or retain information from an entity that is legally prohibited from obtaining or disclosing that information, or who has illegally gathered the information.

**5. Quality Assurance**

MIAC contracts with reputable commercial databases that provide an assurance that their methods for gathering personal information in compliance with all applicable laws, and whose methods are not based on misleading or questionable collection practices. MIAC 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. Analysts will investigate suspected errors and deficiencies to the best of their ability, notify the MIAC Division Director and Privacy Officer and correct or destroy deficient information. Hard files containing deficient/incorrect information will be redacted, and data storage files purged of such information. Every effort should be made to notify the original owner of the information as to any errors or deficiencies.
Under no circumstances will an analyst use information known to be erroneous, misleading, or unreliable.

MIAC will notify recipient agencies in the most efficient method possible when information previously disseminated is found to be in error or deficient in some way.

**6. Collation and Analysis**

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 Missouri State Highway Patrol standards, and are authorized to seek, accept, retain, and disseminate appropriate Criminal/Public Safety-related information.

Only MIAC Analysts 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.

Suspicious Activity Reports (SARS) will undergo immediate analysis to determine validity and source credibility before further dissemination. In some cases, due to time sensitivity, SARs will be

disseminated immediately to more competent authorities for validation. SARs will be retained in the audit database regardless of initial validation.
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, an analyst may merge the information. If the information from disparate sources is only a partial match, the recipient agency will be notified of that fact. If any additional information impacts the validity and reliability of the original information the information retained may be reevaluated.

**7. Inquiry, Complaints, and Redress**

Inquiries to MIAC will be screened by the receiving analyst to ensure the requestor is credentialed for the information, and authorized to have access for legitimate law enforcement and public safety purposes. Such assurance may be initiated by re-contacting the requesting agency or through verification from a third party. In certain cases, when specified by the originator, approval from the originator of the information may be needed before dissemination of that information.

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 for 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) or Chapter 32 (State Revenue Laws).

MIAC personnel will not sell, publish, exchange, or disclose information for commercial purposes, or provide information to unauthorized persons. Permission to distribute Law Enforcement Sensitive information to a Non-Law Enforcement public safety entity will be sought from the owner of that information before any release.

Certain other records will not be disclosed to the public:

1. Public records required by law to be kept confidential.

2. Certain investigative records of law enforcement agencies.

3. Certain public records, the release of which could aid in the planning and commission of a terrorist act. Example: Critical Infrastructure information, including vulnerability assessments, security planning, proprietary information, and threat assessments.

4. Certain records owned and controlled by another agency without that agency's express permission.

5. Certain records specified in MSHP General Order 82-01-0881

Upon satisfactory verification of identity, an individual is entitled to know of the existence of, and to review information, including that from ISE* sources, about him/her (including that considered ISE* information as described in ISE* Privacy Guidelines based on the Privacy Act of 1974) retained by MIAC as long as such disclosure would not violate 28 CFR Part 23 and RSMo 610 (State Sunshine Laws). These inquiries should be directed to the MIAC Division Director and/or Privacy Officer via

email at miac@mshp.dps.mo.gov or via toll-free number 1-866-362-6422. The individual may obtain a copy of the information for the purpose of challenging its accuracy.

Access to this information will be processed through the Missouri State Highway Patrol's records section and Custodian of Records via the MIAC Division Director and/or Privacy Officer. Both the MIAC Privacy Officer and the Missouri State Highway Patrol's Custodian of Records will maintain documentation of such requests, and responses. Appeals to official MSHP responses are handled by the MIAC Privacy Officer and MSHP Custodian of Records with the assistance of the MSHP legal counsel. The MSHP response to these requests will be within a reasonable time. These types of requests will not be honored if such 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 MIAC does not own, or did not originate the information or if such disclosure would violate 28 CFR Part 23, Chapter 610 RSMo (State Sunshine Laws), or Chapter 32 (State Revenue Laws).

If an individual has complaints or objections as to the accuracy of information retained, the MIAC Division or the MIAC Privacy Officer will inform the individual of complaint reporting/corrections procedure through the MSHP Custodian of Records. If that information originated with another agency, the MIAC Division Director or MIAC Privacy Officer will notify the originating agency, including ISE sources and coordinate complaint/corrections procedure by assisting in the investigation and subsequent correction or removal of the information. To delineate protected information shared through the ISE from other data, 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 make a determination to correct the information, remove the record, or assert a basis for denial. All progress in the redress procedure will be documented.

The individual to whom information has been disclosed will be provided notification of reason for denial in accordance with MSHP General Order 82-01-0881. The individual will also be informed of the appeals process when MIAC or the originating agency has declined to correct the challenged information.

## 8. Security

An Assistant Division Director or Senior Analyst will be designated and trained as the center's security officer and will ensure the center operates in a secure manner free from facility and network intrusion.

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. MIAC does not store risk and vulnerability statements.

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.

If an individual's personal information retained by MIAC is compromised, 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 Division Director will notify the Criminal Investigation Bureau Commander who may request the Division of Drug and Crime Control (DDCC) assign an officer(s) to provide investigative assistance to identify the source of the leaked information. If the

security breach was directed toward MIAC databases, Information Systems Division personnel will be notified in addition to Criminal Investigation Bureau Commander.

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 MIAC must provide adequate identification and a valid need to visit, and any maintenance or custodial personnel must be escorted.

**9. Retention, Purge, and Destruction**

The Missouri Statewide Police Intelligence Network (MoSPIN) is the official and sole intelligence database utilized by MIAC personnel and administered by MIAC. MoSPIN maintains its own retention and purge mechanism in compliance with 28 CFR, Part 23. A separate MoSPIN Privacy Policy is in place for MoSPIN and is attached to this policy and listed under Appendix D. Purge dates are electronically set by the MoSPIN system on an ongoing five year basis with purge notification provided to both the MoSPIN Director/Analyst and the originating agency. The MoSPIN system provides automatic notification of upcoming purge dates to all MoSPIN-enabled analysts for each intelligence entry based on the original entry date.

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 5 years unless the information is re-validated. All personal identifying information retained in the audit database will be purged every 3 years but the other information will be retained for statistical purposes. Information requiring further analysis, even though not validated, is retained in the audit database for statistical and administrative purposes only up to the 5 year anniversary. Information which is validated is made available to the MoSPIN system.

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 training 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.

**10. Accountability and Enforcement**

MIAC will remain open and accountable to the public regarding information collection practices.

A MIAC Privacy Policy is posted to its public website located at www.miacx.org. Written documentation of the MIAC Privacy Policy is available to those who do not have Internet access.

The MIAC Division Director with guidance from the Missouri State Highway Patrol 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.

MIAC undergoes independent audits by both the Missouri State Highway Patrol's Criminal Justice Information Services Division and the Research and Development Division in their Staff Inspections. MoSPIN audits are conducted on a daily basis and audit database audits occur randomly.

The MIAC Privacy Officer will annually review and, if, suggest to the MIAC Division Director and the other members of the Privacy Committee, updates to the provisions of this policy. The suggested

changes may be in response to changes in the laws, technology, and use of the informational systems. Changes in public expectations may be considered in any review of this policy.

If any MIAC personnel are found to be non-compliant with the provisions of the MIAC Privacy Policy, the MIAC Division Director will be notified immediately and will immediately notify the Criminal Investigation Bureau Commander and suspend access to MIAC Databases, pending a thorough investigation. Further punitive actions will be taken in accordance with Missouri State Highway Patrol General Orders, MIAC Division Special Orders, or other administrative rules.

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 MIAC to refer the matter to appropriate law enforcement authorities for investigation and possible criminal prosecution.

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 ensure user identification and identify information accessed. All users who access MoSPIN information agree to abide by the MoSPIN Privacy Policy. MIAC does not provide electronic access to any databases other than the MoSPIN system. Periodic audits of the MoSPIN system assess and evaluate user compliance with MoSPIN policy. Violations of MoSPIN policy result in denial of further access.

## 11. Training

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 Missouri State Highway Patrol staff attorney, 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. MIAC Privacy Policy training will include, but not be limited to the following: Purposes of the Privacy Policy, the intent of all provisions of the policy, the application of policy in day-to-day work, and the potential impact of user abuse of information systems.

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.

ISE is the Information Sharing Environment-The agencies, policies, procedure, and technologies linked to facilitate terrorism and homeland security information sharing.

Appendix A

## 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.

**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 user names 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. See Authentication.

**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 citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

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

**Confidentiality—**Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

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

**Criminal Intelligence Information—**Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR, Part 23.

**Data—**Inert symbols, signs, descriptions, or measures; elements of information.

**Data Breach—**The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media such as computer tapes, hard drives, or laptop computers containing such media upon which such information is stored unencrypted, posting such information on the world wide web or on a computer otherwise accessible from the Internet without proper information security precautions, transfer of such information to a system which is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail, or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

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

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

**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.

**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.

**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 pieces of information can be:

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

**Persons—**Executive Order 12333 defines "United States persons" as United States citizens, aliens known by the intelligence agency 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 person and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information;
- Media organizations; and

- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:
- Employees of the agency;
- People or entities, private or governmental, who assist the agency/center in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

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

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

**Redress—**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:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

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

With regard to the 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, 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.

**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.

**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.

## Appendix B

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*

1. 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.

2. 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 rules 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. Awareness.

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

11. 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.

12. 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.

13. 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:

(A) 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,

(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations,

(C) communications of or by such groups or individuals, or

(D) 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:

(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.

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,

## Appendix C

**Section 1016 (d) Intelligence Reform and Terrorism Prevention Act of 2004**

**SEC. 1016. INFORMATION SHARING.**

(a) DEFINITIONS.—In this section:

(1) INFORMATION SHARING COUNCIL.—The term ‘‘Information Sharing Council’’ means the Information Systems Council established by Executive Order 13356, or any successor body designated by the President, and referred to under subsection(g).
6 USC 485.
Applicability.
Applicability.

PUBLIC LAW 108–458—DEC. 17, 2004 118 STAT. 3665

(2) INFORMATION SHARING ENVIRONMENT; ISE.—The terms ‘‘information sharing environment’’ and ‘‘ISE’’ mean an approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section.

(3) PROGRAM MANAGER.—The term ‘‘program manager’’ means the program manager designated under subsection (f).

(4) TERRORISM INFORMATION.—The term ‘‘terrorism information’’ means all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to—

(A) 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;

(B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations;

(C) communications of or by such groups or individuals; or

(D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

(b) INFORMATION SHARING ENVIRONMENT.

(1) ESTABLISHMENT. The President shall:
(A) create an information sharing environment for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties;

(B) designate the organizational and management structures that will be used to operate and manage the ISE; and

(C) determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.

(2) ATTRIBUTES.—The President shall, through the structures described in subparagraphs (B) and (C) of paragraph

(1), ensure that the ISE provides and facilitates the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. The President shall, to the greatest extent practicable, ensure that the ISE provides the functional equivalent of, or otherwise supports, a decentralized, distributed, and coordinated environment that:

(A) connects existing systems, where appropriate, provides no single points of failure, and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;

(B) ensures direct and continuous online electronic access to information;

(C) facilitates the availability of information in a form and manner that facilitates its use in analysis, investigations and operations;

(D) builds upon existing systems capabilities currently in use across the Government;

118 STAT. 3666 PUBLIC LAW 108–458—DEC. 17, 2004

(E) employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;

(F) facilitates the sharing of information at and across all levels of security;

(G) provides directory services, or the functional equivalent, for locating people and information;

(H) incorporates protections for individuals' privacy and civil liberties; and

(I) incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication, and access controls.
(c) PRELIMINARY REPORT.—Not later than 180 days after the date of the enactment of this Act, the program manager shall, in consultation with the Information Sharing Council:

(1) submit to the President and Congress a description of the technological, legal, and policy issues presented by the creation of the ISE, and the way in which these issues will be addressed;

(2) establish an initial capability to provide electronic directory services, or the functional equivalent, to assist in locating in the Federal Government intelligence and terrorism information and people with relevant knowledge about intelligence and terrorism information; and

(3) conduct a review of relevant current Federal agency capabilities, databases, and systems for sharing information.

(d) GUIDELINES AND REQUIREMENTS.—As soon as possible, but in no event later than 270 days after the date of the enactment of this Act, the President shall—

(1) leverage all ongoing efforts consistent with establishing the ISE and issue guidelines for acquiring, accessing, sharing, and using information, including guidelines to ensure that information is provided in its most shareable form, such as by using tearlines to separate out data from the sources and methods by which the data are obtained;

(2) in consultation with the Privacy and Civil Liberties Oversight Board established under section 1061, issue guidelines that:

(A) protect privacy and civil liberties in the development and use of the ISE; and

(B) shall be made public, unless nondisclosure is clearly necessary to protect national security; and

(3) require the heads of Federal departments and agencies to promote a culture of information sharing by—

(A) reducing disincentives to information sharing, including over-classification of information and unnecessary requirements for originator approval, consistent with applicable laws and regulations; and

(B) providing affirmative incentives for information sharing.

(e) IMPLEMENTATION PLAN REPORT.—Not later than one year after the date of the enactment of this Act, the President shall, with the assistance of the program manager, submit to Congress a report containing an implementation plan for the ISE. The report shall include the following:
(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.

PUBLIC LAW 108–458—DEC. 17, 2004 118 STAT. 3667

(2) A description of the impact on enterprise architectures of participating agencies.

(3) A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE.

(5) The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized.

(6) Objective, systemwide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.

(9) The recommendations of the program manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with:

(A) the authority of the Director of National Intelligence under this title, and the amendments made by this title, to set standards for information sharing throughout the intelligence community; and

(B) the authority of the Secretary of Homeland Security and the Attorney General, and the role of the Department of Homeland Security and the Attorney General, in coordinating with State, local, and tribal officials and the private sector.

(11) The recommendations of the program manager, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of program manager should continue to remain in existence.

(f) PROGRAM MANAGER.—

(1) DESIGNATION.—Not later than 120 days after the date of the enactment of this Act, with notification to Congress, the President shall designate an individual as the program manager responsible for information sharing across the Federal Government. The individual designated as the program manager shall serve as program manager during the two-year period beginning on the date of designation under this paragraph unless sooner removed from service and replaced by the President (at the President's sole discretion). The program manager shall have and exercise government wide authority.

(2) DUTIES AND RESPONSIBILITIES.

(A) IN GENERAL.—The program manager shall, in consultation with the Information Sharing Council

118 STAT. 3668 PUBLIC LAW 108–458—DEC. 17, 2004

(i) plan for and oversee the implementation of, and manage, the ISE;

(ii) assist in the development of policies, procedures, guidelines, rules, and standards as appropriate to foster the development and proper operation of the ISE; and

(iii) assist, monitor, and assess the implementation of the ISE by Federal departments and agencies to ensure adequate progress, technological consistency and policy compliance; and regularly report the findings to Congress.

(B) CONTENT OF POLICIES, PROCEDURES, GUIDELINES,
RULES, AND STANDARDS.—The policies, procedures, guidelines, rules, and standards under subparagraph (A)(ii) shall—

(i) take into account the varying missions and security requirements of agencies participating in the ISE;

(ii) address development, implementation, and oversight of technical standards and requirements;

(iii) take into account ongoing and planned efforts that support development, implementation and management of the ISE;

(iv) address and facilitate information sharing between and among departments and agencies of the intelligence community, the Department of Defense, the homeland security community and the law enforcement community;

(v) address and facilitate information sharing between Federal departments and agencies and State, tribal, and local governments;

(vi) address and facilitate, as appropriate, information sharing between Federal departments and agencies and the private sector;

(vii) address and facilitate, as appropriate, information sharing between Federal departments and agencies with foreign partners and allies; and

(viii) ensure the protection of privacy and civil liberties.

(g) INFORMATION SHARING COUNCIL.

(1) ESTABLISHMENT.—There is established an Information Sharing Council that shall assist the President and the program manager in their duties under this section. The Information Sharing Council shall serve during the two-year period beginning on the date of the initial designation of the program manager by the President under subsection (f)(1), unless sooner removed from service and replaced by the President (at the sole discretion of the President) with a successor body.

(2) SPECIFIC DUTIES.—In assisting the President and the program manager in their duties under this section, the Information Sharing Council shall

(A) advise the President and the program manager in developing policies, procedures, guidelines, roles, and standards necessary to establish, implement, and maintain the ISE;

(B) work to ensure coordination among the Federal departments and agencies participating in the ISE in the establishment, implementation, and maintenance of the
ISE;

PUBLIC LAW 108–458—DEC. 17, 2004 118 STAT. 3669

(C) identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used by Federal departments and agencies to share information, and recommend, as appropriate, the redirection of existing resources to support the ISE;

(D) identify gaps, if any, between existing technologies, programs and systems used by Federal departments and agencies to share information and the parameters of the proposed information sharing environment;

(E) recommend solutions to address any gaps identified under subparagraph (D);

(F) recommend means by which the ISE can be extended to allow interchange of information between Federal departments and agencies and appropriate authorities of State and local governments; and

(G) recommend whether or not, and by which means, the ISE should be expanded so as to allow future expansion encompassing other relevant categories of information.
(3) CONSULTATION.—In performing its duties, the Information Sharing Council shall consider input from persons and entities outside the Federal Government having significant experience and expertise in policy, technical matters, and operational matters relating to the ISE.

(4) INAPPLICABILITY OF FEDERAL ADVISORY COMMITTEE
ACT.—The Information Sharing Council shall not be subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App.).

(h) PERFORMANCE MANAGEMENT REPORTS.

(1) IN GENERAL.—Not later than two years after the date of the enactment of this Act, and annually thereafter, the President shall submit to Congress a report on the state of
the ISE and of information sharing across the Federal Government.

(2) CONTENT.—Each report under this subsection shall include—

(A) a progress report on the extent to which the ISE has been implemented, including how the ISE has fared on the performance measures and whether the performance
goals set in the preceding year have been met;

(B) objective system-wide performance goals for the following year;

(C) an accounting of how much was spent on the ISE in the preceding year;

(D) actions taken to ensure that procurement of and investments in systems and technology are consistent with the implementation plan for the ISE;

(E) the extent to which all terrorism watch lists are available for combined searching in real time through the ISE and whether there are consistent standards for placing individuals on, and removing individuals from, the watch lists, including the availability of processes for correcting errors;

(F) the extent to which State, tribal, and local officials are participating in the ISE;

118 STAT. 3670 PUBLIC LAW 108–458—DEC. 17, 2004

(G) the extent to which private sector data, including information from owners and operators of critical infrastructure, is incorporated in the ISE, and the extent to which individuals and entities outside the government are receiving information through the ISE;

(H) the measures taken by the Federal government to ensure the accuracy of information in the ISE, in particular the accuracy of information about individuals;

(I) an assessment of the privacy and civil liberties protections of the ISE, including actions taken in the preceding year to implement or enforce privacy and civil liberties protections; and

(J) an assessment of the security protections used in the ISE.

(i) AGENCY RESPONSIBILITIES.—The head of each department or agency that possesses or uses intelligence or terrorism information, operates a system in the ISE, or otherwise participates (or expects to participate) in the ISE shall—

(1) ensure full department or agency compliance with information sharing policies, procedures, guidelines, rules, and standards established under subsections (b) and (f);

(2) ensure the provision of adequate resources for systems and activities supporting operation of and participation in the ISE;

(3) ensure full department or agency cooperation in the development of the ISE to implement governmentwide information sharing; and

(4) submit, at the request of the President or the program manager, any reports on the implementation of the requirements of the ISE within such department or agency.

(j) AUTHORIZATION OF APPROPRIATIONS.—There is authorized to be appropriated to carry out this section $20,000,000 for each of fiscal years 2005 and 2006.

**Appendix D**

# Missouri Information Analysis Center (MIAC)

**Revised and Approved November 29, 2010**

## Missouri Statewide Police Intelligence Network (MoSPIN)

## Privacy, Civil Liberties, and Civil Rights Policy

## Table of Contents:

## 1. Mission/Purpose

The Missouri Information Analysis Center (MIAC) is tasked with the collection, collation, analysis, and dissemination of information to appropriate agencies and individuals, in an effort to mitigate criminal and terrorist activities and respond to natural and man-made disasters in a way that enhances public safety.

Equally important is our mission to safeguard the privacy, civil rights, and civil liberties of any individual.

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 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 law enforcement and others responsible for public protection. MoSPIN also allows law enforcement to share intelligence information.

The end result is enhancement of the public safety effort and the safeguarding of individual privacy, civil liberties, and civil rights. The purposes of this detailed policy is to document those efforts and to assure that MoSPIN is utilized in conformance with the privacy and constitutional rights of individuals.

## 2. 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 MoSPIN. The MoSPIN database will be in compliance with the Privacy Policy concerning the information itcollects, receives, maintains, archives, accesses, or discloses to law enforcement agencies. Agencies requesting access to MoSPIN will sign an Agency User Agreement, attached to this document and listed as Attachment A. 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 a Security Control Card Form, attached to this document and listed as Attachment B that will list the person's name, address and personal data. By signing this form, they agree with the provisions of MoSPIN and this Privacy Policy.

## 3. Oversight

The MIAC Division Director and the MoSPIN Director/Analyst have overall responsibility for MoSPIN operations and 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. MIAC is also responsible for training personnel on the MoSPIN system.

## 4. 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 the political, religious, or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(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. In an multijurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) The MoSPIN database shall not include any criminal intelligence information that has been obtained in violation of any applicable Federal, State, or local law or ordinance.

(e) The MoSPIN database or authorized recipient disseminates 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.

(f) The MoSPIN database disseminates 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 insure against unauthorized access and against intentional or unintentional damage. MoSPIN maintains a record indicating, the reason for viewing a MoSPIN record, and the date each viewing of the record(s) occurred.

(h) The MIAC Division Director, Assistant Director or MoSPIN 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, the credibility, if known, and the 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 MoSPIN database shares information with 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 has reduced the need for duplicate entry regarding subject deconfliction.

(l) The MIAC Division Director, Assistant Director or MoSPIN Analysts assure that the following security requirements are implemented: (1) MoSPIN has adopted effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system; (2) MoSPIN stores information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization; (3) MoSPIN has instituted procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or man-made disaster; (4) 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 (5) 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.

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

1. 28 CFR, Part 23 regarding criminal intelligence information;

2. Criminal Justice Guidelines established by the Department of Justice.

3. State statute and Missouri State Highway Patrol General Orders and MIAC Division Special Orders.

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.

**5. Acquiring and Receiving Information**

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

**6. Quality Assurance**

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. MoSPIN will re-evaluate new information that is received into the database. Originating agencies providing data into MoSPIN remain the owners of the data contributed.

MoSPIN personnel will advise the appropriate data owner if its data is found to be inaccurate, incomplete, or unverifiable.

**7. Collation and Analysis**

If an agency is a member of the Mid-States Organized Crime Information Center (MOCIC), personnel selected by the agency chief can have access to MoSPIN. If the agency does not have access to MOCIC, only sworn officers will have access to MoSPIN. All users are authorized to seek, accept, retain, and disseminate appropriate 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.

**8. Merging Records**

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 Division Director, Assistant Director, or MoSPIN Analyst to merge the information.

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.

**9. Sharing and Disclosure**

Three different groups are set up in MoSPIN. SPIN Level 1 Admin Group will have access to modify all records and view hidden fields within MoSPIN records. The SPIN Level 1 Admin Group will consist of the MoSPIN Director and MoSPIN Analysts. SPIN Level 1 Group will consist of MIAC Criminal Intelligence Analysts and MIAC 1000-hour Analysts, who will have access to modify all records. SPIN Level 2 Group will consist of the agency users of MoSPIN. SPIN Level 2 Group will have access to all records but will only be allowed to edit their own data.

**10. Security Safeguards**

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.

If an individual's personal information retained by MoSPIN is compromised, MIAC will notify that individual without delay, provided that notification does not compromise an ongoing investigation. The MIAC Division Director will notify the Criminal Investigation Bureau Commander and request assistance from the Director of the Division of Drug and Crime Control (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, Information Systems Division personnel will be notified in addition to Criminal Investigation Bureau Commander and the DDCC Commander.

## 11. 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 5 years unless the information is re-validated. Notification may or may not be made to the owner of the information, depending on previous agreements.

## 12. Accountability and Enforcement

MoSPIN undergoes independent audits by the Department of Justice.

MIAC personnel will periodically 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.

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.

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

## 13. Training

MIAC will require all employees who have access to MoSPIN, be trained in using MoSPIN. In addition new users will perform online training regarding 28 CFR, Part 23 and present to the MIAC a certificate of completion. New users will also read and certify they understand and will comply will all provisions of this Privacy Policy.

## APPENDIX E
# AGENCY USER AGREEMENT

1. The Missouri State Highway Patrol (MSHP) authorizes:

_____
(Name of Agency)

herein referred to as Agency, access to the Missouri Statewide Police Intelligence Network (MoSPIN) database. Each agency must have a user agreement signed by the agency director on file, and each individual user must have a completed Security Control Card Form and a User Registration Form on file.

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

3. The agency 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. In the NVPS, responses indicating a possible deconfliction "hit" will be disbursed to your agency by the Missouri State Highway Patrol's Missouri Information Analysis Center.

4. This agreement will also verify that the agency 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.)

5. In addition, this agreement will verify that the agency 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 Agency Director Printed name of Agency Director

_____
Date

# MOSPIN

## Agency Information Form

Agency Name:_____

Agency Mailing Address: _____

_____

_____

Agency County: _____

Agency Telephone Number:_____

Agency Fax Number:_____

Agency E-mail: _____

Agency ORI or Sponsoring Agency ORI: _____

Agency Executive Representative or Appointee:

_____

Please complete the following fields if your agency is a member of MOCIC:

MOCIC Number: _____

MOCIC Contact: _____

**APPENDIX F**

# INDIVIDUAL USER AGREEMENT

1. The Missouri State Highway Patrol (MSHP) authorizes:

_____
(Name of User)

herein referred to as User, access to the Missouri Statewide Police Intelligence Network (MoSPIN) database. Each agency must have an Agency User Agreement signed by the agency director on file, and each individual user must have a User Agreement signed by the user and the agency director on file, along with a completed Security Control Card Form and a User Registration Form on file.

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

3. 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. In the NVPS, responses indicating a possible deconfliction "hit" will be disbursed to your agency by the Missouri State Highway Patrol's Missouri Information Analysis Center.

4. 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.)

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 Signature of Agency Director

_____ _____
Date Date

# MOSPIN

## SECURITY CONTROL CARD APPLICATION and REGISTRATION

This form must be completed to allow dissemination of confidential information from MoSPIN.

Name (First/Middle/Last)_____
Date of Birth: _____
Title: _____
Badge: _____
Secure e-mail address_____

If your agency is a member of MOCIC, please provide a RISS.net e-mail address. OR
If you have a HIDTA.net e-mail address, please provide that address. OR
If your agency is NOT a member of MOCIC, and you do not have a HIDTA e-mail address, please obtain a free LEO.gov
e-mail address. An application for a LEO e-mail account is available upon request. The process takes approximately 10 business days.

Agency: _____
Phone Number: _____
Fax Number: _____

Password:* _____

Passwords must meet the following criteria:
1. Must be at least 8 characters in length
2. Cannot contain all or part of the user's first or last name
3. Contain characters from three of the following four categories
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Number (0 through 9)
- Non-alphanumeric (for example: !, $, #. %)

Four unique personal facts are needed to verify your identity when contacting MoSPIN. These can be anything
from your mother's maiden name to your favorite childhood pet -- facts about yourself that are not common
knowledge nor likely to change. Please provide both the questions and answers.

1.

_____

2.

_____

3. _____

4. _____

Through my association with the Missouri Statewide Police Intelligence Network (MoSPIN), any information
received from MoSPIN is considered confidential and sensitive. I will be responsible for not revealing such
information by any means except in accordance with current MoSPIN security policies.

_____ _____
Applicant Signature Date

_____ _____
Signature of Agency Head Date