OFFICE OF THE GOVERNOR

KENTUCKY OFFICE OF HOMELAND SECURITY

KENTUCKY INTELLIGENCE FUSION CENTER

PRIVACY POLICY

A. Purpose Statement

The Kentucky Intelligence Fusion Center (KIFC) was established to provide timely information sharing and exchange of crime-related information among members of the law enforcement community. The primary focus of the KIFC is the development and dissemination of criminal intelligence information, as well as other lead information for the purpose of supporting law enforcement activities and promoting public safety. The KIFC also collects, maintains and disseminates suspicious activity information for the purpose of protecting critical infrastructure/key resources within the Commonwealth. This process consists of collection, integration, evaluation, analysis and dissemination through established procedures exclusively for law enforcement purposes and in the interest of public safety. The intelligence products and services are made available to law enforcement agencies and other entities contributing to public safety (e.g. Public Health, Emergency Management, Fire Service) throughout the state and country.

The KIFC recognizes the importance of ensuring the protection of individual constitutional rights, civil liberties, civil rights, and privacy interests throughout the criminal investigative and intelligence processes. In recognition of the importance of individual constitutional rights and civil liberties, it shall be the policy of the KIFC to maintain and safeguard the integrity of personal data that may be collected, integrated, evaluated, analyzed or disseminated, in accordance with applicable state and federal laws to include the following appropriate privacy and civil liberties safeguards as outlined in the principles of the Organization for Economic Co-operation and Developments (OECD) Fair Information Principles. The formal adoption of the KIFC Privacy Policy will ensure that the information privacy and other legal rights of individuals and organizations are protected and will serve to protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.

B. Policy Applicability and Legal Compliance

All agencies and individual users, participating in the KIFC, are responsible for compliance with this policy and applicable state and federal laws governing the collection, maintenance, and dissemination of law enforcement intelligence and other investigative information. Participating and contributing agencies are responsible for ensuring that the information submitted to KIFC has been obtained in compliance with applicable state and federal laws and that such information is submitted for the purpose of analysis and dissemination to participating agencies based on legal authority to receive said information; as well as the “need to know”. The Memorandum of Understanding (MOU) between participating agencies and the KIFC contains an express statement of agreement to comply with this Privacy Policy.

The KIFC and participating agencies will abide by daily operating procedures that have been established regarding the collection, verification, storage, maintenance, and sharing of criminal intelligence and other investigative information. (*See Kentucky Intelligence Fusion Center Standard Operating Procedures*). The KIFC will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services and to participating

agencies and individual users and will require written acknowledgement of receipt and written agreement to comply with the terms of this policy. All KIFC personnel are required to attend a Privacy, Civil Rights and Civil Liberties training session. The KIFC Privacy Officer is responsible for coordinating and conducting this training and for completing an annual review of this policy and distributing amendments to KIFC personnel and participating agencies.

All KIFC personnel, participating agency personnel, personnel providing information technology services to the center, contractors, agencies from which KIFC information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties including, but not limited to 28 CFR Part 23, U.S. Constitution, Kentucky Constitution, KRS 61.870 KY Open Records ACT, KRS 61.878 Relating to Exchange of Information between Public Agencies, KRS Chapter 16 and KRS Chapter 39G, and Kentucky State Police Criminal Justice Information Systems Usage Policies (refer to Appendix). KIFC daily operating procedures are in compliance with these laws.

C. Governance and Oversight

The Kentucky Intelligence Fusion Center exists within the Kentucky Office of Homeland Security by way of Statute 39G.050 effective June 25, 2013. The daily operations of the KIFC will be administered by the Fusion Center Director. The Kentucky Office of Homeland Security (KOHS) Fusion Center Operations Coordinator currently serves as the KIFC Privacy Officer. The Fusion Center Director may serve as the Security Officer for the KIFC when necessary. Since neither the Privacy Officer nor Fusion Center Director is a law enforcement officer, the administration of justice systems will be handled by the Commander of Kentucky State Police Intelligence Branch. The oversight of Privacy Policy development, review of Privacy Policy violations, compliance with ISE Privacy Guidelines, and ensuring that enforcement procedures and sanctions outlined in Section N., are adequate and enforced, will be handled by the Privacy Officer, in consultation with the Fusion Center Director, Commander, Kentucky State Police Intelligence Branch, or other designated agency representative. Violations of the Privacy Policy as well as other Standard Operating Procedures of the KIFC will be handled by the designated agency representative (e.g. Kentucky State Police Intelligence Commander, KIFC Director, FBI ASAC, etc.) in accordance with respective participating agency personnel policies. The Fusion Center Director is responsible for Information Collection and retention procedures as well as the Coordination of personnel assigned to the Fusion Center.

The Fusion Center Director is appointed by the Executive Director, KOHS (gubernatorial appointee) with the concurrence of the Governance Board (board). The Privacy Officer is appointed by the Fusion Center Director with the concurrence of the Executive Director. The KIFC Governance Board is the body that oversees the mission of the Fusion Center. The board consists of a representative official from each KIFC participating agency, and conducts all meetings in accordance with applicable state laws.

Fusion Center Director

Keith Rossmiller, Fusion Center Director
Office of the Governor
Kentucky Office of Homeland Security
200 Mero Street
Frankfort, KY 40601
502-564-2081
keith.rossmiller@ky.gov

Privacy Officer

Jason Childers, KIFC Operations Coordinator
Office of the Governor
Kentucky Office of Homeland Security
200 Mero Street
Frankfort, KY 40601
502-564-2081
jason.childers@ky.gov

While the KIFC does not have a Privacy Oversight Committee, the mission of the board is to improve the administration of justice and protect the public by promoting practices and technologies for the secure sharing and distribution of criminal justice information. The board will be vocal and visible in creating and communicating a shared vision regarding information sharing within the justice, public safety, and first-responder communities. The board will work collaboratively and inclusively, bringing together representatives from the entire justice community and related entities, to address and overcome the barriers to justice information sharing across agencies, disciplines, and levels of government. The board will identify and seek solutions to impediments to information sharing and make all recommendations on the basis of increasing public safety. The board promotes the development and implementation of standards that facilitate seamless exchange of information among justice and related systems. The board provides information that supports sound business decisions for the planning, design, and procurement of cost-effective, interoperable information systems. The board promotes constitutional values and individual rights by ensuring the accuracy and security of justice information and the implementation of appropriate privacy safeguards.

The goals of the board are as follows:

- Define a framework that will assist the KIFC management in establishing an operational environment that will enable the sharing of justice information within the guiding principles of the board. The framework will identify those critical components, programmatic and technical, necessary to develop and maintain a sound infrastructure.

- Ensure that personal information will not be inappropriately disseminated or misused

and safeguards are in place against the collection and use of inaccurate information.

Authority to Establish the Kentucky Intelligence Fusion Center Governance Board

Kentucky Intelligence Fusion Center Governance Board: The board was chartered by the participating agencies to provide governance and direction to the operation of the Fusion Center. The Fusion Center was originally established by Executive Order of the Governor of the Commonwealth of Kentucky, then by Statute 39G.050. Its mission is accomplished through Memoranda of Understanding between KIFC and participating agencies.

Membership: The board consists of one member from each participating agency; one member each from Kentucky Department of Military Affairs, Louisville Metro Police, Lexington Metro Police, and Federal Bureau of Investigation regardless if they are a participating agency; two members from Kentucky State Police, one member from the Kentucky Transportation Cabinet, one member from the Kentucky Sheriff's Association, one member from the Kentucky Association of Chiefs of Police, one member from the Kentucky Department of Corrections, one member from the Bureau of Alcohol, Tobacco, Firearms, and Explosives, one member from the U.S. Secret Service, and one member from an international airport police in Kentucky. The board at their discretion may approve membership to other agencies. Each board member shall be of command level and authorized to make decisions for their respective agency.

D. Definitions

Access

With regard to the Information Sharing Environment (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.

Criminal Conduct

Conduct prohibited by the government because it threatens and harms public safety and welfare and has established punishment to be imposed for the commission of such acts.

Criminal Intelligence Information

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

CJIS

Criminal Justice Information Services

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 a consideration of privacy, focusing on information which may be available only to individuals with a legal need to know.

Fair Information Principles

The Fair Information Principles (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

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

Firewall

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

Fusion Center Director

Manager appointed by the Executive Director, KOHS, to oversee the daily operations of the fusion center.

Governance Board

The management body overseeing the direction of the KIFC.

Information Privacy

Information privacy is the interest individuals have in controlling, or at least significantly influencing, the handling of data about themselves.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)

A SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

KIFC

The Kentucky Intelligence Fusion Center consists of analysts, watch officers, and other supervisors.

KSP

Kentucky State Police

Lawful Purpose

The request for data can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirmed information that requires intervention to prevent a criminal act or threat to public safety.

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.

Open Source (Research)

Much like open-source schemes that are built around a source code that is made public, the central theme of open research is to make clear accounts of the methodology, along with data and results extracted there from, freely available via the Internet.

Personal Data

Any information relating to an identifiable individual.

Public Safety

Any department or agency which has the primary goal of protecting the public and keeping it safe. Public safety is sometimes used interchangeably with the term "criminal justice agency." KRS 17.131 states … "criminal justice agencies" include all departments of the Kentucky Justice and Public Safety Cabinet except the Department of Public Advocacy, the Unified Prosecutorial System, Commonwealth's Attorney's, county attorneys, the Transportation Cabinet, the Cabinet for Health and Family Services, and any agency with the authority to issue a citation or make an arrest. KRS 17.131 does not preclude other organizations/agencies, such a fire or emergency management, from inclusion in the definition of public safety.

Requestor

The individual law enforcement officer or agency making a request for information from, or reporting an incident to, the KIFC; synonymous with "user."

Reasonable Suspicion/Criminal Predicate

When sufficient facts are established to give a trained law enforcement officer or employee a basis to believe there is a reasonable possibility an individual or organization is involved in a definable criminal activity or enterprise. (28 CFR Part 23)

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.

Suspicious Activity

Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR)

Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. SAR information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if

applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information

Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, U.S. persons, or U.S. interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information

In accordance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended by the 9/11 Commission Act (August 3, 2007, P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in the IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information may include intelligence information.

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), SAR, and /or field information report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or Computer Aided Dispatch (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 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.

E. Information

All criminal intelligence information containing personal data or identifying organizations as criminal subjects that are collected by the KIFC will be retained in compliance with 28 Code of Federal Regulations (CFR) Part 23 and any other applicable state or local statutes governing the collection of criminal intelligence information. The KIFC will adhere to criminal intelligence collection guidelines established under the National Criminal Intelligence Sharing Plan (NCISP). Stakeholder agencies are responsible for ensuring criminal intelligence information submitted to KIFC complies with the following minimal guidelines:

1. The source reliability and content validity of the information (confidence) is indicated.

2. Information in source agency files supports reasonable suspicion of the individual or organization is involved in criminal conduct, and the information is relevant to that conduct or the identification of the criminal subject.

3. Information was gathered or collected in a lawful manner, with knowledge and consent of the individual, if appropriate.

4. Information may not be collected about individuals or organizations solely on the basis of their political, religious or social views or activities; their participation in a particular noncriminal organization or lawful event or their race ethnicity, citizenship, place of origin, age, disability, gender or sexual orientation.

5. Information is accurate and current per 28 CFR Part 23.

The KIFC applies labels to center-originated information (or assures that originating agencies provide such labels) to indicate to the user that:

1. The information is protected “personal data,” as defined in Section D., above, on any individual and, to the extent expressly provided in this policy, includes organizational entities.
2. The information is subject to federal, state, and local laws (as referenced in section B. and the Appendix) restricting access, use, or disclosure.

At the time a decision is made by KIFC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Protect confidential sources and police undercover techniques and methods.

- Not interfere with or compromise pending criminal investigations.

- Protect an individual's right of privacy or his or her civil rights and civil liberties.

- Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

The KIFC will abide by daily operating procedures for the initial collection, verification, and categorization of information and criminal intelligence, to determine its nature, usability, and quality, including the screening process by an analyst/call taker and the subsequent review by supervisory personnel, as provided above. This information may originate with a line police officer, a member of the public, a private corporation or another State or Urban Area Fusion Center. Information received through the Kentucky Open Portal System (KYOPS) will be evaluated under ISE-SAR criteria for inclusion in the National SAR database. Information received from other sources will be validated utilizing checks enumerated elsewhere in this policy. Information received through KYOPS is always categorized as law enforcement information and is deemed, on its face, to already have some degree of reliability, whereas, information reported through the KIFC SAR reporting tool or through the KIFC tipline may bear more scrutiny or may require a longer period of time to validate the reliability.

The KIFC will identify and review protected information that may be accessed from or disseminated by the KIFC prior to sharing that information through the ISE. The KIFC 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.

In addition to the collection, development and dissemination of criminal intelligence information, KIFC may also collect, review, analyze, store, and disseminate other types of information, including, but not limited to "tip and lead" information, criminal history information, driver history, information from correctional facilities, information regarding residence, unemployment benefits, and place of employment and earnings. The Kentucky State Police maintains MOUs with each of the source agencies for access to the above referenced information. The KIFC maintains MOUs with agencies that participate in the Fusion Center (including the Kentucky State Police). The KIFC also collects, maintains and disseminates SAR information for the purpose of protecting critical infrastructure/key resources within the Commonwealth. Collection/maintenance of SAR information will be based on the "reasonably indicative" standard. If the SAR information meets the reasonable suspicion standard, it may be integrated into existing processes and systems used to manage other crime related information and criminal intelligence. SAR information, collected via the KOHS web portal, which does not meet the above state standard, will be maintained in a database which is housed on a server located behind the Kentucky State Police firewall; but accessible by KIFC analysts. This data will be reviewed on an annual basis for applicability to law enforcement criminal investigations. Information that is deemed of no investigative value will be purged from the database at the direction of the Fusion Center Director. This process consists of collection, integration, evaluation, analysis and dissemination through established procedures for law enforcement purposes and in the interest of public safety. SAR data is collected and maintained in a secure database maintained by the Kentucky State Police and is subject to federal and state Criminal Justice Information Services (CJIS) policies (including the current

version of the ISE-SAR Functional Standard for Suspicious Activity Reporting) relating to storage, access, dissemination, and retention and security of the information. KIFC complies with applicable federal and state laws regarding the collection, maintenance and dissemination of Protected Critical Infrastructure Information (PCII) and SAR information.

KIFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and SAR information. KIFC personnel will:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The KIFC will use a standard reporting format and data collection codes for SAR information.

- Store the information using the same storage method used for data which rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.

- Allow access to or disseminate the information using the same access or dissemination standard that is used for data that rises to the level of reasonable suspicion.

- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.

- Retain information for one year in order to work an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a “disposition” label so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

- Adhere to and follow the KIFC’s physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

The KIFC requires that certain basic descriptive information (labels) be entered and associated with each record, data set, or system of records containing personally identifiable information that will be accessed, used, and disclosed, including terrorism-related information shared through the ISE. The types of information include:

- The name of the originating center, department or agency.
- If applicable, the name of the center's justice information system from which the information is disseminated.
- The date the information was collected and, where feasible, the date its accuracy was last verified.
- The title and contact information for the person to who questions regarding the information should be directed.

The KIFC is maintained for the purpose of developing information and intelligence for and by participating stakeholder agencies. The decision of the agencies to participate with the KIFC and to decide which databases to provide for KIFC access is voluntary and will be governed by the laws and rules governing those individual agencies, as well as any applicable federal laws.

Information obtained from or through the KIFC can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation, or is a response to confirmed information that requires intervention to prevent a criminal act or threat to public safety.

The KIFC Governance Board or designee, e.g., Privacy Officer, will take necessary measures to ensure access to the KIFC's information and intelligence resources are secure. Unauthorized access or use of the resources is forbidden. The board and the Kentucky Office of Homeland Security Executive Director reserve the right to restrict the qualifications and number of personnel having access to the KIFC and to suspend or withhold service to any individual violating this *Privacy Policy*. The board, or persons acting on its behalf, further reserves the right to conduct inspections concerning the proper use and security of the information received from the KIFC.

Information disseminated by the KIFC will be to authorized users on a "need to know" basis serving agencies with a "right to know" the information in the performance of a law enforcement activity, and will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel who receive, handle, or have access to KIFC data will be trained as to those laws, rules, and regulations. All personnel having access to KIFC data agree to abide by the following rules:

1. The KIFC's data will be used only in support of official law enforcement activities in a manner authorized by the requestor's employer.
2. Individual passwords will not be disclosed to any other person, except as authorized by KIFC management.
3. Individual passwords of authorized personnel will be changed if the password is compromised or improperly disclosed.
4. Background checks will be completed on personnel who will have direct access to the KIFC at a level determined by the Governance Board.
5. Use of the KIFC's data in an unauthorized or illegal manner will subject the requestor to denial of further use of the KIFC, discipline by the requestor's employing agency, and/or criminal prosecution.

The KIFC reserves the right to deny access to any KIFC user who fails to comply with the applicable restrictions and limitations of the KIFC policy. The KIFC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification. Subsequent to the receipt of information by KIFC, if the source agency provides updated information relative to the original submission, KIFC will re-evaluate the information for the purpose of determining if the update will cause a change in the labeling, access or disclosure of this information. If the update does cause a change in either/all of the aforementioned, then KIFC will make the appropriate changes to the status of the information.

F. Acquiring and Receiving Information

Requests for information from KIFC shall be submitted via email to the Fusion Center Email Inbox. The email will identify the requestor, the type of information sought and the applicable criminal investigation which is being conducted. Since the primary "owner", of criminal intelligence information, is the Kentucky State Police; all dissemination of information will be in compliance with applicable Kentucky State Police Policies and Procedures as well as applicable State (KRS Chapter 16 and KRS Chapter 39G) and Federal (28CFR Part 23) laws and regulations. There are no specific statutes that apply to the KIFC, with regard to seeking and receiving information. The Kentucky State Police performs internal audits of criminal intelligence information systems. Since KIFC relies on these systems as sources of information, the Kentucky State Police audit will suffice to ensure our compliance with the above statutes and regulations. Information submitted to KIFC will be submitted by participating agencies through the use of the Kentucky State Police Field Information Report (FIR) through KYOPS. NOTE: The FIR is a Kentucky-specific name for SAR. SAR and FIR can be used interchangeably. This information is reviewed by a Kentucky State Police analyst to determine if it meets the requirements (28 CFR Part 23) for inclusion in the Virtual Intelligence System (VIS). Information not meeting the requirements, established under 28 CFR Part 23, is maintained in the records management system and is subject to Kentucky State Police retention policies. All sources of information requested are maintained with the transmitted/received report; with the exception of suspicious activity anonymously reported through the KOHS web portal.

KIFC analysts will review SAR information to ensure the information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. KIFC analysts who are responsible for vetting SAR information are required to complete training specified by the NSI. Records of the completion of this training will be maintained by the Fusion Center Director. KIFC has no authority to mandate completion of training by potential submitters of SAR information, however, line officers will be provided with the availability of such training and encouraged to complete the training. Information-gathering techniques used by the KIFC should be the least intrusive necessary to gather necessary and authorized information.

The KIFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared

through the ISE. These safeguards are intended to ensure that information that could violate civil rights will not be intentionally or inadvertently gathered, documented, processed, and shared.

The KIFC will contract only with commercial database entities that provide assurance that their methods for gathering personally identifiable information comply with applicable local, state, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices. KFIC personnel are prohibited from receiving, seeking, accepting, or retaining information knowingly obtained illegally or in violation of the federal or state constitutions or statutory laws protecting privacy, civil rights and civil liberties, from any foreign, domestic, governmental, non-governmental, private or public source. Information obtained in accordance with the federal or state constitutions and applicable statutes, from private, public, governmental, or non-governmental sources which have been deemed to be reliable, will be collected, gathered, maintained, analyzed, and disseminated. If KIFC becomes aware that information was obtained contrary to proscribed standards, the originating agency will be informed by the most expeditious means. A copy of any written correspondence (if generated) will be maintained in the KIFC Correspondence file for the current year, plus 2 additional years.

KIFC will not seek, gather, collect, accept, keep or retain information that has not been deemed reliable/valid by appropriately trained analysts.

G. Information Quality Assurance

Stakeholder agencies participating in the KIFC and providing data remain the owners of the data contributed. These agencies are responsible for the quality and accuracy of the data accessed by the KIFC. KIFC personnel will ensure that data is complete, accurate, current, and reliable through periodic database searches, by cross-checks with other data systems, and open source information. In order to maintain the integrity of the KIFC, any information obtained through the KIFC will be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. User agencies and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data. KIFC personnel, as part of the information validation and intelligence cycle process, will research suspected information errors and deficiencies and will notify the originating agency of receipt of any erroneous information. KIFC will not utilize information that has not been deemed reliable, accurate, complete, or current through cross checks, review of other data systems and open source information. This policy also applies to information originated by KIFC. KIFC will utilize confidence labels of low, medium, and high with regard to the quality of information shared in the ISE. KIFC analysts will re-evaluate the labeling of information, when new information is gathered that impacts the original confidence label attached to an ISE submission.

Notifications regarding erroneous information will be made via e-mail to the originating agency. In the event KIFC determines that it has passed erroneous information to another agency, it will notify them via e-mail and provide instructions for further handling of the information (i.e., destruction/modification).

H. Collation and Analysis

The purpose of the KIFC is to collect, maintain, analyze and disseminate intelligence information in support of law enforcement agencies throughout the Commonwealth. Analysis of supplied or available information is performed to determine the following:

- patterns of criminal activity
- similarities between/among criminal acts
- whereabouts of wanted suspects
- associations between/among groups or individuals for the purposes of committing criminal acts
- threats to critical infrastructure/key resources

The KIFC requires that all analytical products receive an appropriate privacy review (and approval) by the Director and Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the KIFC.

I. Merging Records

KIFC will not merge multiple or partial records on the same individual.

J. Sharing and Disclosure

Information sharing will be in strict compliance with the dissemination policies adopted by KIFC and participating agencies. Information will only be shared with users authorized by law to have such access who have a legitimate "need to know/right to know" and only in the performance of official duties in accordance with established state and federal laws (refer to Appendix). Information access will be granted to individuals after completion of a fingerprint-supported background check and applicable clearance or confirmation by the sponsoring agency that these checks have already been completed. Query and dissemination logs will be maintained and these will be audited in accordance with established agency policies and applicable federal regulations. Audits of query and dissemination logs will be maintained for the current year plus two additional years for which audits were performed. Additionally, information cannot be disclosed or published without the prior approval of the contributing agency. Information is not accessible to members of the public, unless it is required to be disclosed under the Kentucky Open Records Law or other state law.

KIFC controls user access and permissions with regard to Homeland Security Information Network (HSIN) and the suspicious activity reporting web portal. All other user access and permissions are controlled by the agency which owns the system being accessed, i.e. HSDN, KYOPS, CCH, CourtNet, JusticeXchange. Access/permissions to KIFC owned systems are controlled by the Privacy Officer and the Fusion Center Director. Access/permissions may range from read only to add/modify/delete records depending on the roles and responsibilities of the individual accessing the system.

KIFC is not the custodian of criminal history or criminal intelligence information. The Kentucky State Police, pursuant to Chapter 17 of the Kentucky Revised Statutes, maintains criminal history information. Additionally, the Administrative Office of the Court maintains criminal history information (felonies are maintained in perpetuity; misdemeanor records are maintained for a period of five years). The determination of release of information by KIFC is made by the Executive Director.

K. Redress

Disclosure

Information maintained by KIFC is for Official Use Only and is not accessible to members of the public, unless it is required to be disclosed under the Kentucky Open Records Law or other state law. Further, information will only be disseminated in accordance with participating agency policies and applicable state and federal laws. Records of requests for disclosure (as well as the information disclosed) are maintained by the KIFC Privacy Officer and at his/her discretion. The KIFC Privacy Officer coordinates with the KOHS Executive Director with regard to information requests and related complaints and corrections requests pertaining to KIFC records.

Kentucky Open Records Law: KRS 61.870 to 61.884 establishes a right of access to public records. Certain records are exempt from public record to include records of law enforcement agencies or agencies involved in administrative adjudication if disclosure of the records would harm the agency by premature release. Any record which is not exempted by the aforementioned statute is a public record. Final determination of the release of such records is the responsibility of the Executive Director and records of this are maintained by the KIFC Privacy Officer.

To inspect a public record, you must make a written request to the official custodian of the records of the agency. The custodian is the agency employee who is responsible for maintaining the agency records. You should describe the records you want to inspect, sign the request, and print your name on it. You may hand-deliver, mail, or fax your request to the agency.

The official custodian of records for the KIFC is the Executive Director, KOHS.

Complaints and Corrections

Complaints regarding information that has been maintained or disseminated shall be made to the agency maintaining or disseminating the information. Inter-agency disputes will be presented to the Governance Board by the Executive Director of the KOHS or his/her designee. Public complaints regarding the maintenance or dissemination shall be directed to the agency which maintains the information. If they require assistance in contacting the originating/maintaining agency, they will be provided with the telephone number for that agency. The KIFC may coordinate and assist other agencies investigating and correcting identified information deficiencies.

If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

(a) Is exempt from disclosure.

(b) Has been or may be shared through the ISE.

(1) Is held by the KIFC and

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

The KIFC will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer at the following address: Jason Childers, KIFC Operations Support Coordinator, Office of the Governor, Kentucky Office of Homeland Security, 200 Mero Street, Frankfort, KY 40602, 502-564-2081, or via e-mail at jason.childers@ky.gov. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the KIFC, the Privacy Officer will notify the originating agency in writing or electronically within 10 business days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the KIFC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the KIFC will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

To delineate protected information shared through the ISE from other data, the KIFC maintains records of agencies sharing terrorism-related information and employs systems/mechanisms to identify the originating agency when the information is shared. For the purpose of accessing and sharing data in the ISE, the ISE Privacy Official is Jason Childers, Kentucky Office of Homeland Security.

A record of complaints or requests for correction and the resulting action will be maintained by the Privacy Officer for a period of time not to exceed one year. Additionally, the Executive Director will be provided with copies of the complaints.

The Executive Director is responsible for handling complaints regarding any open records request, including terrorism related records. All complainants will be provided with the contact information for the Executive Director. Conversely, the Executive Director will be provided with the contact information of those individuals/entities wishing to file a complaint regarding the handling of an open records request. A request denial will be provided in writing. Those wishing to file an appeal of denial of an open records request may do so in accordance with the following procedure:

If your request is denied, you may file an appeal with the Kentucky Attorney General for review of the agency's actions. Your appeal must consist of a letter describing the circumstances of the denial, a copy of your written request, and a copy of the agency's written denial, if available. Unless you are an inmate confined in a jail or correctional facility who is aggrieved by a denial issued by the Corrections Cabinet, you may bypass the Attorney General's Office and file your appeal in Circuit Court. If you choose to go directly to Circuit Court, you will incur the costs of bringing a lawsuit, including filing fees and your attorney's fees. The Attorney General will review your appeal and issue a decision. The decision will state whether the agency violated the Open Records Act by denying your request. You will receive a copy of the decision along with the agency. You or the public agency may appeal the Attorney General's decision to the Circuit Court of the County where the agency has its principal place of business or where the record is maintained. The Attorney General should be notified of any Circuit Court action, but may not be named as a party in the action. If an appeal is not filed within 30 days, the Attorney General's decision has the force and effect of law and can be enforced in Circuit Court. However, the Attorney General does not have authority to force an agency to release records or otherwise enforce the decision after it is issued. If you prevail against an agency in Circuit Court, you may be awarded costs, including reasonable attorney fees, if the court finds that the records were willfully withheld. The court may also award you up to $25 for each day that you were denied the right to inspect the records.

L. Security Safeguards

Information obtained from or through the KIFC will not be used or publicly disclosed for purposes other than those specified in the MOUs signed with the participating agency. *Information cannot be*:

- Sold, published, exchanged, or disclosed for commercial purposes;
- Disclosed or published without prior approval of the contributing agency; or
- Disseminated to unauthorized persons.

Research of KIFC's data sources is limited to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the KIFC will be granted only to fully authorized personnel who have been screened with state and national fingerprint-based background checks, as well as any additional background standards or clearance requirements established by the KIFC Governance Board.

The designated KIFC Security Officer will identify technical resources to establish a secure facility for Fusion Center operations with restricted electronic access, security cameras, and alarm systems to guard against external breach of the facility. In addition, the Security Officer will identify technological support to develop secure internal and external safeguards against network intrusion of KIFC data systems. Access to the KIFC's databases from outside of the facility will only be allowed over secure network lines. Risk and vulnerability assessments will not be available for public review. Risk and vulnerability assessments are stored in locked cabinets within the Critical Infrastructure work area of the Fusion Center. If these assessments contain PCII, then they are marked and stored in compliance with PCII guidelines. The KIFC

Security Officer is designated by the Executive Director, KOHS and is responsible for the physical security of the KIFC as well as security of data systems and information maintained therein.

The KIFC will notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly following the discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release. The KIFC will immediately notify the originating agency from which the Fusion Center received personal information of a suspected or confirmed breach of such information.

The KIFC Security Officer has attended the National Fusion Center Security Liaison Workshop to accelerate the implementation of security-related baseline capabilities in the Fusion Center, as identified in the Baseline Capabilities for State and Major Urban Area Fusion Centers.

KIFC maintains a web-based SAR reporting tool, with the supporting database housed behind a firewall within the Kentucky State Police network infrastructure. The access to the database is provided to those with responsibility for reviewing/vetting SAR information. The Fusion Center Director determines, based on roles and responsibilities, who will have access to the database.

M. Information Retention and Destruction

Criminal intelligence information is maintained by law enforcement agencies. KOHS is not a law enforcement agency and neither is the KIFC. The Fusion Center is made up of law enforcement as well as non-law enforcement (KOHS, KYTC) agencies. Inasmuch as it is the role and responsibility of law enforcement agencies to enact policies regarding retention and destruction of criminal intelligence information, this Privacy Policy must yield to the provisions of the Kentucky State Police, Intelligence Branch. The Kentucky State Police operates the primary law enforcement intelligence database for the Commonwealth of Kentucky and maintains it in compliance with the provisions of 28 CFR Part 23. Additionally, the Kentucky State Police has agency policies governing the maintenance and dissemination of criminal intelligence information and retention and destruction of said information to include intelligence and other crime related data contained in various criminal justice information systems.

KIFC will observe a one year retention schedule for information collected/gathered through the KIFC owned web portal. Information gathered/collected through this portal will be purged after one year unless it can be linked to an ongoing criminal investigation. Currently, the process for reviewing and purging information is a manual process initiated by the Fusion Director, in which he or she directs analysts to review records based on their date of creation/modification; however, no formal approval will be required from the originating agency before information held by the KIFC is destroyed or returned. The KIFC Director will direct review of records

meeting the above criteria by the Privacy Officer and direct removal of the records in excess of one year. Electronic records and any associated hard copy records will be deleted/shredded. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the KIFC, depending on the relevance of the information and any agreement with the originating agency.

The information maintained in the Kentucky State Police Intelligence Data Base (Virtual Intelligence System) features an automated purge feature which prompts KSP Intelligence personnel when a record has reached the designated purge threshold. The records are then reviewed and purged or maintained in accordance with 28 CFR Part 23.

N. Accountability and Enforcement

The KIFC will be open with the public in regard to information and intelligence collection practices. The KIFC's privacy policy will be made available to the public via the Kentucky Office of Homeland Security's website at www.homelandsecurity.ky.gov. Privacy Policy supporting documentation may or may not be made available to the public. Any determination related to the dissemination of supporting documentation will be referred to the KIFC Privacy Officer.

The KIFC Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The Privacy Officer may refer certain complaints or inquiries to the appropriate legal counsel of a participating agency.

Information System Transparency

In an effort to demonstrate transparent information collection practices, the KIFC will make available a copy of the Privacy Policy via its website www.homelandsecurity.ky.gov It is the intent of the KIFC and participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. KIFC will refer citizens to the originating agency of information as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation. KIFC will not confirm the nonexistence of a record.

Open records requests to the KIFC will be forwarded to the Executive Director or Kentucky State Police Commissioner for review and determination of who should respond to the request.

Accountability

Queries made to the KIFC data applications will be logged into the KIFC's data system identifying the user initiating the query. When such information is disseminated outside of the originating agency, a secondary dissemination log will be created in order to capture updated information and provide an appropriate audit trail, as required by applicable law. Secondary dissemination of information can only be to a law enforcement agency for investigative

purposes or to other agencies as provided by law. The agency *from* which the information is requested will maintain a record of any secondary dissemination of information. This record should reflect at a minimum:

- Date of release
- The subject of the information
- To whom the information was released (including address and telephone number)
- An identification number or other indicator that clearly identifies the data released
- The purpose for which the information was requested.

The KIFC will coordinate with the KSP CJIS audit staff for conducting or coordinating internal or special audits, and for investigating misuse of the KIFC's information systems. Annual audits will be scheduled and conducted within the availability of audit staff. Additional "random audits" may be conducted if requested by the Fusion Center Director or the Kentucky State Police Intelligence Branch Commander. These audits will consist of an independent review of records maintained by KIFC to ensure that records are maintained in compliance to the retention schedule, that appropriate purges of records have been completed, that appropriate changes have been made to records based on subsequent submissions and appropriate cross-checks, and that other documentation related to Open Records Requests, denials, disclosures and complaints are maintained in accordance with the provisions of this policy. *All confirmed or suspected violations of KIFC policies will be reported through the KIFC Director to the Board and/or Kentucky State Police, if a violation of Kentucky State Police policies is discovered*. Individual users of KIFC information remain responsible for the appropriate use of KIFC information. Each user of the KIFC and each participating agency within the Fusion Center are required to abide by this *Privacy Policy* in the use of information disseminated. Failure to abide by the restrictions for the use of the KIFC data may result in the suspension or termination of user privileges; discipline imposed by the user's employing agency, or criminal prosecution. Internal audits are conducted by participating agency management (Kentucky State Police Inspections and Evaluations Branch; Fusion Center Director). External audits of non-law enforcement databases may be conducted by the Kentucky Auditor of Public Accounts at the discretion of the Auditor of Public Accounts. This policy as well as other applicable policies for the Kentucky Intelligence Fusion Center shall be reviewed on an annual basis by the Privacy Officer and the Fusion Center Director. Policy revisions will be performed as indicated by the review.

Enforcement

Unauthorized access, use, handling, or disclosure of information may result in suspension or denial of future services, agency discipline, or appropriate criminal or civil remedies. The enforcement of these sanctions will be handled by the employing agency in consultation with the Fusion Center Director.

O. Training

The KIFC will require all assigned personnel to the Fusion Center to participate in training regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy. The KIFC will make this training, while not required, available to the following individuals:

- Personnel providing information technology services to the KIFC.
- Staff in other agencies or private contractors providing services to the KIFC

The KIFC will make available, as necessary, special training regarding the Fusion Center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

The KIFC's privacy policy training will cover:

- Purpose and intent of the privacy policy.
- Provision of the policy relating to collection, use, analysis, retention, destruction, sharing and disclosure of information retained by the center.
- Originating and participating agency responsibilities under applicable law and policy.
- Day-to-day implementation of the policy in the working environment.
- Procedures for reporting violations of center privacy protection policies.
- The nature and possible penalties for policy violations.

APPENDIX

Applicable State Law and Policies

Kentucky Intelligence Fusion Center Standard Operating Procedures
Kentucky Intelligence Fusion Center Security Policy
Kentucky Revised Statutes Chapter 16
Kentucky Revised Statutes Chapter 39G
Kentucky Revised Statutes Chapter 61
Executive Order #2009-0771
Criminal Justice Information Systems (CJIS) Policy

Federal Laws

The following is a partial listing of applicable federal laws relevant to seeking, retaining, and disseminating justice information arranged in alphabetical order by popular name:

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

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

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III,
§ 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272