Kansas City Regional TEW
Inter-Agency Analysis Center

A Terrorism Early Warning Group

PRIVACY, CIVIL LIBERTIES, AND CIVIL RIGHTS POLICY

Table of Contents

I. Mission/Purpose

The Kansas City Terrorist Early Warning Center (KCTEW) is tasked to implement a collaborative effort to collect, collate, analyze, and disseminate information to appropriate agencies and individuals, in an effort to mitigate terrorist and criminal related activities. Equally important is our mission to safeguard the privacy, civil rights, and civil liberties of every individual. 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.

II. Scope and Compliance

All KCTEW employees, whether full, part-time, or temporarily assigned, will be trained in and comply with this policy. Internal KCTEW operating policies govern our operations and comply with all applicable laws. Agencies and individual users of KCTEW work products are also required to comply with applicable sections of this policy. Additional notifications of that requirement will be made as appropriate, by an attachment to individual work products. All KCTEW users, personnel providing information technology services, and private contractors will be directed to review this policy and will comply with all federal and state privacy laws cited in the appendix to this policy. The KCTEW will provide a printed copy of this policy to all KCTEW and non-KCTEW personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users. All will comply with the KCTEW's privacy policy concerning the information the KCTEW collects, receives, maintains, archives, accesses, or discloses to KCTEW personnel, government agencies, including Information Sharing Environment (ISE) participating agencies, and participating justice and public safety, as well as to private contractors and the general public. An agreement will be signed to indicate an understanding of the privacy policy. This agreement is contained in APPENDIX A of this document.

KCTEW will make a copy of this policy available to any interested party, public or private.

III. Oversight

The KCTEW is an inter-disciplinary, collaborative initiative administered by the Mid-America Regional Council (MARC). Primary responsibility for the operation of the KCTEW, its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information, quality, analysis, destruction, sharing, and disclosure of information, and the enforcement of this policy is assigned to the Director and/or designee of the KCTEW. A KCTEW Intelligence Specialist (IS) will be designated as the "Privacy Officer" whose duties will include training assurance, reception and evaluation of errors and violations of this policy, and is responsible for

receiving, handling, and maintaining records of complaints from the general public regarding this policy.

As appropriate, MARC staff, members of the Executive Committee, the KCTEW Director or the agency's Privacy Officer will, when necessary, interact with privacy advocacy groups to address issues regarding the KCTEW's information collection, retention, and dissemination processes.

IV. Information

In fulfilling its public safety role, the KCTEW may actively seek, analyze, disseminate, and retain information that is based on terrorism related criminal predicates, a reasonably suspected terrorism nexus, or that which negatively impacts on public safety. Such information must be believed to 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 actionable intelligence, the KCTEW may also engage in research toward that end. All KCTEW employees will ensure that information is verifiable, collected in a lawful manner, and lawfully disseminated. Only KCTEW employees, vetted and approved contractors, and other pre-authorized personnel will be able to access the information. The limitations on the quality of the information will be noted if a source is of doubtful credibility and as provided in Section VI., Data Quality. KCTEW may retain preliminary information such as tips and leads, and suspicious activity reports, providing the information is arguably of public safety interest. KCTEW 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. Information will be disseminated to individuals based on the need-to-know and right-to-know concept.

The KCTEW applies labels to center-owned information to indicate to the accessing authorized user that:

- The information pertains to a United States citizen or a lawful permanent resident
- The information is subject to Chapter 45 of Kansas Statute Annotated and Chapter 610 of Revised Missouri State Statutes.

The KCTEW personnel will ensure certain basic descriptive information is entered and associated with data for which there are specific laws, rules, or policies regarding access, use, and disclosure. The types of information that will be included is the name of the originating department, component, and subcomponent, the name of the agency or department's justice system where the information was obtained, the date the information was collected, and when available, the date its accuracy was last verified, the title and contact information for the person who provided the information, and the person to whom future questions regarding the information can be directed. KCTEW personnel will ensure that labels and metadata have been applied to the information that will be used, accessed, and disseminated to clearly indicate any legal restrictions on information

sharing based and on information sensitivity or classification. A record will be kept of all information which the KCTEW will retain. Such information will be entered into an activity-tracking database. Upon entry into the activity-tracking database, consideration must also be given 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, sex abuse victim, resident of a substance abuse/mental health treatment program or resident of a domestic abuse shelter.

During receipt, storage, or dissemination of information, KCTEW personnel will assess the information for sensitivity, evaluate to determine its credibility, label the information as either unsubstantiated/uncorroborated if the validation or reliability is uncertain, and document the information received/disseminated. 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. All information obtained from outside agencies with a sensitivity label will be evaluated by KCTEW personnel and relabeled with the same labels used by KCTEW personnel. The original label will be maintained with the information. All information will be labeled as Unclassified, Controlled Unclassified Information, and Classified. See APPENDIX B, Definitions for further information.

Information received, analyzed, and disseminated at the KCTEW will include at a minimum, indicators for type of criminal investigation, tips and leads, source information, requestor identification, reliability of the source and validity of the content, sensitivity, juvenile information, and protected status information. Information may be reclassified whenever new information is added that would increase/decrease the sensitivity of disclosure.

The KCTEW will keep a record of the source of all information sought, collected, and retained by the agency.

V. Acquiring and Receiving Information

Information gathering, including acquisition and access, and investigative techniques used by the KCTEW and information-originating agencies are in compliance with and will adhere to applicable regulation and guidelines, including, but not limited to:

- 28 CFR Part 23 regarding criminal intelligence information
- Organization for Economic Co-operation and Development's (OECD) Fair Information Practices (under certain circumstances, there may be exceptions to the Fair Information Practices, based, for example, on authorities paralleling those provided in the Federal Privacy Act; state, local, and tribal laws, or KCTEW policy)
- Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan NCISP)

- Applicable constitutional provisions, Revised Missouri State Statute Chapter 610 (Missouri Sunshine Laws), Chapter 45 of Kansas Statute Annotated (Kansas Open Records Act, KORA and Kansas Open Meetings Act, KOMA), and the applicable administrative rules, as well as any other regulations that apply to multijurisdictional intelligence databases.

In providing information, KCTEW contributors are governed by the laws and rules of their individual agencies as well as by applicable state and federal laws restricting access, use, or disclosure. KCTEW 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. A human review of the information ensures the information was gathered legally and ensures all information that is disseminated or shared through the ISE does not violate civil rights or civil liberties.

Information gathering and investigative techniques used by the KCTEW will (and from the originating agencies should) be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain. The KCTEW will contract only with commercial database entities that demonstrate that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information collection practices

The KCTEW will identify and review protected information that is originated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

Any further information regarding processes and day-to-day operations can be found in the numerous duty and software manuals. These manuals will not be available to the general public because of sensitivity issues involving the release of security information.

VI. Quality Assurance

The KCTEW will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard [Refer to Section VIII Merging Records] has been met.

At the time of retention in the system, the information will be labeled regarding its level of quality (accurate, complete, current, verifiable, and reliable). For further information refer to KCTEW Policies and Procedures manual.

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

The labeling of retained information will be reevaluated when new information is gathered that has an impact on the validity and reliability of retained information.

The KCTEW will make every reasonable effort to ensure that information will be corrected or deleted from the system when the center learns that the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather the information or to provide the information to the center; or the source used prohibited means to gather the information, except when the source did not act as an agent to a bona fide law enforcement officer.

Center participating agencies are responsible for the quality and accuracy of the data accessed by the center. Center participating agencies providing data remain the owners of the data contributed. The KCTEW will advise the appropriate data owner, in writing, if its data is found to be inaccurate, incomplete, out of date, or unverifiable.

The KCTEW will use written or documented electronic notification to inform recipient agencies when information previously provided by the KCTEW is deleted or changed by the center (for example, it is determined to be inaccurate or includes incorrectly merged information).

VII. Collation and Analysis

All KCTEW Intelligence Specialists have successfully passed a background check, may possess an appropriate security clearance, and have been selected, approved, and trained according to KCTEW requirements. As such they 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.

As an employee of the KCTEW (MARC) or an employee of a federal, state and local agency that has provided staff to the KCTEW, individuals working in the KCTEW may have the right to access criminal history record information or health-related information on individuals. The information that KCTEW personnel and planners receive and review must be necessary for their work. All disseminations of written information from KCTEW personnel and planners on an individual must be recorded.

VIII. 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, an analyst may merge the information within KCTEW work products and records. In such an instance, the contributing and recipient agency will be notified of that fact. No alterations or modifications will ever be made by KCTEW personnel to a contributing, participating, or recipient agency's data systems.

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.

If the matching requirements are not fully met but there is an identified partial match, the information may be associated if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

IX. Inquiry, Complaints, and Redress

Credentialed, role-based access criteria will be used, as appropriate, to control:

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

The KCTEW adheres to national standards for the Suspicious Activity Reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with ISE Functional Standards for suspicious activity reporting.

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

Records retained by the KCTEW may be accessed or disseminated to those responsible for public protection, safety, or public health only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with

applicable laws and procedures. An audit trail will be kept of access by or dissemination of information to such persons. Information that is considered open-source or public record may be released outside the public safety community if such disclosure will further the KCTEW mission and the recipient has a valid "need to know." In addition, KCTEW personnel will not disclose the existence or non-existence of information to any organization or person that would not be eligible to receive the information itself.

KCTEW personnel will not sell, publish exchange or disclose information for commercial purposes, or provide information to unauthorized persons. Permission to distribute any information to any person or organization will be sought from the owner of that information before any release, unless that information is obtained from open sources available to anyone in the public or prior approval has been granted. Organizations external to the KCTEW may not disseminate KCTEW information received from KCTEW without approval from the originator of the information.

Certain other records will not be disclosed to the public, including but not limited to:

- Records required to be kept confidential by law are exempt from disclosure requirements under Missouri Sunshine laws or Kansas Open Records Act (KORA).
- Investigatory records of law enforcement agencies are exempt from disclosure requirements under Missouri Sunshine laws or KORA. However, certain law enforcement records must be made available for inspection and copying under Missouri Sunshine laws and KORA.
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempt from disclosure requirements under Chapter 610 of Revised Missouri State Statute and Chapter 45 of Kansas Statute Annotated. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Chapter 610 of Revised Missouri State Statute, Chapter 45 of Kansas Statute Annotated or an act of agricultural terrorism under Chapter 610 of Revised Missouri State Statute and Chapter 45 of Kansas Statute Annotated, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.
- A violation of an authorized nondisclosure agreement.

Upon satisfactory verification of identity, an individual is entitled to know of the existence of, and to review information, including that from ISE (ISE is the Information Sharing Environment-The agencies, policies, procedure, and technologies linked to facilitate terrorism and homeland security information sharing) sources, about him/her that is owned and retained by KCTEW as long as such disclosure would not violate federal or state laws. The individual may obtain a copy of the information for personal use or for the purpose of challenging its accuracy. Access to this information will be processed by and provided by the KCTEW Privacy Officer, to whom requests for

disclosure may be addressed at: KCTEW@KCPD.org. The KCTEW response to these requests will be made within a reasonable time. If the information has been provided to the complainant, the originating agency must make a determination to as to whether to correct the information, remove the record, or ascertain a basis for denial. The individual to whom information has been disclosed will be provided notification of reason for denial. The individual will also be informed of the appeals process when KCTEW or the originating agency has declined to correct the challenged information. A copy of the appeals process is available from the KCTEW Privacy Officer at the address above.

An audit trail will be kept for a minimum of five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request. This will be completed for all requests.

Record requests will not be honored if disclosure would compromise an ongoing investigation, compromise a source of information, constitute a release of criminal intelligence, the information does not reside within KCTEW, or KCTEW does not own, or did not originate the information, or if such disclosure would violate federal or state laws.

If an individual has complaints or objections as to the accuracy or completeness of terrorism-related information alleged to be in the possession of KCTEW, and to which the individual has no right of access, KCTEW will inform the individual to file a complaint with the KCTEW Privacy Officer, and advise of the complaint reporting/corrections procedure. Upon receipt, the privacy officer will document the complaint. If information related to the complaint exists and originated with another agency, KCTEW will notify the originating agency and facilitate the complaint/corrections procedure. To delineate protected information shared through the ISE from other data, the KCTEW 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 organization, including ISE participating organizations, is identified within the information. The KCTEW will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence or nonexistence of the information. However, any personal information will be reviewed and verified or corrected in or deleted from KCTEW records if the information is determined through review to be erroneous, include incorrectly merged information, or be out of date. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

X. Security

A KCTEW Intelligence Specialist will be designated as the center's security officer and will ensure the center operates in a secure manner free from facility and network intrusion. The designated security officer will attend training through a federally approved program and will be able to obtain additional information and resources from agreements with the Federal Bureau of Investigation. Access to KCTEW databases is strictly limited from inside the facility or similar secure facility with preapproval of

access permissions and it will only be allowed in a secure manner. KCTEW will store information in such a way that it cannot be accessed, modified, destroyed, or purged by unauthorized personnel.

Queries made to the KCTEW data applications will be logged into the data system identifying the user initiating the query. The KCTEW will utilize watch logs to maintain audit trails of requested and disseminated information.

If an individual's personal information retained by KCTEW is compromised, KCTEW will notify that individual without delay, provided that notification does not compromise an ongoing investigation. The Executive Committee of the KCTEW will also be notified and a determination made as to whether additional investigative assistance is required. If the security breach was directed toward KCTEW Databases and/or Information Systems, personnel from all concerned or potentially impacted agencies will be notified.

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

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

XI. Retention, Purge, and Destruction

The KCTEW will follow 28 CFR Part 23 regarding retention, purging and destruction of information. Information that has no further investigative or research value 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. Notification may or may not be made to the owner of the information, depending on previous agreements. Exact processes for purging and destroying information are stated in KCTEW Policies and Procedures manual. A record of information to be reviewed for retention will be maintained by the KCTEW and, for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

XII. Accountability and Enforcement

The KCTEW will remain open and accountable to the public regarding information collection practices. Written copies of the KCTEW Privacy Policy are available to any interested party, public or private on the following web site: KCTEW.ORG

The KCTEW, operating as a program of the MARC, the Director of KCTEW, or his/her designee, with guidance from the Executive Committee and designated legal counsel, is responsible for responding to inquiries and complaints about privacy, civil rights and

civil liberties within the KCTEW. Inquiries and complaints, other than as expressly provided in this policy may be directed to: Bob Kolenda at Robert.Kolenda@kcpd.org

The audit log queries made to the KCTEW will identify the user initiating the query. The KCTEW will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.
The KCTEW will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in provisions of this policy and applicable law. This will include logging access of these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits, to be conducted by KCTEW staff, will be mandated at least yearly and randomly, and a record of the audits will be maintained by the Security Officer of the KCTEW. The KCTEW may be subject to independent audits as deemed appropriate by the Executive Committee.

The KCTEW's personnel or other authorized users shall report violations or suspected violations of KCTEW policies relating to protected information to the KCTEW's privacy officer. The KCTEW Privacy Officer will 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 at a minimum of once a year or when changes to the above cited laws occurs. Changes in public expectations may be considered in any review of this policy.

If any KCTEW personnel are found to be non-compliant with the provisions of the KCTEW privacy policy, the Director of KCTEW will immediately suspend access to KCTEW Databases and notify the Executive Committee. Non-compliance with the KCTEW privacy policy could subject those individuals to civil or criminal penalties and pending a thorough investigation, further punitive actions taken in accordance with the administrative rules of the KCTEW and any related inter-agency agreements.

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

KCTEW reserves the right to limit personnel having access to the systems, and to withhold or suspend service to any agency or individual violating the KCTEW Privacy Policy.

XIII. Training

KCTEW will require all employees, including full, part-time, and temporary to participate in training regarding the implementation of this policy. Additional training may be provided by various agencies as to applicable state and federal privacy laws. KCTEW 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. KCTEW employees will be familiar with reporting mechanisms regarding violations of the policy, and repercussions, including the potential for dismissal, criminal, and individual civil liability.

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

APPENDIX A

User Agreement

KANSAS CITY REGIONAL TEW
Inter-Agency Analysis Center

Privacy, Civil Liberties, and Civil Rights Policy

POLICY NOTE
This policy does not constitute a contract of any kind. The KCTEW, Executive Committee or MARC reserves the right to change the policy at any time, without any advance notice. A copy of the most current policy will be provided to all employees and others working in the KCTEW.

This policy document was approved via electronic communication and comment by the Executive Committee on the 29th day of February, 2008.
Executive Committee approved as amended the 16th day of April, 2010.

Robert T. Kolenda
Director, KCTEW

XII. EMPLOYEE/CONTRACTOR/VENDOR PRIVACY, CIVIL LIBERTIES, AND CIVIL RIGHTS POLICY ACKNOWLEDGMENT:

I hereby acknowledge that I have received a copy of the KCTEW Privacy, Civil Liberties, and Civil Rights Policy and have read it in its entirety. I agree with and will comply with all of its provisions terms.

_____ _____
Employee/Contractor/Vendor Signature Date

_____
Printed Name

_____
Company/Organization Name – (non-KCTEW)

APPENDIX B

Terms and Definitions

The following is a list of primary terms and definitions used throughout this policy. These terms are useful in understanding the meaning of terms within in this 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. For data access, access is usually specified as read-only access 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 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.

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.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger

(fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Civil Rights—The term "civil rights" is used to imply that the state has a role in ensuring 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 upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Civil Liberties—Civil liberties are fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Classified Information— means any information or material that has been determined by the United States Government pursuant to an Executive order, statute, or regulation, to require protection against unauthorized disclosure for reasons of national security and any restricted data, as defined in paragraph r. of section 11 of the Atomic Energy Act of 1954 (42 U.S.C. 2014 (y))

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.

Controlled Unclassified Information (CUI) — the categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is:

- pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government
- under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination

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

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data—Inert symbols, signs, or measures.

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

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

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

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

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

The eight FIPs are:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle

8. Accountability Principle

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

General Information or Data—Information that could 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 could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information—As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information 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.

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 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 compound of such data as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

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

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, investigatory work product, tips and leads data, and criminal intelligence data.

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.

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.

Kansas City Terror Early Warning Center (KCTEW) —The Kansas City Regional Terrorism Early Warning Group brings local, state and federal law enforcement officials together with public and private organizations to detect, deter and respond to terrorist threats in the Greater Kansas City community. The KCTEW's Interagency Analysis Center collects information from a variety of sources. This data is evaluated and analyzed in an effort to identify potential trends or patterns of terrorist or criminal operations within the region.

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

Law Enforcement Information—For purposes of the 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.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are 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 only authorized individuals are getting access to the data. See also Audit Trail.

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

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular content. 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 upon the type of information and context of use.

Mid-America Regional Council (MARC)—The Mid-America Regional Council promotes regional cooperation and develops innovative solutions. MARC is a nonprofit association of city and county governments and the metropolitan planning organization for the bi-state Kansas City region. Governed by a board of local elected officials, they serve nine counties and 120 cities. MARC is funded by federal, state and private grants, local contributions and earned income. A major portion of our budget is passed through to local governments and other agencies for programs and services.

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

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

Personal Data—Personal data refers to any personally identifiable information that relates to an identifiable individual (or data subject). See also Personally Identifiable Information.

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that when considered together or when considered in the context of how it is presented or how it is gathered is 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 a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, 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 State citizens and lawful permanent residents.

Privacy—Privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable 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 will adhere to those legal requirements and agency 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 finding appropriate balances between privacy and multiple competing interests, such as justice information sharing.

Protected Information—For the non-intelligence 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. For state, local, and tribal governments, it would include applicable state and tribal constitutions and State, Local and Tribal laws, ordinances, and codes. 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.

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 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 in the operation of the justice information system, and agency in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency is specified in law.

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

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

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

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

Retention—Refer to "Storage."

Right to Privacy—The possible right to be let alone, in the absence of some reasonable public interest in a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating that right.

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

Security—Security refers to the range of administrative, technical, and physical 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 homeland security information, terrorism information, and law enforcement information by both the originator of the information and any recipient of the information.

Suspicious Activity—Suspicious activity is defined as "behavior that may be indicative of intelligence gathering or pre-operational planning related to terrorism, criminal espionage, or other illicit intention. Examples of suspicious activity include: surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SAR)—The observation and documentation of a suspicious activity. Suspicious activity reports (SAR) are meant to offer a standardized means for feeding information repositories or data mining tools. Any patterns identified during SAR data mining and analysis may be investigated in coordination with the reporting agency and the state designated fusion center. The suspicious activity report 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-Related Information—In accordance with IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the 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 IRTPA, as well as the following categories of information to

the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)); and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information as a fourth (third statutory) category of ISE information is not called for in P.L. 110-53. Rather, it amends the definition of terrorism information to include WMD information and then defines that term. WMD information probably should not, technically, be cited or referenced as a fourth category of information in the ISE.

Tips and Leads Information or Data—Uncorroborated report or information generated from inside or outside the agency that alleges or indicates some form of possible criminal activity. Tips and leads can also be referred to as suspicious incident reports (SIRs), suspicious activity reports (SARs), and/or field interview reports (FIRs). Tips and leads information does not include incidents that do not have an offense attached, criminal history records, or CAD data.

A tip or lead can result from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but has not been evaluated and vetted.

Tips and leads information is maintained in a secure system similar to data that rises to the level of reasonable suspicion.

APPENDIX C
Applicable Federal and State Regulations

28 CFR Part 23

Executive Order 12291 These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises.

Regulatory Flexibility Act

These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act.

Paperwork Reduction Act

There are no collection of information requirements contained in the proposed regulation.

List of Subjects in 28 CFR Part 23

Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement.

For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows:

PART 23-CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES Sec.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§ 23.3 Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub.

L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System

means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence 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 or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional 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) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, 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.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f) (1) Except as noted in paragraph (f)(2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f)(1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies

and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is 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

participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

(5) The project must promulgate rules and regulations 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

(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require 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, date of review and explanation of decision to retain. 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.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a

class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines. The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity, and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20. The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system. (e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

Laurie Robinson
Acting Assistant Attorney General
Office of Justice Programs
(FR Doc. 93-22614 Filed 9-15-93; 8:45 am)

Criminal Intelligence Sharing Systems; Policy Clarification

[Federal Register: December 30, 1998 (Volume 63, Number 250)] [Page 71752-71753]
From the Federal Register Online via GPO Access [wais.access.gpo.gov]
DEPARTMENT OF JUSTICE 28 CFR Part 23
[OJP(BJA)-1177B]
RIN 1121-ZB40

1993 Revision and Commentary

28 CFR Part 23 Final Revision to the Office of Justice Programs, Criminal Intelligence Systems Operating Policies

---

AGENCY: Office of Justice Programs, Justice.

ACTION: Final Rule

SUMMARY: The regulation governing criminal intelligence systems operating through support under Title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, is being revised to update basic authority citations and nomenclature, to clarify the applicability of the regulation, to define terms, and to modify a number of the regulation's operating policies and funding guidelines.

EFFECTIVE DATE: September 16, 1993

FOR FURTHER INFORMATION CONTACT: Paul Kendall, Esquire, General Counsel, **Office of Justice Programs**, 633 Indiana Ave., NW., Suite 1245-E, Washington, DC 20531, Telephone (202) 307-6235.

SUPPLEMENTARY INFORMATION: The rule which this rule supersedes had been in effect and unchanged since September 17, 1980. A notice of proposed rulemaking for 28 CFR part 23, was published in the Federal Register on February 27, 1992, (57 FR 6691). The statutory authorities for this regulation are section 801(a) and section 812(c) of title I of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, (the Act), 42 U.S.C. 3782(a) and 3789g(c). 42 U.S.C. 3789g (c) and (d) provide as follows:

Confidentiality of Information

Sec. 812....

(c) All criminal intelligence systems operating through support under this title shall collect, maintain, and disseminate criminal intelligence information in conformance with policy standards which are prescribed by the Office of Justice Programs and which are written to assure that the funding and operation of these systems furthers the purpose of this title and to assure that such systems are not utilized in violation of the privacy and constitutional rights of individuals.

(d) Any person violating the provisions of this section, or of any rule, regulation, or order issued thereunder, shall be fined not to exceed $10,000, in addition to any other penalty imposed by law.

This statutory provision and its implementing regulation apply to intelligence systems funded under title I of the Act, whether the system is operated by a single law enforcement agency, is an interjurisdictional intelligence system, is funded with discretionary grant funds, or is funded by a State with formula grant funds awarded under the Act's Drug Control and System Improvement Grant Program pursuant to part E, subpart 1 of the Act, 42 U.S.C. 3751-3759.

The need for change to 28 CFR part 23 grew out of the program experience of the Office of Justice Programs (OJP) and its component agency, the Bureau of Justice Assistance (BJA), with the regulation and the changing and expanding law enforcement agency need to respond to criminal mobility, the National drug program, the increased complexity of criminal networks and conspiracies, and the limited funding available to State and local law enforcement agencies. In addition, law enforcement's capability to perform intelligence data base and analytical functions has been enhanced by technological advancements and sophisticated analytical techniques.

28 CFR part 23 governs the basic requirements of the intelligence system process. The process includes:

1. Information submission or collection

2. Secure storage

3. Inquiry and search capability

4. Controlled dissemination

5. Purge and review process

Information systems that receive, store and disseminate information on individuals or organizations based on reasonable suspicion of their involvement in criminal activity are criminal intelligence systems under the regulation. The definition includes both systems that store detailed intelligence or investigative information on the suspected criminal activities of subjects and those which store only information designed to identify

individuals or organizations that are the subject of an inquiry or analysis (a so-called "pointer system"). It does not include criminal history record information or identification (fingerprint) systems.

There are nine significant areas of change to the regulation:

(1) Nomenclature changes (authority citations, organizational names) are included to bring the regulation up to date.

(2) Definitions of terms (28 CFR 23.3(b)) are modified or added as appropriate. The term "intelligence system" is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation; the terms "interjurisdictional intelligence system", "criminal intelligence information", "participating agency", "intelligence project", and "validation of information" are key terms that are defined in the regulation for the first time.

(3) The operating principles for intelligence systems (28 CFR 23.20) are modified to define the term "reasonable suspicion" or "criminal predicate". The finding of reasonable suspicion is a threshold requirement for entering intelligence information on an individual or organization into an intelligence data base (28 CFR 23.20(c)). This determination, as well as determinations that information was legally obtained (28 CFR 23.20(d)) and that a recipient of the information has a need to know and a right to know the information in the performance of a law enforcement function (28 CFR 23.20(e)), are established as the responsibility of the project for an interjurisdictional intelligence system. However, the regulation permits these responsibilities to be delegated to a properly trained participating agency which is subject to project inspection and audit (28 CFR 23.20(c),(d),(g)).

(4) Security requirements are established to protect the integrity of the intelligence data base and the information stored in the data base (28 CFR 23.20(g)(1)(i)-(vi)).

(5) The regulation provides that information retained in the system must be reviewed and validated for continuing compliance with system submission criteria within a 5-year retention period. Any information not validated within that period must be purged from the system (28 CFR 23.20(h)).

(6) Another change continues the general prohibition of direct remote terminal access to intelligence information in a funded intelligence system but provides an exception for systems which obtain express OJP approval based on a determination that the system has adequate policies and procedures in place to insure that access to system intelligence information is limited to authorized system users (28 CFR 23.20(i)(1)). OJP will carefully review all requests for exception to assure that a need exists and that system integrity will be provided and maintained (28 CFR 23.20(i)(1)).

(7) The regulation requires participating agencies to maintain back-up files for information submitted to an interjurisdictional intelligence system and provide for inspection and audit by project staff (28 CFR 23.20(h)).

(8) The final rule also includes a provision allowing the Attorney General or the Attorney General's designee to authorize a departure from the specific requirements of this part, in those cases where it is clearly shown that such waiver would promote the purposes and effectiveness of a criminal intelligence system while at the same time ensuring compliance with all applicable laws and protection for the privacy and constitutional rights of individuals. The Department recognizes that other provisions of federal law may be applicable to (or may be adopted in the future with respect to) certain submitters or users of information in criminal intelligence systems. Moreover, as technological developments unfold over time in this area, experience may show that particular aspects of the requirements in this part may no longer be needed to serve their intended purpose or may even prevent desirable technological advances. Accordingly, this provision grants the flexibility to make such beneficial adaptations in particular cases or classes without the necessity to undertake a new rulemaking process. This waiver authority could only be exercised by the Attorney General or designee, in writing, upon a clear and convincing showing (28 CFR 23.20 (o)).

(9) The funding guidelines (28 CFR 23.30) are revised to permit funded intelligence systems to collect information either on organized criminal activity that represents a significant and recognized threat to the population or on criminal activity that is multi-jurisdictional in nature.

Rulemaking History On February 27, 1992, the Department of Justice, Office of Justice Programs, published a notice of proposed rulemaking in the Federal Register (57 FR 6691). The Office of Justice Programs received a total of eleven comments on the proposed regulation, seven from State agencies, two from Regional Information Sharing Systems (RISS) program fund recipients, one from a Federal agency, and one from the RISS Project Directors Association. Comments will be discussed in the order in which they address the substance of the proposed regulation.

Discussion of Comments

Title - Part 23 Comment: One commentor suggested reinserting the word "Operating" in the title of the regulation to read "Criminal Intelligence Systems Operating Policies" to reflect that the regulation applies only to policies governing system operations.

Response: Agreed. The title has been changed.

APPLICABILITY - SECTION 23.3(a)

Comment: A question was raised by one respondent as to whether the applicability of the regulation under Section 23.3(a) to systems "operating through support" under the Crime Control Act included agencies receiving any assistance funds and who operated an intelligence system or only those who received assistance funds for the specific purpose of funding the operation of an intelligence system.

Response: The regulation applies to grantees and subgrantees who receive and use Crime Control Act funds to fund the operation of an intelligence system.

Comment: Another commentor asked whether the purchase of software, office equipment, or the payment of staff salaries for a criminal intelligence system would constitute "operating through support" under the Crime Control Act.

Response: Any direct Crime Control Act fund support that contributes to the operation of a criminal intelligence system would subject the system to the operation of the policy standards during the period of fund support.

Comment: A third commentor inquired whether an agency's purchase of a telephone pen register or computer equipment to store and analyze pen register information would subject the agency or its information systems to the regulation.

Response: No, neither a pen register nor equipment to analyze telephone toll information fall under the definition of a criminal intelligence system even though they may assist an agency to produce investigative or other information for an intelligence system.

APPLICABILITY - SECTION 23.3(b)

Comment: Several commentors questioned whether information systems that are designed to collect information on criminal suspects for purposes of inquiry and analysis, and which provide for dissemination of such information, qualify as "criminal intelligence systems." One pointed out that the information qualifying for system submission could not be "unconfirmed" or "soft" intelligence. Rather, it would generally have to be: One respondent asked whether the definition of criminal intelligence system covered criminal history record information (CHRI) systems, fugitive files, or other want or warrant based information systems. investigative file-based information to meet the "reasonable suspicion" test.

Response: The character of an information system as a criminal intelligence system does not depend upon the source or categorization of the underlying information as "raw" or "soft" intelligence, preliminary investigation information, or investigative information, findings or determinations. It depends upon the purpose for which the information system exists and the type of information it contains. If the purpose of the system is to collect and share information with other law enforcement agencies on individuals reasonably suspected of involvement in criminal activity, and the information is identifying or descriptive information about the individual and the suspected criminal activity, then the system is a criminal intelligence system for purposes of the regulation. Only those criminal intelligence systems that receive, store and provide for the interagency exchange and analysis of criminal intelligence information in a manner consistent with this regulation are eligible for funding support with Crime Control Act funds.

Comment One respondent asked whether the definition of criminal intelligence system covered criminal history record information (CHRI) systems, fugitive files, or other want or warrant based information systems.

Response: No. A CHRI system contains information collected on arrests, detention, indictments, informations or other charges, dispositions, sentencing, correctional supervision, and release. It encompasses systems designed to collect, process, preserve, or disseminate such information. CHRI is factual, historical and objective information which provides a criminal justice system "profile" of an individual's past and present involvement in the criminal justice system. A fugitive file is designed to provide factual information to assist in the arrest of individuals for whom there is an outstanding want or warrant. Criminal intelligence information, by contrast, is both factual and conjectural (reasonable suspicion), current

and subjective. It is intended for law enforcement use only, to provide law enforcement officers and agencies with useful information on criminal suspects and to foster interagency coordination and cooperation. A criminal intelligence system can have criminal history record information in it as an identifier but a CHRI system would not contain the suspected criminal activity information contained in a criminal intelligence system. This distinction provides the basis for the limitations on criminal intelligence systems set forth in the operating policies. Because criminal intelligence information is both conjectural and subjective in nature, may be widely disseminated through the interagency exchange of information and cannot be accessed by criminal suspects to verify that the information is accurate and complete, the protections and limitations set forth in the regulation are necessary to protect the privacy interests of the subjects and potential subjects of a criminal intelligence system.

Comment: Another commentor asked whether a law enforcement agency's criminal intelligence information unit, located at headquarters, which authorizes no outside access to information in its intelligence system, would be subject to the regulation.

Response: No. The sharing of investigative or general file information on criminal subjects within an agency is a practice that takes place on a daily basis and is necessary for the efficient and effective operation of a law enforcement agency. Consequently, whether such a system is described as a case management or intelligence system, the regulation is not intended to apply to the exchange or sharing of such information when it takes place within a single law enforcement agency or organizational entity. For these purposes, an operational multi-jurisdictional task force would be considered a single organizational entity provided that it is established by and operates under a written memorandum of understanding or interagency agreement. The definition of "Criminal Intelligence System" has been modified to clarify this point. However, if a single agency or entity system provides access to system information to outside agencies on an inquiry or request basis, as a matter of either policy or practice, the system would qualify as a criminal intelligence system and be subject to the regulation.

Comment: A commentor questioned whether the proposed exclusion of "analytical information and work products" from the definition of "Intelligence System" was intended to exclude all dissemination of analytical results from coverage under the regulation.

Response: No. The exceptions in the proposed definition of "Intelligence System" of modus operandi files, historical telephone toll files and analytical information and work products are potentially confusing. The exceptions reflect types of data that may or may not qualify as "Criminal Intelligence Information" depending on particular facts and circumstances. Consequently, these exceptions have been deleted from the definition of "Intelligence System" in the final rule. For example, analytical information and work products that are derived from unevaluated or bulk data (i.e. information that has not been tested to determine that it meets intelligence system submission criteria) are not intelligence information if they are returned to the submitting agency. This information and its products cannot be retained, stored, or made available for dissemination in an intelligence system unless and until the information has been evaluated and determined to meet system submission criteria. The proposed definition of "Analytical Information and Work Products" in Section 23.3(b) has also been deleted. To address the above issues, the definition of "Intelligence System" has been modified to define a "Criminal Intelligence System or Intelligence System" to mean "the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information."

Comment: Several commentors raised questions regarding the concept of "evaluated data" in the definition of "Criminal Intelligence Information", requesting guidance on what criteria to use in evaluating data. Another questioned whether there needed to be an active investigation as the basis for information to fall within the definition and whether information on an individual who or organization which is not the primary subject or target of an investigation or other data source, e.g. a criminal associate or co-conspirator, can qualify as "Criminal Intelligence Information."

Response: The definition of "Criminal Intelligence Information" has been revised to reflect that data is evaluated for two purposes related to criminal intelligence system submissions: (1) to determine that it is relevant in identifying a criminal suspect and the criminal activity involved; and (2) to determine that the data meets criminal intelligence system submission criteria, including reasonable suspicion of involvement in criminal activity. As rewritten, there is no requirement that an "active investigation" is necessary. Further, the revised language makes it clear that individuals or organizations who are not primary subjects or targets can be identified in the criminal intelligence information, provided that they independently meet system submission criteria.

Comment: One commentor requested clarification of the role of the "Project" in the operation of an intelligence system, i.e. is the project required to have physical control (possession) of the information in an intelligence system or will authority over the system (operational control) suffice?

Response: Operational control over an intelligence system's intelligence information is sufficient. The regulation seeks to establish a single locus of authority and responsibility for system information. Once that principle is established, the regulation permits, for example, the establishment of remote (off premises) data bases that meet applicable security requirements.

OPERATING PRINCIPLES - SECTION 23.20(c)

Comment: One respondent took the position that "Reasonable Suspicion", as defined in Section 23.20 (c), is not necessary to the protection of individual privacy and Constitutional rights, suggesting instead that information in a funded intelligence system need only be "necessary and relevant to an agency's lawful purposes."

Response: While it is agreed that the standard suggested is appropriate for investigative or other information files maintained for use by or within an agency, the potential for national dissemination of information in intelligence information systems, coupled with the lack of access by subjects to challenge the information, justifies the reasonable suspicion standard as well as other operating principle restrictions set forth in this regulation. Also, the quality and utility of "hits" in an information system is enhanced by the reasonable suspicion requirement. Scarce resources are not wasted by agencies in coordinating information on subjects for whom information is vague, incomplete and conjectural.

Comment: The prior commentor also criticized the proposed definition of reasonable suspicion for its specific reference to an "investigative file" as the source of intelligence system information, the potential inconsistency between the concepts of "infer" and "conclude" as standards for determining whether reasonable suspicion is justified by the information available, and the use of "reasonable possibility" rather than "articulable" or "sufficient" facts as the operative standard to conclude that reasonable suspicion exists.

Response: The reference to an "investigative file" as the information source has been broadened to encompass any information source. The information available must provide a basis for the submitter to "believe" there is a reasonable possibility of the subject's involvement in the criminal activity or enterprise. The concept of a "basis to believe" requires reasoning and logic coupled with sound judgment based on experience in law enforcement rather than a mere hunch, whim, or guess. The belief that is formed, that there is a "reasonable possibility" of criminal involvement, has been retained because the proposed standard is appropriately less restrictive than that which is required to establish probable cause.

OPERATING PRINCIPLES - SECTION 23.20(d)

Comment: Section 23.20(d) prohibits the inclusion in an intelligence system of information obtained in violation of Federal, State, or local law or ordinance. Would a project be potentially liable for accepting, maintaining and disseminating such information even if it did not know that the information was illegally obtained?

Response: In addition to protecting the rights of individuals and organizations that may be subjects in a criminal intelligence system, this prohibition serves to protect a project from liability for disseminating illegally obtained information. A clear project policy that prohibits the submission of illegally obtained information, coupled with an examination of supporting information to determine that the information was obtained legally or the delegation of such authority to a properly trained participating agency, and the establishment and performance of routine inspection and audit of participating agency records, should be sufficient to shield a project from potential liability based on negligence in the performance of its intelligence information screening function.

OPERATING PRINCIPLES - SECTION 23.20(h)

Comment: One commentor requested clarification of the "periodic review" requirement in Section 23.20(h) and what constitutes an "explanation of decision to retain" information.

Response: The periodic review requirement is designed to insure that system information is accurate and as up-to-date as reasonably possible. When a review has occurred, the record is appropriately updated and notated. The explanation of decision to retain can be a variety of reasons including "active investigation", "preliminary review in progress", "subject believed still active in jurisdiction", and the like. When information that has been reviewed or updated and a determination made that it continues to meet system submission criteria, the information has been "validated" and begins a new retention period. The regulation limits the retention period to a maximum of five years without a review and validation of the information.

OPERATING PRINCIPLES - SECTION 23.20(i)

Comment: One commentor requested a definition of "remote terminal" and asked how OJP would determine whether "adequate policies and procedures" are in place to insure the continued integrity of a criminal intelligence system.

Response: A "remote terminal" is hardware that enables a participating agency to input into or access information from a project's criminal intelligence data base without the intervention of project staff. While the security requirements set forth in Section 23.20(g)(1)-(5) should minimize the threat to system integrity from unauthorized access to and the use of system information, special measures are called for when direct remote terminal access is authorized. The Office of Justice Programs will expect any request for approval of remote terminal access to include information on the following system protection measures:

1. Procedures for identification of authorized remote terminals and security of terminals;

2. Authorized access officer (remote terminal operator) identification and verification procedures;

3. Provisions for the levels of dissemination of information as directed by the submitting agency;

4. Provisions for the rejection of submissions unless critical data fields are completed;

5. Technological safeguards on system access, use, dissemination, and review and purge;

6. Physical security of the system;

7. Training and certification of system-participating agency personnel;

8. Provisions for the audit of system-participating agencies, to include: file data supporting submissions to the system; security of access terminals; and policy and procedure compliance; and

9. Documentation for audit trails of the entire system operation.

Moreover, a waiver provision has been added to ensure flexibility in adapting quickly to technological and legal changes which may impact any of the requirements contained in this regulation. See Section 23.20 (o).

Comment: Related to the above discussion, another commentor asked whether restrictions on direct remote terminal access would prohibit remote access to an "index" of information in the system.

Response: Yes. The ability to obtain all information directly from a criminal intelligence system through the use of hardware based outside the system constitutes direct remote terminal access contrary to the provisions of Section 23.20(i)(1), except as specifically approved by OJP. Thus, a hit/no hit response, if gleaned from an index, would bring a remote terminal within the scope of the requirement for OJP approval of direct remote terminal access.

Comment: One commentor pointed out that the requirement for prior OJP approval of "modifications to system design" was overly broad and could be read to require that even minor changes be submitted for approval. The commentor proposed a substitute which would limit the requirement to those modifications "that alter the system's identified goals in a way contrary to the requirements of (this regulation)."

Response: While it is agreed that the language is broad, the proposed limitation is too restrictive. The intent was that "modifications to system design" refer to "major" changes to the system, such as the nature of the information collected, the place or method of information storage, the authorized uses of information in the system, and provisions for access to system information by authorized participating agencies. This clarification has been incorporated in the regulation. In order to decentralize responsibility for approval of system design modifications, the proposed regulation has been revised to provide for approval of such modifications by the grantor agency rather than OJP. A similar change has been made to Section 23.20(j).

OPERATING PRINCIPLES - SECTION 23.20(n)

Comment: Several commentors expressed concern with the verification procedures set forth in Section 23.20(n). One suggested that file information cannot "verify" the correctness of submissions but instead serves to "document" or "substantiate" its correctness. Another proposed deleting the requirements that (1) files maintained by participating agencies to support system submissions be subject to the operating principles, and (2) participating agencies are authorized to maintain such files separately from other agency files. The first requirement conflicts with the normal investigative procedures of a law enforcement agency in that all information in agency source files cannot meet the operating principles, particularly the reasonable suspicion and relevancy requirements. The important principle is that the information which is gleaned from an agency's source files and submitted to the system meet the operating principles. The second requirement has no practical value. At most, it results in the creation of duplicative files or in submission information being segregated from source files.

Response: OJP agrees with both comments. The word "documents" has been substituted for "verifies" and the provisions subjecting participating agency source files to the operating principles and authorizing maintenance of separate files have been deleted. Projects should use their audit and inspection access to agency source files to document the correctness of participating agency submissions on a sample basis.

FUNDING GUIDELINES - SECTION 23.30(b)

Comment: One commentor asked: Who defines the areas of criminal activity that "represent a significant and recognized threat to the population?"

Response: The determination of areas of criminal activity focus and priority are matters for projects, project policy boards and member agencies to determine, provided that the additional regulatory requirements set forth in Section 23.30(b) are met.

MONITORING AND AUDITING OF GRANTS - SECTION 23.40(a)

Comment: One commentor asked: "Who is responsible for developing the specialized monitoring and audit of awards for intelligence systems to insure compliance with the operating principles"?

Response: The grantor agency (the agency awarding a sub-grant to support an intelligence system) shall establish and approve a plan for specialized monitoring and audit of sub-awards prior to award. For the BJA Formula Grant Program, the State agency receiving the award from BJA is the grantor agency. Technical assistance and support in establishing a monitoring and audit plan is available through BJA.

INFORMATION ON JUVENILES

Comment: Can intelligence information pertaining to a juvenile who otherwise meets criminal intelligence system submission criteria be entered into an intelligence data base?

Response: There is no limitation or restriction on entering intelligence information on juvenile subjects set forth in Federal law or regulation. However, State law may restrict or prohibit the maintenance or dissemination of such information by its law enforcement agencies. Therefore, State laws should be carefully reviewed to determine their impact on this practice and appropriate project policies adopted.

Executive Order 12291 These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises.

Regulatory Flexibility Act These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act.

Paperwork Reduction Act There are no collection of information requirements contained in the proposed regulation.

List of Subjects in 28 CFR Part 23 Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement. For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows:

PART 23--CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES Sec.

1. Purpose.
2. Background.
3. Applicability.
4. Operating principles.
5. Funding guidelines.
6. Monitoring and auditing of grants for the funding of intelligence systems.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose. The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430,

Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background. It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy. **.** (a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity. (b) A project shall not collect or maintain criminal intelligence 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) be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§ 23.3 Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjurisdictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project Validation of Information

§ 23.20 Operating principles

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence 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 or organization is involved in a definable criminal activity or enterprise. In an interjurisdictional 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) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State,

or local laws, 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.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f) (1) Except as noted in paragraph (f) (2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f) (1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is 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 participating agency which is subject to routine inspection and audit procedures established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project; (3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization; (4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster; (5) The project must promulgate rules and regulations 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 (6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require 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, date of review and explanation of decision to retain. 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. (i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and (2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines. The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or (3) Are not limited to one jurisdiction.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

(1) assume official responsibility and accountability for actions taken in the name of the joint entity, and

(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20. The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.

Laurie Robinson
Acting Assistant Attorney General
Office of Justice Programs
(FR Doc. 93-22614 Filed 9-15-93; 8:45 am)

1998 Policy Clarification

AGENCY: Bureau of Justice Assistance (BJA), Office of Justice Programs (OJP), Justice.

ACTION: Clarification of policy.

SUMMARY: The current policy governing the entry of identifying information into criminal intelligence sharing systems requires clarification. This policy clarification is to make clear that the entry of individuals, entities and organizations, and locations that do not otherwise meet the requirements of reasonable suspicion is appropriate when it is done solely for the purposes of criminal identification or is germane to the criminal subject's criminal activity. Further, the definition of "criminal intelligence system" is clarified.

EFFECTIVE DATE: This clarification is effective December 30, 1998.

FOR FURTHER INFORMATION CONTACT: Paul Kendall, General Counsel, Office of Justice Programs, 810 7th Street NW, Washington, DC 20531, (202) 307-6235.

SUPPLEMENTARY INFORMATION: The operation of criminal intelligence information systems is governed by 28 CFR Part 23. This regulation was written to both protect the privacy rights of individuals and to encourage and expedite the exchange of criminal intelligence information between and among law enforcement agencies of different jurisdictions. Frequent interpretations of the regulation, in the form of policy guidance and correspondence, have been the primary method of ensuring that advances in technology did not hamper its effectiveness.

Comments

The clarification was opened to public comment. Comments expressing unreserved support for the clarification were received from two Regional Intelligence Sharing Systems (RISS) and five states. A comment from the Chairperson of a RISS, relating to the use of identifying information to begin new investigations, has been incorporated. A single negative comment was received, but was not addressed to the subject of this clarification.

Use of Identifying Information

28 CFR 23.3(b)(3) states that criminal intelligence information that can be put into a criminal intelligence sharing system is "information relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and . . . meets criminal intelligence system submission criteria." Further, 28 CFR 23.20(a) states that a system shall only collect information on an individual if "there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity." 28 CFR 23.20(b) extends that limitation to [page 71753] collecting information on groups and corporate entities.

In an effort to protect individuals and organizations from the possible taint of having their names in intelligence systems (as defined at 28 CFR Sec. 23.3(b)(1)), the Office of Justice Programs has previously interpreted this section to allow information to be placed in a system only if that information independently meets the requirements of the regulation. Information that might be vital to identifying potential criminals, such as favored locations and companions, or names of family members, has been excluded from the systems. This policy has hampered the effectiveness of many criminal intelligence sharing systems.

Given the swiftly changing nature of modern technology and the expansion of the size and complexity of criminal organizations, the Bureau of Justice Assistance (BJA) has determined that it is necessary to clarify this element of 28 CFR Part 23. Many criminal intelligence databases are now employing "Comment" or "Modus Operandi" fields whose value would be greatly enhanced by the ability to store more detailed and wide-ranging identifying information. This may include names and limited data about people and organizations that are not suspected of any criminal activity or involvement, but merely aid in the

identification and investigation of a criminal suspect who independently satisfies the reasonable suspicion standard.

Therefore, BJA issues the following clarification to the rules applying to the use of identifying information. Information that is relevant to the identification of a criminal suspect or to the criminal activity in which the suspect is engaged may be placed in a criminal intelligence database, provided that (1) appropriate disclaimers accompany the information noting that is strictly identifying information, carrying no criminal connotations; (2) identifying information may not be used as an independent basis to meet the requirement of reasonable suspicion of involvement in criminal activity necessary to create a record or file in a criminal intelligence system; and (3) the individual who is the criminal suspect identified by this information otherwise meets all requirements of 28 CFR Part 23. This information may be a searchable field in the intelligence system.

For example: A person reasonably suspected of being a drug dealer is known to conduct his criminal activities at the fictional "Northwest Market." An agency may wish to note this information in a criminal intelligence database, as it may be important to future identification of the suspect. Under the previous interpretation of the regulation, the entry of "Northwest Market" would not be permitted, because there was no reasonable suspicion that the "Northwest Market" was a criminal organization. Given the current clarification of the regulation, this will be permissible, provided that the information regarding the "Northwest Market" was clearly noted to be non-criminal in nature. For example, the data field in which "Northwest Market" was entered could be marked "Non-Criminal Identifying Information," or the words "Northwest Market" could be followed by a parenthetical comment such as "This organization has been entered into the system for identification purposes only - it is not suspected of any criminal activity or involvement." A criminal intelligence system record or file could not be created for "Northwest Market" solely on the basis of information provided, for example, in a comment field on the suspected drug dealer. Independent information would have to be obtained as a basis for the opening of a new criminal intelligence file or record based on reasonable suspicion on "Northwest Market." Further, the fact that other individuals frequent "Northwest Market" would not necessarily establish reasonable suspicion for those other individuals, as it relates to criminal intelligence systems.

The Definition of a "Criminal Intelligence System"

The definition of a "criminal intelligence system" is given in 28 CFR 23.3(b)(1) as the "arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information . . . ." Given the fact that cross-database searching techniques are now common-place, and given the fact that multiple databases may be contained on the same computer system, BJA has determined that this definition needs clarification, specifically to differentiate between criminal intelligence systems and non-intelligence systems.

The comments to the 1993 revision of 28 CFR Part 23 noted that "the term 'intelligence system' is redefined to clarify the fact that historical telephone toll files, analytical information, and work products that are not either retained, stored, or exchanged and criminal history record information or identification (fingerprint) systems are excluded from the definition, and hence are not covered by the regulation . . . ." 58 FR 48448-48449 (Sept. 16, 1993.) The comments further noted that materials that "may assist an agency to produce investigative or other information for an intelligence system . . ." do not necessarily fall under the regulation. Id.

The above rationale for the exclusion of non-intelligence information sources from the definition of "criminal intelligence system," suggests now that, given the availability of more modern non-intelligence information sources such as the Internet, newspapers, motor vehicle administration records, and other public record information on-line, such sources shall not be considered part of criminal intelligence systems, and shall not be covered by this regulation, even if criminal intelligence systems access such sources during searches on criminal suspects. Therefore, criminal intelligence systems may conduct searches across the spectrum of non-intelligence systems without those systems being brought under 28 CFR Part 23. There is also no limitation on such non-intelligence information being stored on the same computer system as criminal intelligence information, provided that sufficient precautions are in place to separate the two types of information and to make it clear to operators and users of the information that two different types of information are being accessed.

Such precautions should be consistent with the above clarification of the rule governing the use of identifying information. This could be accomplished, for example, through the use of multiple windows, differing colors of data or clear labeling of the nature of information displayed.

Additional guidelines will be issued to provide details of the above clarifications as needed.

Dated: December 22, 1998.

Nancy Gist Director,
Bureau of Justice Assistance
[FR Doc. 98-34547 Filed 12-29-98; 8:45 am]
BILLING CODE 4410-18-P

Kansas Statute Annotated Chapter 45

45-220
Chapter 45.--PUBLIC RECORDS, DOCUMENTS AND INFORMATION
Article 2.--RECORDS OPEN TO PUBLIC

45-220. Procedures for obtaining access to or copies of records; request; office hours; provision of information on procedures. (a) Each public agency shall adopt procedures to be followed in requesting access to and obtaining copies of public records, which procedures shall provide full access to public records, protect public records from damage and disorganization, prevent excessive disruption of the agency's essential functions, provide assistance and information upon request and insure efficient and timely action in response to applications for inspection of public records.

(b) A public agency may require a written request for inspection of public records but shall not otherwise require a request to be made in any particular form. Except as otherwise provided by subsection (c), a public agency shall not require that a request contain more information than the requester's name and address and the information necessary to ascertain the records to which the requester desires access and the requester's right of access to the records. A public agency may require proof of identity of any person requesting access to a public record. No request shall be returned, delayed or denied because of any technicality unless it is impossible to determine the records to which the requester desires access.

(c) If access to public records of an agency or the purpose for which the records may be used is limited pursuant to K.S.A. 45-221 or K.S.A. 2008 Supp. 45-230, and amendments thereto, the agency may require a person requesting the records or information therein to provide written certification that:

(1) The requester has a right of access to the records and the basis of that right; or

(2) the requester does not intend to, and will not: (A) Use any list of names or addresses contained in or derived from the records or information for the purpose of selling or offering for sale any property or service to any person listed or to any person who resides at any address listed; or (B) sell, give or otherwise make available to any person any list of names or addresses contained in or derived from the records or information for the purpose of allowing that person to sell or offer for sale any property or service to any person listed or to any person who resides at any address listed.

(d) A public agency shall establish, for business days when it does not maintain regular office hours, reasonable hours when persons may inspect and obtain copies of the agency's records. The public agency may require that any person desiring to inspect or obtain copies of the agency's records during such hours so notify the agency, but such notice shall not be required to be in writing and shall not be required to be given more than 24 hours prior to the hours established for inspection and obtaining copies.

(e) Each official custodian of public records shall designate such persons as necessary to carry out the duties of custodian under this act and shall ensure that a custodian is available during regular business hours of the public agency to carry out such duties.

(f) Each public agency shall provide, upon request of any person, the following information:

(1) The principal office of the agency, its regular office hours and any additional hours established by the agency pursuant to subsection (c).

(2) The title and address of the official custodian of the agency's records and of any other custodian who is ordinarily available to act on requests made at the location where the information is displayed.

(3) The fees, if any, charged for access to or copies of the agency's records.

(4) The procedures to be followed in requesting access to and obtaining copies of the agency's records, including procedures for giving notice of a desire to inspect or obtain copies of records during hours established by the agency pursuant to subsection (c).

History: L. 1984, ch. 187, § 6; L. 1984, ch. 282, §3; L. 2003, ch. 126, § 2; July 1.

45-221
Chapter 45.--PUBLIC RECORDS, DOCUMENTS AND INFORMATION
Article 2.--RECORDS OPEN TO PUBLIC

45-221. Certain records not required to be open; separation of open and closed information required; statistics and records over 70 years old open. (a) Except to the extent disclosure is otherwise required by law, a public agency shall not be required to disclose:

(1) Records the disclosure of which is specifically prohibited or restricted by federal law, state statute or rule of the Kansas supreme court or rule of the senate committee on confirmation oversight relating to information submitted to the committee pursuant to K.S.A. 2008 Supp. 75-4315d, and amendments thereto, or the disclosure of which is prohibited or restricted pursuant to specific authorization of federal law, state statute or rule of the Kansas supreme court or rule of the senate committee on confirmation oversight relating to information submitted to the committee pursuant to K.S.A. 2008 Supp. 75-4315d, and amendments thereto, to restrict or prohibit disclosure.

(2) Records which are privileged under the rules of evidence, unless the holder of the privilege consents to the disclosure.

(3) Medical, psychiatric, psychological or alcoholism or drug dependency treatment records which pertain to identifiable patients.

(4) Personnel records, performance ratings or individually identifiable records pertaining to employees or applicants for employment, except that this exemption shall not apply to the names, positions, salaries or actual compensation employment contracts or employment-related contracts or agreements and lengths of service of officers and employees of public agencies once they are employed as such.

(5) Information which would reveal the identity of any undercover agent or any informant reporting a specific violation of law.

(6) Letters of reference or recommendation pertaining to the character or qualifications of an identifiable individual, except documents relating to the appointment of persons to fill a vacancy in an elected office.

(7) Library, archive and museum materials contributed by private persons, to the extent of any limitations imposed as conditions of the contribution.

(8) Information which would reveal the identity of an individual who lawfully makes a donation to a public agency, if anonymity of the donor is a condition of the donation, except if the donation is intended for or restricted to providing remuneration or personal tangible benefit to a named public officer or employee.

(9) Testing and examination materials, before the test or examination is given or if it is to be given again, or records of individual test or examination scores, other than records which show only passage or failure and not specific scores.

(10) Criminal investigation records, except as provided herein. The district court, in an action brought pursuant to K.S.A. 45-222, and amendments thereto, may order disclosure of such records, subject to such conditions as the court may impose, if the court finds that disclosure:

(A) Is in the public interest;

(B) would not interfere with any prospective law enforcement action, criminal investigation or prosecution;

(C) would not reveal the identity of any confidential source or undercover agent;

(D) would not reveal confidential investigative techniques or procedures not known to the general public;

(E) would not endanger the life or physical safety of any person; and

(F) would not reveal the name, address, phone number or any other information which specifically and individually identifies the victim of any sexual offense in article 35 of chapter 21 of the Kansas Statutes Annotated, and amendments thereto.

If a public record is discretionarily closed by a public agency pursuant to this subsection, the record custodian, upon request, shall provide a written citation to the specific provisions of paragraphs (A) through (F) that necessitate closure of that public record.

(11) Records of agencies involved in administrative adjudication or civil litigation, compiled in the process of detecting or investigating violations of civil law or administrative rules and regulations, if disclosure would interfere with a prospective administrative adjudication or civil litigation or reveal the identity of a confidential source or undercover agent.

(12) Records of emergency or security information or procedures of a public agency, or plans, drawings, specifications or related information for any building or facility which is used for purposes requiring security measures in or around the building or facility or which is used for the generation or transmission of power, water, fuels or communications, if disclosure would jeopardize security of the public agency, building or facility.

(13) The contents of appraisals or engineering or feasibility estimates or evaluations made by or for a public agency relative to the acquisition of property, prior to the award of formal contracts therefor.

(14) Correspondence between a public agency and a private individual, other than correspondence which is intended to give notice of an action, policy or determination relating to any regulatory, supervisory or enforcement responsibility of the public agency or which is widely distributed to the public by a public agency and is not specifically in response to communications from such a private individual.

(15) Records pertaining to employer-employee negotiations, if disclosure would reveal information discussed in a lawful executive session under K.S.A. 75-4319, and amendments thereto.

(16) Software programs for electronic data processing and documentation thereof, but each public agency shall maintain a register, open to the public, that describes:

(A) The information which the agency maintains on computer facilities; and

(B) the form in which the information can be made available using existing computer programs.

(17) Applications, financial statements and other information submitted in connection with applications for student financial assistance where financial need is a consideration for the award.

(18) Plans, designs, drawings or specifications which are prepared by a person other than an employee of a public agency or records which are the property of a private person.

(19) Well samples, logs or surveys which the state corporation commission requires to be filed by persons who have drilled or caused to be drilled, or are drilling or causing to be drilled, holes for the purpose of discovery or production of oil or gas, to the extent that disclosure is limited by rules and regulations of the state corporation commission.

(20) Notes, preliminary drafts, research data in the process of analysis, unfunded grant proposals, memoranda, recommendations or other records in which opinions are expressed or policies or actions are proposed, except that this exemption shall not apply when such records are publicly cited or identified in an open meeting or in an agenda of an open meeting.

(21) Records of a public agency having legislative powers, which records pertain to proposed legislation or amendments to proposed legislation, except that this exemption shall not apply when such records are:

(A) Publicly cited or identified in an open meeting or in an agenda of an open meeting; or

(B) distributed to a majority of a quorum of any body which has authority to take action or make recommendations to the public agency with regard to the matters to which such records pertain.

(22) Records of a public agency having legislative powers, which records pertain to research prepared for one or more members of such agency, except that this exemption shall not apply when such records are:

(A) Publicly cited or identified in an open meeting or in an agenda of an open meeting; or

(B) distributed to a majority of a quorum of any body which has authority to take action or make recommendations to the public agency with regard to the matters to which such records pertain.

(23) Library patron and circulation records which pertain to identifiable individuals.

(24) Records which are compiled for census or research purposes and which pertain to identifiable individuals.

(25) Records which represent and constitute the work product of an attorney.

(26) Records of a utility or other public service pertaining to individually identifiable residential customers of the utility or service, except that information concerning billings for specific individual customers named by the requester shall be subject to disclosure as provided by this act.

(27) Specifications for competitive bidding, until the specifications are officially approved by the public agency.

(28) Sealed bids and related documents, until a bid is accepted or all bids rejected.

(29) Correctional records pertaining to an identifiable inmate or release, except that:

(A) The name; photograph and other identifying information; sentence data; parole eligibility date; custody or supervision level; disciplinary record; supervision violations; conditions of supervision, excluding requirements pertaining to mental health or substance abuse counseling; location of facility where incarcerated or location of parole office maintaining supervision and address of a releasee whose crime was committed after the effective date of this act shall be subject to disclosure to any person other than another inmate or releasee, except that the disclosure of the location of an inmate transferred to another state pursuant to the interstate corrections compact shall be at the discretion of the secretary of corrections;

(B) the ombudsman of corrections, the attorney general, law enforcement agencies, counsel for the inmate to whom the record pertains and any county or district attorney shall have access to correctional records to the extent otherwise permitted by law;

(C) the information provided to the law enforcement agency pursuant to the sex offender registration act, K.S.A. 22-4901 et seq., and amendments thereto, shall be subject to disclosure to any person, except that the name, address, telephone number or any other information which specifically and individually identifies the victim of any offender required to register as provided by the Kansas offender registration act, K.S.A. 22-4901 et seq. and amendments thereto, shall not be disclosed; and

(D) records of the department of corrections regarding the financial assets of an offender in the custody of the secretary of corrections shall be subject to disclosure to the victim, or such victim's family, of the crime for which the inmate is in custody as set forth in an order of restitution by the sentencing court.

(30) Public records containing information of a personal nature where the public disclosure thereof would constitute a clearly unwarranted invasion of personal privacy.

(31) Public records pertaining to prospective location of a business or industry where no previous public disclosure has been made of the business' or industry's interest in locating in, relocating within or expanding within the state. This exception shall not include those records pertaining to application of agencies for permits or licenses necessary to do business or to expand business operations within this state, except as otherwise provided by law.

(32) Engineering and architectural estimates made by or for any public agency relative to public improvements.

(33) Financial information submitted by contractors in qualification statements to any public agency.

(34) Records involved in the obtaining and processing of intellectual property rights that are expected to be, wholly or partially vested in or owned by a state educational institution, as defined in K.S.A. 76-711, and amendments thereto, or an assignee of the institution organized and existing for the benefit of the institution.

(35) Any report or record which is made pursuant to K.S.A. 65-4922, 65-4923 or 65-4924, and amendments thereto, and which is privileged pursuant to K.S.A. 65-4915 or 65-4925, and amendments thereto.

(36) Information which would reveal the precise location of an archeological site.

(37) Any financial data or traffic information from a railroad company, to a public agency, concerning the sale, lease or rehabilitation of the railroad's property in Kansas.

(38) Risk-based capital reports, risk-based capital plans and corrective orders including the working papers and the results of any analysis filed with the commissioner of insurance in accordance with K.S.A. 40-2c20 and 40-2d20 and amendments thereto.

(39) Memoranda and related materials required to be used to support the annual actuarial opinions submitted pursuant to subsection (b) of K.S.A. 40-409, and amendments thereto.

(40) Disclosure reports filed with the commissioner of insurance under subsection (a) of K.S.A. 40-2,156, and amendments thereto.

(41) All financial analysis ratios and examination synopses concerning insurance companies that are submitted to the commissioner by the national association of insurance commissioners' insurance regulatory information system.

(42) Any records the disclosure of which is restricted or prohibited by a tribal-state gaming compact.

(43) Market research, market plans, business plans and the terms and conditions of managed care or other third party contracts, developed or entered into by the university of Kansas medical center in the operation and management of the university hospital which the chancellor of the university of Kansas or the

chancellor's designee determines would give an unfair advantage to competitors of the university of Kansas medical center.

(44) The amount of franchise tax paid to the secretary of revenue or the secretary of state by domestic corporations, foreign corporations, domestic limited liability companies, foreign limited liability companies, domestic limited partnership, foreign limited partnership, domestic limited liability partnerships and foreign limited liability partnerships.

(45) Records, other than criminal investigation records, the disclosure of which would pose a substantial likelihood of revealing security measures that protect: (A) Systems, facilities or equipment used in the production, transmission or distribution of energy, water or communications services; (B) transportation and sewer or wastewater treatment systems, facilities or equipment; or (C) private property or persons, if the records are submitted to the agency. For purposes of this paragraph, security means measures that protect against criminal acts intended to intimidate or coerce the civilian population, influence government policy by intimidation or coercion or to affect the operation of government by disruption of public services, mass destruction, assassination or kidnapping. Security measures include, but are not limited to, intelligence information, tactical plans, resource deployment and vulnerability assessments.

(46) Any information or material received by the register of deeds of a county from military discharge papers (DD Form 214). Such papers shall be disclosed: To the military dischargee; to such dischargee's immediate family members and lineal descendants; to such dischargee's heirs, agents or assigns; to the licensed funeral director who has custody of the body of the deceased dischargee; when required by a department or agency of the federal or state government or a political subdivision thereof; when the form is required to perfect the claim of military service or honorable discharge or a claim of a dependent of the dischargee; and upon the written approval of the commissioner of veterans affairs, to a person conducting research.

(47) Information that would reveal the location of a shelter or a safehouse or similar place where persons are provided protection from abuse.

(b) Except to the extent disclosure is otherwise required by law or as appropriate during the course of an administrative proceeding or on appeal from agency action, a public agency or officer shall not disclose financial information of a taxpayer which may be required or requested by a county appraiser or the director of property valuation to assist in the determination of the value of the taxpayer's property for ad valorem taxation purposes; or any financial information of a personal nature required or requested by a public agency or officer, including a name, job description or title revealing the salary or other compensation of officers, employees or applicants for employment with a firm, corporation or agency, except a public agency. Nothing contained herein shall be construed to prohibit the publication of statistics, so classified as to prevent identification of particular reports or returns and the items thereof.

(c) As used in this section, the term "cited or identified" shall not include a request to an employee of a public agency that a document be prepared.

(d) If a public record contains material which is not subject to disclosure pursuant to this act, the public agency shall separate or delete such material and make available to the requester that material in the public record which is subject to disclosure pursuant to this act. If a public record is not subject to disclosure because it pertains to an identifiable individual, the public agency shall delete the identifying portions of the record and make available to the requester any remaining portions which are subject to disclosure pursuant to this act, unless the request is for a record pertaining to a specific individual or to such a limited group of individuals that the individuals' identities are reasonably ascertainable, the public agency shall not be required to disclose those portions of the record which pertain to such individual or individuals.

(e) The provisions of this section shall not be construed to exempt from public disclosure statistical information not descriptive of any identifiable person.

(f) Notwithstanding the provisions of subsection (a), any public record which has been in existence more than 70 years shall be open for inspection by any person unless disclosure of the record is specifically prohibited or restricted by federal law, state statute or rule of the Kansas supreme court or by a policy adopted pursuant to K.S.A. 72-6214, and amendments thereto.

(g) Any confidential records or information relating to security measures provided or received under the provisions of subsection (a)(45) shall not be subject to subpoena, discovery or other demand in any administrative, criminal or civil action.

History: L. 1984, ch. 187, § 7; L. 1984, ch. 282, § 4; L. 1986, ch. 193, § 1; L. 1987, ch. 176, § 4; L. 1989, ch. 154, § 1; L. 1991, ch. 149, § 12; L. 1994, ch. 107, § 8; L. 1995, ch. 44, § 1; L. 1995, ch. 257, § 6; L. 1996, ch. 256, § 15; L. 1997, ch. 126, § 44; L. 1997, ch. 181, § 15; L. 2000, ch. 156, § 3; L. 2001, ch. 211, § 13; L. 2002, ch. 178, § 1; L. 2003, ch. 109, § 22; L. 2004, ch. 171, § 30; L. 2005, ch. 126, § 1; L. 2008, ch. 121, § 4; July 1.

Revised Missouri State Statute Chapter 610

610.021. Closed meetings and closed records authorized when, exceptions.

Except to the extent disclosure is otherwise required by law, a public governmental body is authorized to close meetings, records and votes, to the extent they relate to the following:

(1) Legal actions, causes of action or litigation involving a public governmental body and any confidential or privileged communications between a public governmental body or its representatives and its attorneys. However, any minutes, vote or settlement agreement relating to legal actions, causes of action or litigation involving a public governmental body or any agent or entity representing its interests or acting on its behalf or with its authority, including any insurance company acting on behalf of a public government body as its insured, shall be made public upon final disposition of the matter voted upon or upon the signing by the parties of the settlement agreement, unless, prior to final disposition, the settlement agreement is ordered closed by a court after a written finding that the adverse impact to a plaintiff or plaintiffs to the action clearly outweighs the public policy considerations of section 610.011, however, the amount of any moneys paid by, or on behalf of, the public governmental body shall be disclosed; provided, however, in matters involving the exercise of the power of eminent domain, the vote shall be announced or become public immediately following the action on the motion to authorize institution of such a legal action. Legal work product shall be considered a closed record;

(2) Leasing, purchase or sale of real estate by a public governmental body where public knowledge of the transaction might adversely affect the legal consideration therefor. However, any minutes, vote or public record approving a contract relating to the leasing, purchase or sale of real estate by a public governmental body shall be made public upon execution of the lease, purchase or sale of the real estate;

(3) Hiring, firing, disciplining or promoting of particular employees by a public governmental body when personal information about the employee is discussed or recorded. However, any vote on a final decision, when taken by a public governmental body, to hire, fire, promote or discipline an employee of a public governmental body shall be made available with a record of how each member voted to the public within seventy-two hours of the close of the meeting where such action occurs; provided, however, that any employee so affected shall be entitled to prompt notice of such decision during the seventy-two-hour period before such decision is made available to the public. As used in this subdivision, the term **"personal information"** means information relating to the performance or merit of individual employees;

(4) The state militia or National Guard or any part thereof;

(5) Nonjudicial mental or physical health proceedings involving identifiable persons, including medical, psychiatric, psychological, or alcoholism or drug dependency diagnosis or treatment;

(6) Scholastic probation, expulsion, or graduation of identifiable individuals, including records of individual test or examination scores; however, personally identifiable student records maintained by public educational institutions shall be open for inspection by the parents, guardian or other custodian of students under the age of eighteen years and by the parents, guardian or other custodian and the student if the student is over the age of eighteen years;

(7) Testing and examination materials, before the test or examination is given or, if it is to be given again, before so given again;

(8) Welfare cases of identifiable individuals;

(9) Preparation, including any discussions or work product, on behalf of a public governmental body or its representatives for negotiations with employee groups;

(10) Software codes for electronic data processing and documentation thereof;

(11) Specifications for competitive bidding, until either the specifications are officially approved by the public governmental body or the specifications are published for bid;

(12) Sealed bids and related documents, until the bids are opened; and sealed proposals and related documents or any documents related to a negotiated contract until a contract is executed, or all proposals are rejected;

(13) Individually identifiable personnel records, performance ratings or records pertaining to employees or applicants for employment, except that this exemption shall not apply to the names, positions, salaries and lengths of service of officers and employees of public agencies once they are employed as such, and the names of private sources donating or contributing money to the salary of a chancellor or president at all public colleges and universities in the state of Missouri and the amount of money contributed by the source;

(14) Records which are protected from disclosure by law;

(15) Meetings and public records relating to scientific and technological innovations in which the owner has a proprietary interest;

(16) Records relating to municipal hotlines established for the reporting of abuse and wrongdoing;

(17) Confidential or privileged communications between a public governmental body and its auditor, including all auditor work product; however, all final audit reports issued by the auditor are to be considered open records pursuant to this chapter;

(18) Operational guidelines and policies developed, adopted, or maintained by any public agency responsible for law enforcement, public safety, first response, or public health for use in responding to or preventing any critical incident which is or appears to be terrorist in nature and which has the potential to endanger individual or public safety or health. Nothing in this exception shall be deemed to close information regarding expenditures, purchases, or contracts made by an agency in implementing these guidelines or policies. When seeking to close information pursuant to this exception, the agency shall affirmatively state in writing that disclosure would impair its ability to protect the safety or health of persons, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records. This exception shall sunset on December 31, 2008;

(19) Existing or proposed security systems and structural plans of real property owned or leased by a public governmental body, and information that is voluntarily submitted by a nonpublic entity owning or operating an infrastructure to any public governmental body for use by that body to devise plans for protection of that infrastructure, the public disclosure of which would threaten public safety:

> **(a)** Records related to the procurement of or expenditures relating to security systems purchased with public funds shall be open;
>
> **(b)** When seeking to close information pursuant to this exception, the public governmental body shall affirmatively state in writing that disclosure would impair the public governmental body's ability to protect the security or safety of persons or real property, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records;
>
> **(c)** Records that are voluntarily submitted by a nonpublic entity shall be reviewed by the receiving agency within ninety days of submission to determine if retention of the document is necessary in furtherance of a state security interest. If retention is not necessary, the documents shall be returned to the nonpublic governmental body or destroyed;
>
> **(d)** This exception shall sunset on December 31, 2008;

(20) Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or

unlawful disruption of a computer, computer system, computer network, or telecommunications network of a public governmental body. This exception shall not be used to limit or deny access to otherwise public records in a file, document, data file or database containing public records. Records related to the procurement of or expenditures relating to such computer, computer system, computer network, or telecommunications network, including the amount of moneys paid by, or on behalf of, a public governmental body for such computer, computer system, computer network, or telecommunications network shall be open; and

(21) Credit card numbers, personal identification numbers, digital certificates, physical and virtual keys, access codes or authorization codes that are used to protect the security of electronic transactions between a public governmental body and a person or entity doing business with a public governmental body. Nothing in this section shall be deemed to close the record of a person or entity using a credit card held in the name of a public governmental body or any record of a transaction made by a person using a credit card or other method of payment for which reimbursement is made by a public governmental body.

(L. 1987 S.B. 2, A.L. 1993 H.B. 170, A.L. 1995 H.B. 562, A.L. 1998 H.B. 1095, A.L. 2002 S.B. 712, A.L. 2004 S.B. 1020, et al., A.L. 2008 H.B. 1450, A.L. 2009 H.B. 191)
*Subdivisions 18 and 19 of this section sunset 12-31-12
CROSS REFERENCE:
Child's school records to be released to parents, attorney's fees and costs assessed, when, RSMo 452.375