SAINT LOUIS FUSION CENTER
TERRORISM EARLY WARNING GROUP

PRIVACY, CIVIL LIBERTIES, AND CIVIL RIGHTS POLICY

JANUARY 2023
REVISION

Table of Contents

Table of Contents

I. Mission/Purpose

I-1. The mission of the Saint Louis Fusion Center--Terrorism Early Warning Group (referred to in this document as the STLFC) is to responsibly gather, receive, evaluate, analyze, and disseminate information and intelligence data (records) in order to detect, prevent, and respond to threats and incidents of terrorist and criminal activity in the Saint Louis, Missouri, region (generally understood as the Saint Louis Urban Area Security Initiative, or "UASI"), while adhering to appropriate and applicable privacy and civil liberty safeguards established by law and as outlined (a) in the DHS/DOJ Privacy, Civil Rights, and Civil Liberties Policy Template document (March 2019) and (b) in the Fair Information Practice Principles (FIPPs) (see Apdx. D) and the Organization for Economic Cooperation and Development (OECD) Fair Information Principles. The STLFC mission expressly includes the safeguarding of individual and group privacy, civil rights, and civil liberties, lawfully exercised, and thus includes mitigating criminal and terrorist activities and facilitating responses to natural and man-made disasters in ways that enhance public safety and health and promote and protect the concept of ordered liberty. The STLFC regards protection of privacy and constitutional rights as both a welcome obligation of government officials and a crucial component of the long-term success of criminal- and terrorism-intelligence sharing. The STLFC's public safety efforts and safeguarding of privacy, civil rights, and civil liberties are complementary, intertwined components of a single mission.

I-2. The purpose of this privacy, civil rights, and civil liberties protection policy is to promote STLFC and user conduct that

(a) complies with applicable federal, state, tribal, and local law (see this policy document's Appendix B, Terms and Definitions, as well as Appendix C, Applicable Federal and State Regulations) and

(b) assists the STLFC and its users in:

- Increasing public safety and improving national, state, regional, and local security,
- Minimizing the threat and risk of injury to specific individuals,
- Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health,
- Minimizing the threat and risk of damage to real or personal property,
- Promoting individual and group privacy, civil rights, civil liberties, and other protected interests,
- Protecting the integrity of criminal investigation, criminal intelligence, and justice system processes and information,
- Concurrently encouraging individuals and groups to trust and cooperate with the criminal justice system, and minimizing their reluctance to use or cooperate with the system,
- Supporting the role of the justice system in society,
- Promoting governmental legitimacy and accountability,
- Not unduly burdening the ongoing business of the justice system, and
- Making the most effective use of public resources allocated to public safety agencies

II. Scope and Compliance

II-1. All STLFC employees, whether full, part-time, or temporarily assigned, will be trained in and comply with this policy. Internal STLFC operating policies govern the operations and comply with all applicable laws protecting privacy, civil rights, and civil liberties, including but not limited to those listed in Appendix C. Chief among these laws are the federal policy standards governing criminal intelligence systems, 28 CFR Part 23; the Missouri Sunshine Law, Missouri Revised Statutes, Ch. 610, and sections 109.180-.190 and 407.1500; the Illinois State Records Act, 5 ILCS 160; and applicable U.S. and state constitutional provisions.

Agencies and individual users of STLFC work products are also required to comply with applicable sections of this policy and to provide STLFC with their written electronic or hard-copy (a) acknowledgement of review of this policy, and (b) agreement to comply with this policy. Additional notifications of this requirement will be made, as appropriate, by an attachment to or notation on individual work products.

All STLFC (i) personnel, (ii) users, (iii) personnel providing information technology services, (iv) private contractors, and (v) participating agencies will be directed to review this policy, must agree in electronic or hard-copy writing timely conveyed to the STLFC to comply with applicable provisions, and will comply with all federal, state, and local privacy laws cited in Appendix C of this policy, as applicable. The STLFC will provide a printed or electronic copy of this policy to all STLFC and non-STLFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized users.

All will comply with the STLFC's privacy policy concerning the information the STLFC collects, receives, maintains, archives, accesses, or discloses to STLFC personnel, government agencies (including Information Sharing Environment (ISE) participating agencies and LPRD- and/or SMRT-Project-participating agencies), and participating justice and public safety agencies and personnel, as well as to private contractors and the general public. An agreement, either in hard-copy or electronic format, will be signed to indicate an understanding of the privacy policy and of the obligation to comply with it. The text of this agreement is contained in APPENDIX A of this document.

II-2. STLFC will make a copy of this policy available to any interested party, public or private, as a downloadable .pdf file at www.STLFC.gov.

II-3. The STLFC will conduct random periodic self-assessments and internal or external compliance verification, at least annually, in order (i) to determine that this privacy policy and its procedures are being followed and (ii) to identify and implement any needed strengthening of this policy document and the STLFC's procedural protections of privacy, civil rights, and civil liberties. These verification examinations will utilize the methodology set out in the June 2010 publication, "Privacy, Civil Rights, and Civil Liberties Verification for the Intelligence Enterprise" (Bureau of Justice Assistance, U.S. Department of Justice).

III. Oversight

III-1. The STLFC is an interdisciplinary collaborative initiative involving law enforcement, fire protection, emergency management, public health, and various private sector elements concerned with homeland security. Primary responsibility is assigned to the Director of the STLFC, and to such designees as the Director chooses, for (1) the operation of the STLFC, its justice systems, and coordination of personnel, (2) the receiving, seeking, retention, evaluation, quality, analysis, destruction, sharing, and disclosure of information, and (3) the enforcement of this policy.

III-2. The STLFC Director will designate senior personnel, appropriately trained, as the "Privacy Officer," whose duties include (i) training assurance, (ii) serving as the liaison for the Information Sharing Environment, and (iii) responsibility for receiving, handling, evaluating, and maintaining records of complaints from the general public regarding errors and violations of this policy; coordinating complaint resolution under the STLFC's redress policy (see VI-7 and X-1 through X-6, infra); and timely reporting findings or recommendations to the Director. The Privacy Officer can be contacted at the following email address: info@stlfc.gov.

III-3. The STLFC is guided by a designated Privacy Oversight Committee that liaises with the community to ensure that privacy, civil rights, and civil liberties are protected as provided in this policy and by the STLFC's information gathering and collection, retention, and dissemination processes and procedures. The Committee will annually review and, if needed, recommend updates to the policy in response to changes in law and implementation experience, including the results of audits and inspections. As resources permit, the Committee will (i) coordinate its work with the Privacy Officer and with the oversight committee (the Saint Louis Area Police Chiefs Association (SLAPCA) Technology Committee) for the LPRD- and SMRT-Projects, with the Privacy Oversight Committee remaining independent of the SLAPCA Technology Committee; and (ii) solicit and receive comments from the public on the development of or proposed updates to the policy.

III-4. The STLFC's Privacy Officer ensures that enforcement procedures and sanctions outlined in XIII-6 are adequate and enforced.

III-5. Key definitions and terms for this policy are provided in Appendix B of this policy.

IV. Information

IV-1. The STLFC, in fulfilling its public safety role, may seek, accept, analyze, disseminate, or retain information only when

- The source of the information is reliable and verifiable or limitations on the quality of the information are identified, **and**
- The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate, **and**

the information:

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

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

IV-2. The STLFC will not seek or retain, and information-originating agencies will agree not to submit, information about individuals or organizations solely on the basis of (i) their religious, political, or noncriminal social views or activities; (ii) their participation in a particular noncriminal organization or lawful event; or (iii) their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, gender identities, or sexual orientations. Neither will the STLFC, when participating in a federal law enforcement task force or when documenting a SAR or an ISE-SAR, consider the attributes at (i), (ii), or (iii), above, as factors which, alone, create suspicion; however, those attributes may be documented in specific suspect descriptions for identification purposes.

IV-3. The STLFC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Typically, and to the extent permitted by the information received and any supplemental information, the assessment considers factors such as:

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

IV-4. The STLFC applies labels or notifications to STLFC-originated information (or ensures that the originating agency has applied labels or notifications) when, and to indicate to the accessing authorized user that:

- The information is "protected information," to include "personal data" on any individual (see Appendix B) and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to local, tribal, state, or federal laws (see Appendix C) restricting access, use, or disclosure.

IV-5. Also, at the time a decision is made by the STLFC to retain information, it will be labeled or otherwise designated (by record, data set, or system of records), to the extent feasible and necessary, pursuant to applicable limitations on access and sensitivity of disclosure to:

- Protect confidential sources and police undercover techniques and methods.
- Not interfere with or compromise pending criminal investigations.
- Protect an individual's right of privacy or his or her civil rights and civil liberties.
- Provide legally required protections based on the individual's status as a (i) child, (ii) sexual abuse victim, (iii) resident of a substance abuse treatment program, (iv) resident of a mental health treatment program, or (v) resident of a domestic abuse shelter.

IV-6. The labels or designations assigned to existing information, as described immediately above, will be reevaluated whenever:

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

IV-7. STLFC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. STLFC personnel will:

- Prior to allowing access to or dissemination of the information, endeavor to ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it, as practicable, to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated, if attempts to validate or determine the reliability of the information have been unsuccessful. The STLFC will use a standard reporting format and data collection codes for SAR information.
- Store the information using the same or similar storage method used for data which rises to the level of reasonable suspicion and which includes an audit or similar accountability review and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion

(for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).

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

- Retain information in accordance with the NSI SAR Data Repository CONOPS (dated January 2014, at p. 10, Section 9) and the eGuardian System Privacy Impact Assessment Update of January 8, 2014, which provide that (i) information originators have the ability to determine the record retention schedule for their SARs in the SAR Data Repository, and (ii) when the information originator does not elect its own record retention schedule, then the retention schedule will default to the FBI's eGuardian record retention schedule. That FBI eGuardian schedule, in turn, is based upon the SAR's disposition as determined by the FBI, and the retention period begins based on the date the SAR receives its disposition; should a SAR with this default schedule receive a disposition of "no nexus to terrorism," it will be removed from the SAR Data Repository after 180 days; whereas SARs determined to have an "inconclusive" or "positive nexus to terrorism" with this default schedule will reside in the SAR Data Repository for five years. Information originators may determine a schedule that is shorter or longer than these defaults.

To the extent the STLFC may be regarded as an information originator for a SAR, the information will be retained for only a period, which shall not exceed 180 days (unless the period is expressly extended in writing by the STLFC Director for good cause, with the "cause" described in the extension authorization) required to work or investigate an unvalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label. (If an information originator which is not the STLFC elects its own record retention policy, it will be able to (i) locally administer that policy in eGuardian using the administrative functions made available to approved eGuardian users, and (ii) delete the SAR at any point in time; i.e., the information originator need not wait until the expiration of the record retention period to delete the SAR).

- Adhere to and follow the STLFC's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information.

IV-8. The STLFC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as individual and group information privacy, civil rights, and civil liberties.

IV-9. The STLFC identifies and reviews protected information that may be accessed from or disseminated by the STLFC prior to sharing that information through the Information

Sharing Environment (ISE). Further, the STLFC provides notice mechanisms, including but not limited to metadata or data field labels, to enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

IV-10. The STLFC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:

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

IV-11. The STLFC will attach (or endeavor to ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

IV-12. The STLFC will keep a record of the source of all information sought and collected, during the full period that the information is retained, by the STLFC.

IV-13. In fulfilling its public safety role, the STLFC may actively seek, analyze, disseminate, and/or retain information that is based on terrorism-related criminal predicates, a potential nexus to terrorism, or that which negatively impacts on public safety. Such information must be believed to be relevant to the investigation, prosecution, prevention, and/or mitigation of genuine public safety incidents. The STLFC may engage in research in order to provide law enforcement, public safety, and other appropriate agencies with actionable intelligence and/or useful, reliable, verifiable information pertaining to public safety and related policies. STLFC-researched or received information must be verifiable or labeled as unverified, as applicable, collected in a lawful manner, and lawfully disseminated. Only STLFC employees, vetted and approved contractors, and other pre-authorized personnel will be able to access the information. Limitations on or reservations about the quality of information will be noted if a source is of unknown or doubtful credibility and as provided in this section, above, and in Section VI, Quality Assurance. STLFC may retain preliminary information such as tips and leads, and suspicious activity reports, provided the information is arguably relevant to public safety intereSaint STLFC will not seek, analyze, disseminate, or retain information about individuals or organizations based solely on religious, political, or noncriminal social views and/or activities or participation in a particular noncriminal organization or lawful event, nor based solely on race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity, or sexual orientation. (See IV-2, above.) Information containing personal data will be disseminated to individuals based on the need-to-know and right-to-know concepts. Threat information will be disseminated to organizations and

individuals appropriately to protect public and asset safety. See Section IX, Sharing and Disclosure, *infra*.

IV-14. STLFC personnel will ensure that certain basic descriptive information is entered and associated with personally-identifiable information for which there are specific laws, rules, or policies regarding access, use, and disclosure. The descriptive 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; when available, the date its accuracy was last verified; and 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. As stated above, STLFC personnel will ensure that labels or markings and metadata have been applied, as appropriate, to the information that will be used, accessed, and disseminated to clearly indicate any legal restrictions on information-sharing based on information sensitivity or classification. A record will be kept of the source of all information sought and collected by the STLFC. Such information will be entered into the report system maintained by the senior intelligence analyst/privacy officer. The system logs the date of entry, title of report, and the employee identification number of the investigator or analyst writing or accessing the report.

IV-15. During receipt, storage, or dissemination of information, STLFC personnel will assess the information source, credibility, and content to determine if the information will be retained, for how long, and if it should be further disseminated. Tips and Leads information will be clearly labeled as such and be retained long enough to complete reasonable attempts 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 giving rise to reasonable suspicion. All information will be labeled as *Controlled Unclassified Information (CUI)* (See APPENDIX B, Definitions, for further information, as well as the November 4, 2010, Executive Order 13556 titled "Controlled Unclassified Information," and the National Archives and Record Administration final rule on CUI, at 81 Fed. Reg. 63324 (Sept. 14, 2016)), *Law Enforcement Sensitive (LES)*, or *For Official Use Only (FOUO)*, as deemed appropriate in the circumstances.

IV-16. Information received, analyzed, and disseminated at the STLFC will include at a minimum and as applicable, indicators for type of criminal/terrorism 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 and/or relabeled whenever new information is added that would increase/decrease the sensitivity of disclosure.

V. Acquiring and Receiving Information

V-1. Information gathering, including acquisition and access, and investigative techniques used by the STLFC and information-originating agencies are to comply with and adhere to applicable regulations and guidelines, including, but not limited to:

- 28 CFR Part 23, regarding criminal intelligence information;

- Fair Information Practice Principles (FIPPs), to the extent not superseded or modified by authorities paralleling those provided in the federal Privacy Act, state, tribal, or local law, or published fusion center policy;
- Applicable criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP)(ver. 2);
- Applicable federal and state constitutional provisions, Revised Missouri State Statutes Chapter 610 (Missouri Sunshine Laws) or the Illinois State Records Act, 5 ILCS 160, and either state's applicable administrative rules, as well as any other federal or applicable state regulations that apply to multijurisdictional intelligence and information databases.

V-2. In providing information, STLFC 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. STLFC analysts will not knowingly seek, receive, accept, disseminate, or retain information, directly or indirectly, from an entity that is legally prohibited from obtaining or disclosing that information, or which has illegally gathered the information. A STLFC human review of the information, including SAR information, ensures (i) the information was gathered legally; (ii) that information disseminated or shared through the ISE does not violate civil rights or civil liberties; and (iii) also, where applicable, that the information is determined to have a potential terrorism nexus. Law enforcement officers and appropriate STLFC and participating agency staff will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

V-3. The STLFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could, if misused, violate civil rights (race, religion, nation origin, ethnicity, etc., considered alone) will not be intentionally or inadvertently gathered, documented, processed, and shared.

V-4. Information gathering and investigative techniques used by the STLFC will (and from the originating agencies should) be the least intrusive means necessary in the particular circumstances to most effectively gather reliable information it is authorized to seek or retain. The STLFC will contract only with commercial database entities that provide written assurance (i) that their methods for gathering personally-identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and (ii) that these methods are not based on misleading information collection practices.

V-5. External agencies that access the STLFC's information or share information with the STLFC are governed by the laws and rules applicable to those individual agencies, including applicable federal and state laws.

V-6. The STLFC will not directly or indirectly receive, seek, accept, or retain information from:

- An individual who, or a nongovernmental entity that, may receive a fee or benefit for providing the information, except as expressly provided by law or STLFC policy.

- An individual who, or an information provider that, is legally prohibited from obtaining or disclosing the information.

V-7. Additional information regarding STLFC processes and day-to-day operations can be found in the numerous participating agencies' duty and software manuals. These manuals may not be available to the general public because of sensitivity issues involving the release of security information. Each participating agency retains authority over such materials' availability to the public, and STLFC participation in no way diminishes that authority.

V-8. To ensure privacy, civil rights, and civil liberties protections, the STLFC requires that its analytical products be reviewed and approved by the Privacy Officer, the Privacy Oversight Committee, the Director (or the Acting Director, in the Director's absence), or the Director-designated personnel who have completed training on 28 CFR Part 23, prior to the product(s) dissemination or sharing by the STLFC.

VI. Quality Assurance

VI-1. The STLFC 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 has been met (ensuring the identity or noting the perceived level of (un)certainty regarding identity, threat, risk, or incident).

VI-2. Where a SAR includes PII and is based on behavior not inherently criminal, the STLFC will engage in additional fact development during the vetting process and will articulate additional facts or circumstances to support any determination that the desired behavior is reasonably indicative of preoperational planning associated with terrorism or crime.

VI-3. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [*i.e.*, verifiability and reliability]).

VI-4. The labeling of retained information will be reevaluated by the STLFC when new information is gathered by the STLFC or by an originating agency conveying it to the STLFC and that new information has an impact on the validity and reliability of retained information.

VI-5. The STLFC will make every reasonable effort, including periodic data quality reviews, to ensure that information will be corrected in, or deleted from, the system when the center learns that (i) the information is erroneous, misleading, obsolete, or otherwise unreliable; (ii) the source of the information did not have authority to gather the information or to provide the information to the center; or (iii) the source used prohibited means to gather the information (except when the source did not act, in gathering the information, as an agent for a *bona fide* law enforcement officer or for the STLFC).

VI-6. Participating agencies are responsible for the quality and accuracy of the data provided to or accessed by the STLFC. Participating agencies providing data remain the owners of the data

contributed. The STLFC will promptly advise the appropriate data owner, in writing or electronically, if its data is found to be inaccurate, incomplete, out of date, or unverifiable.

VI-7. The STLFC will investigate, in a timely manner, alleged errors and deficiencies and must correct, delete, or refrain from using protected information found to be erroneous or deficient. The STLFC will, in writing or electronically, refer the error or deficiency to the originating agency.

VI-8. The STLFC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the STLFC because information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the referenced individual or organization may be affected.

VII. Merging Records

VII-1. Records about an individual or organization from two or more sources will not be merged by the STLFC 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 a higher accuracy of match.

VII-2. If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the STLFC, if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

VIII. Security Clearance and Analysis

VIII-1. All STLFC personnel must successfully pass a criminal history, security, and character background check, may possess an appropriate security clearance, and must have been selected, approved, and trained according to STLFC requirements. As such, they are authorized to seek, accept, retain, and disseminate appropriate information. Information subject to collation and analysis is information as defined in this document's Section IV, Information. This information undergoes STLFC analysis in order to enhance public safety, assist in investigations and prosecutions, and provide tactical and strategic intelligence services to authorized recipients.

VIII-2. Information acquired or received by the STLFC or accessed from other sources is analyzed according to priorities and needs and solely to:

- Further crime- (including terrorism-) prevention, disruption, deterrence, response, and mitigation; and law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the STLFC.
- Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities, including but not limited to planning, aiding, abetting, facilitating, funding, procuring, providing material support for, or conspiring or attempting to engage in such conduct.

IX. Sharing and Disclosure

IX-1. 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.

IX-2. The STLFC adheres to current national standards for the Suspicious Activity Reporting (SAR) process, including the use of (i) a standard reporting format and commonly accepted data collection codes and (ii) a reporting and sharing process that complies with the ISE-SAR Functional Standards for suspicious activity potentially associated with terrorism.

IX-3. Access to or disclosure of records retained by the STLFC will be provided only to persons within the STLFC or in other governmental agencies (i) who are authorized to have access and (ii) only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and (iii) only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An electronic audit trail will be kept by the STLFC of access by or dissemination of information to such persons. The audit trail shall be sufficient to allow for the identification of each individual who accessed information retained by the STLFC and the nature of the information accessed.

IX-4. Agencies external to the STLFC may not disseminate information accessed or disseminated from the STLFC without approval from the STLFC or other originator of the information.

IX-5. Information that is considered open-source or public record may be released outside the public safety community if such disclosure will further the STLFC mission and the recipient has a valid "need to know." In addition, STLFC 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, unless otherwise required by law.

IX-6. Information gathered or collected and retained by the STLFC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the STLFC, the nature of the information requested, accessed, or received, and the specific purpose will be kept by the STLFC for a minimum of five (5) years.

IX-7. Information gathered or collected and records retained by the STLFC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the STLFC's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with law and procedures applicable to the STLFC for this type of information. An audit trail sufficient to allow the

identification of each individual member of the public who accessed or received information retained by the STLFC and the nature of the information accessed will be kept by the STLFC, as above.

IX-8. STLFC 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 (i) that information is obtained from open sources available to anyone in the public or (ii) prior approval has been granted by the owner of the information or the STLFC Director. Organizations external to the STLFC may not disseminate STLFC information received from STLFC without approval from the originator of the information, and the disseminated information will include a label or marking advising of that limitation.

IX-9. Certain other records will not be disclosed to the public, including but not limited to:

- Records required to be kept confidential by law and which are exempt from disclosure requirements under Missouri Sunshine laws, Section 610.021 RSMo., or the Illinois State Records Act, 5 ILCS 160.
- Investigatory records of law enforcement agencies exempt from disclosure requirements under Missouri Sunshine laws or the Illinois State Records Act. However, certain law enforcement records must be made available for inspection and copying under Missouri Sunshine laws and the Illinois State Records Act.
- 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 the Revised Missouri Statutes and under the Illinois State Records Act, 5 ILCS 160. This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Chapter 610 of the Revised Missouri Statutes, or the Illinois State Records Act, 5 ILCS 160, and/or an act of agricultural terrorism under Chapter 610 of the Revised Missouri Statutes and/or the Illinois State Records Act, 5 ILCS 160, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606, and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency, that cannot consistently with the above-cited U.S., Missouri, or Illinois statutes be shared without permission. *E.g.,* 28 CFR Part 23; Chapter 32 RSMo. (Mo. Revenue Laws); 5 ILCS Chapter 35 (Il. Revenue Laws)*;* 5 U.S.C. §552a.
- A record, the disclosure of which would constitute a violation of an authorized nondisclosure agreement made within the scope of the above-cited U.S., Missouri, or Illinois statutes. See, *e.g.,* SF-312, DHS Form 11000-6, 6 CFR Part 29, 28 CFR 17.18, 32 CFR 2003.20, 49 CFR Part 1520; *cf.* American Foreign Service Ass'n. v. Garfinkel, 490 U.S. 153, 109 S. Ct. 1693, 104 L.Ed2d 139 (1989)(*per curiam*); NSSD 84 (March 11, 1983).

- Legally privileged information. See, *e.g.,* Fed.R.Ev. 501; Ill. R. Ev. 501; and RSMo. §§191.317.1 (certain medical test results and information), 191.656.1 (HIV testing information), 191.737 & 743 (referrals regarding children exposed to substance abuse; high risk pregnancies), 191.928 (newborn hearing loss information), 198.174-177 (nursing home fraud investigation records), 324.001 (certain division of professional registration records), 326.322 (accountant's client records), 337.636 & .736 (certain psychologist, counselor, and social worker records), 338.100 (pharmacy records), 340.286 (veterinarian records), 354.515 (certain HMO records), 356.181 (professional corporations retain natural persons' privileges re: communications), 374.071 (certain insurance dept. records), 409.6-607(b) (exempted securities commission records), 546.260.1 (spousal privilege), and 590.118 & 180 (peace officer investigation records & application/licensure records); *cf.* Mo. R. Civ. P. 56.01(c) (information subject to protective order). See, *generally*, O'Brien, Stewart, and Imwinkelried, Missouri Evidentiary Foundations, 4th ed. (Juris Pub'g., Inc. 2018), ch. 7.
- A record, or part thereof, that constitutes trade secrets or information that (i) whether commercial, financial, or otherwise is subject to a lawful non-disclosure agreement, (ii) was not obtained from a person, and (iii) is privileged and confidential under applicable law.

IX-10. The STLFC shall not confirm the existence or non-existence of information to any person or agency that would not be eligible to receive such information, unless otherwise required by law.

X. Inquiry, Complaints, and Redress

X-1. Upon satisfactory verification of identity and valid physical residence address, an individual making a written request is entitled to know of the existence of, and to review, information about him/her that is owned and retained by STLFC, as long as such disclosure would not violate federal or state laws or compromise an ongoing authorized investigation or prosecution. The individual may obtain a copy of the information for personal use or for the purpose of challenging its accuracy. Requests to access this information will be processed by, and access provided by, the STLFC Privacy Officer, to whom requests for disclosure may be addressed at: info@stlfc.gov. The STLFC response to these requests will be made within a reasonable time and in a form readily intelligible to the requesting individual. If the information has been provided to a complainant, and if an individual requests correction of information originating with the STLFC that has been disclosed, the STLFC's Privacy Officer, or designee, will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. The originating agency, whether the STLFC or external to the STLFC, must make a determination as to whether to correct the information, remove the record, or ascertain a basis for denial of a complaint. The individual to whom information has been disclosed will be provided notification of the reason(s) for denial. The individual will also be informed of the appeals process when STLFC or the originating agency has declined to correct the challenged information. A copy of the appeals process is available from the STLFC Privacy Officer at the address above.

X-2. For a minimum of five (5) years, post-request, an audit trail will be kept of each request for access to information for specific purposes and of what information is disseminated to each person in response to the requeSaint This will be completed for all requests.

X-3. Record requests will not be honored if disclosure would compromise an ongoing investigation, compromise a source of information (5 U.S.C. §552(b) & (c)), constitute an improper release of criminal intelligence subject to 28 CFR Part 23, or the information relates to or consists of information described (above) which is not subject to disclosure, including under Missouri Sunshine laws (Ch. 610, R.S. Mo.) or the Illinois State Records Act (5 ILCS 160), the information does not reside within STLFC, or STLFC does not own, or did not originate the information (5 U.S.C. §552a), or if such disclosure would violate federal or state laws or would endanger the health or safety of an individual, organization, or community.

X-4. If the information does not originate with the STLFC, the requestor will be referred to the originating agency, if appropriate or required, or the STLFC will notify the source agency of the request and its determination that disclosure by the STLFC or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

X-5. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the STLFC or the originating agency. The individual will also be informed of the procedure for appeal when the STLFC or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

X-6. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

(a) Is exempt from disclosure, and

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

(1) Is held by the STLFC and

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

the STLFC will inform the individual of the procedure for submitting and resolving such complaints. Complaints will be received by the STLFC's Privacy Officer at the following address: info@stlfc.gov. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant, unless otherwise required by law. If the information did not originate with the STLFC, the Privacy Officer or designee will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the STLFC that is the subject of a complaint will be reviewed within 30 business days and confirmed or corrected/purged if determined to be inaccurate or incomplete (to include incorrectly merged information, or information determined to be out of date). If there is no resolution within 30 business days, the STLFC will not share the information until such time as the complaint has been resolved. A record will be kept by the STLFC of all complaints and the resulting action taken in response to the complaint.

X-7. To delineate protected information shared through the ISE from other data, the STLFC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

XI. Security

XI-1. The STLFC Director will designate an experienced STLFC investigator as the center's security officer, who will ensure the center operates in a secure manner free from physical and network intrusion. The designated security officer will attend training through a federally-approved program and will seek additional site and network security information and resources from agreements with the Federal Bureau of Investigation and the Department of Homeland Security. Access to STLFC databases is strictly limited to occur from inside the facility (or via similar secure facility with pre-approval, by the Director or Deputy Director, of access permissions) and it will only be allowed in a secure manner. STLFC will store information in such a way that it cannot be accessed, modified, destroyed, or purged by unauthorized personnel.

XI-2. The STLFC will secure tips, leads, SAR, and LPRD Project information in a separate repository system using security procedures and policies that are the same as, or similar to, those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

XI-3. Access to STLFC information will be granted only to STLFC-authorized personnel (i) whose positions and job duties require such access; (ii) who have successfully completed the above-described background check and, if applicable, holding appropriate security clearance; and (iii) who have been selected, approved, and trained accordingly. Access to LPRD Project and SMRT Project information will be pursuant to applicable STLFC-generated Standard Operating Procedures, Memoranda of Understanding, and End User Agreements.

XI-4. Queries made to the STLFC data applications will be logged into the data system identifying the user initiating the query. The STLFC will utilize watch logs to maintain audit trails of requested and disseminated information and will maintain these logs as securely as other stored information.

XI-5. If an individual's personal information retained by STLFC is, or is reasonably believed to have been, compromised (that is, breached, altered, or obtained by an unauthorized person and access to which threatens physical, reputation, or financial harm to the person), STLFC will notify the individual promptly and without unreasonable delay, consistent with (i) applicable laws, regulations, and procedures, and (ii) with the legitimate needs of law enforcement to investigate the compromise or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release. The information may not be provided if notification compromises an ongoing investigation. The Executive Committee of the STLFC will also be notified and a determination made as to whether additional investigative assistance is required. If the security breach was directed toward STLFC Databases and/or Information Systems, supervisory personnel from all concerned or potentially-impacted agencies will be notified.

XI-6. The STLFC Director will designate a qualified staff person as Cybersecurity Officer, responsible for developing and annually updating the STLFC's data breach response plan in accordance with any changes in law, guidance, standards, agency policy, procedures, staffing, and/or technology; for maintaining documentation about each data breach reported to the center and the center's response; and for keeping center administrators informed of the status of an ongoing response. The Director will determine when a breach response is concluded, based on input from the Cybersecurity Officer and the Privacy Officer.

XI-7. STLFC 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-identifying information must also be secured. Visitors through STLFC must provide adequate identification and a valid need to visit, and any maintenance personnel, as well as approved visitors, must be escorted by STLFC personnel at all times when in the STLFC facility.

XI-8. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly-available data.

XII. Retention, Purge, and Destruction

XII-1. All criminal intelligence information (as that term is defined in 28 CFR §23.3) will be reviewed for record retention (validation or purge) by the STLFC at least every five (5) years, as provided by 28 CFR Part 23. For other information or intelligence, the record retention will comport with state law or applicable local ordinance in accordance with a record retention schedule established by the STLFC. To the extent that all STLFC data sets are systematically and regularly reviewed, updated, and purged (when applicable) the STLFC will (i) identify its data sets, (ii) ensure that retention thereof aligns with and is needed for the STLFC's mission and purpose, and (iii) develop and implement a retention schedule for each data set that (a) provides for the periodic review and update, and (b) establishes purge criteria, operational procedures, and destruction/disposition records.

XII-2. When information has no further value or meets the criteria for removal according to the STLFC's retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

XII-3. Information, which contains identifiable personal or group information, that has been reasonably connected, through a thorough investigation, to criminal or terrorist activity will be retained by the STLFC and periodically reviewed for accuracy and relevancy. This task will be accomplished at least every five (5) years, unless the information is previously re-validated as being connected to criminal or terrorist activity.

XII-4. Information, which contains identifiable personal or group information, that has been determined, through a thorough investigation, to have no reasonable connection to criminal or

terrorist activity will not be retained by the STLFC, and no documentation of the information will be stored.

XII-5. However, information that is reasonably believed to be connected to criminal or terrorist activity, which does not contain any identifiable personal or organizational information, may be held indefinitely in the event similar activity is observed at a future time.

XII-6. All purged information, whether electronic or physical, will be deleted, destroyed, or returned to the originating agency by STLFC personnel.

XII-7. No approval will be required from the originating agency before information held by the STLFC is destroyed or returned in accordance with this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

XII-8. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the STLFC, depending on the relevance of the information and any agreement with the originating agency.

XII-9. A record of information to be reviewed for retention will be maintained by the STLFC, and for appropriate system(s), notice will be given to the submitter, if then-identifiable, at least 30 days prior to the required review and validation/purge date.

XII-10. A printed or electronic confirmation of the deletion of information will be provided to the originating agency when required by law or pursuant to any pre-established agreement with an agency requiring such confirmation.

XIII. Accountability and Enforcement

XIII-1. The STLFC will remain open and accountable to the public regarding information collection practices. Printed copies of the STLFC Privacy Policy are available to any interested party, public or private, upon request, and the policy can be viewed on the following web site: www.stlfc.gov. Inquiries and complaints regarding the privacy policy or STLFC practices arguably concerning privacy, civil rights, or civil liberties protections can be submitted to the Privacy Officer through the "contact us" feature found at www.stlfc.gov or by emailing info@stlfc.gov.

XIII-2. For a minimum of five (5) years, post-access, the STLFC will maintain an electronic audit trail documenting any access to, request for, or dissemination of retained information. This audit trail will identify the person accessing, requesting, or receiving the dissemination of retained records, the date and time of the access/request/dissemination, and state what information was accessed/requested/disseminated.

XIII-3. The STLFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems requirements, with the provisions of this policy, and with applicable law. This will include logging access to these systems and periodic auditing of these systems, performed so as to not establish a predictable pattern of the audits. These

audits will be mandated at least annually and a record of the audits will be maintained by the Privacy Officer of the STLFC. Audits may be completed by an independent third party or by a STLFC-designated representative of a STLFC participating agency, or by the state or federal government. Audit outcomes may be compiled into a report to be provided to participating agencies' command staff and the STLFC Executive Committee (as described in the July 2014 STLFC Nationwide SAR Initiative Site-Specific Plan).

XIII-4. STLFC personnel or other authorized users shall report errors and violations or suspected violations of STLFC policies relating to protected information to the STLFC's Privacy Officer, who shall report confirmed violations to the STLFC Director and Executive Committee. The STLFC Privacy Officer will review and update the provisions of this policy at least once a year and make appropriate and public changes to it in response to changes in the relevant laws, technology, and/or in the use, purpose, or design of the STLFC's informational systems. Changes in public expectations may be considered in any review of this policy.

XIII-5. The STLFC will annually conduct an audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by the STLFC's designated independent Information Technology auditor, as selected by the STLFC Executive Committee. This auditor has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the STLFC. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s).

XIII-6. If STLFC personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the STLFC will:

- Suspend or discontinue access to information by the STLFC personnel, the participating agency, or the authorized user.
- Suspend, demote, transfer, or terminate STLFC personnel, as permitted by applicable personnel policies.
- Apply administrative actions or sanctions as provided by STLFC rules and regulations or as provided in agency/STLFC personnel policies.
- If the authorized user is from an agency external to the agency/STLFC, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

XIII-7. STLFC reserves the right to limit by any lawful means, including by setting reasonable standards, qualifications, and numeric limitations, personnel having access to the systems, and to deny, withhold or suspend access to any agency or individual violating the STLFC Privacy Policy, directly or through another.

XIII-8. This policy document is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United

States, the State of Missouri, the State of Illinois, the STLFC, its/their departments, agencies, or entities, its/their officers, employees, or agents, or any other person.

XIV. Training

XIV-1. The STLFC will require all the following individuals:

(i) full, part-time, and temporary STLFC staff,

(ii) programmers of STLFC-owned systems and, if they access content in STLFC data storage locations, personnel providing information technology services to the STLFC,

(iii) staff of other public agencies or private contractors providing services to the STLFC, which are services which expose the staff person(s) to controlled unclassified information retained in the STLFC, and

(iv) authorized users who are not employed by the STLFC or a contractor but who are exposed to controlled unclassified information retained in the STLFC,

to participate in training regarding the implementation of and adherence to this policy. Additional training may be provided by various agencies as to applicable state and federal privacy laws and may also be required, at the discretion of the STLFC.

XIV-2. STLFC privacy policy training will include, but not be limited to, the following: (i) purposes of the Privacy Policy; (ii) the substance and intent of all provisions of the policy; (iii) originating and participating agency responsibilities and obligations under applicable law and policy; (iv) the application of the policy in day-to-day work; (v) the potential impact of user abuse of information systems; (vi) reporting mechanisms regarding violations of the policy; and (vii) repercussions from policy violations, including the potential for transfer, suspension, dismissal, criminal, and individual civil liability.

XIV-3. All STLFC employees will also be required to successfully complete training on 28 CFR Part 23, offered by the United States Department of Justice, Bureau of Justice Assistance. This training is typically available at https://www.ncirc.gov/28CFR/default.aspx but, if that site is for some reason unavailable, then equivalent training selected by the Privacy Officer and approved by the Director must be completed.

XIV-4. The STLFC will provide and require special training for personnel authorized to collect, use, share, and disclose protected information through the Information Sharing Environment (ISE). The training will address the STLFC and ISE requirements and policies for collection, use, sharing, and disclosure of protected information.

APPENDIX A

Policy Note & User Agreement

Saint Louis Fusion Center: Terrorism Early Warning Group

Privacy, Civil Liberties, and Civil Rights Policy

POLICY NOTE

This policy does not constitute a contract of any kind. The Saint Louis Fusion Center: Terrorism Early Warning Group 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 Saint Louis Fusion Center: Terrorism Early Warning Group.

Saint Louis Fusion Center
Terrorism Early Warning Group

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

I hereby acknowledge that I have received a current copy of the Saint Louis Fusion Center: Terrorism Early Warning Group *Privacy, Civil Liberties, and Civil Rights Policy* and have read it in its entirety. I understand, agree with, and will comply with all of its provisions and terms.

_____ _____

Employee/Contractor/Vendor Signature Date

_____

Printed Name

_____

Company/Organization Name

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 Internet/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 Information Sharing Environment (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.

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency— See Originating Agency, Owning Agency, Participating Agency, Source Agency, Submitting Agency. Depending on context, the term may refer to the STLFC and all agencies that access, contribute, and share information in the STLFC's justice information system.

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

Audit Trail—Audit trail is a generic term for recording (logging) a sequence of activities. An appropriate audit trail is sufficient to all for the identification of each individual who accessed information retained by STLFC and the nature of the information accessed. 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—A general term used alternatively to describe a characteristic or a process. (1) As a characteristic: a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. Measurable characteristic 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. (2) As a process: automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. See, Glossary, Facial Identification Scientific Working Group (FISWG), version 2.0, Oct. 25, 2019, https://fiswg.org/fiswg_glossary_v2.0_20191025.pdf.

Center--Refers to the Saint Louis Fusion Center and all participating federal, state, local, and private entities or agencies of the Saint Louis Fusion Center.

Civil Liberties—According to the U.S. Dept. of Justice's Global Justice Information Sharing Initiative, "civil liberties" refers to 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 to protect against infringement, while the term "civil liberties" involves restrictions on government.

Civil Rights—The term "civil rights" refers to those rights and privileges of equal protection that government entities must afford to all individuals in the United States regardless of race, ethnicity, religion, gender, national origin, sexual orientation, gender identity, or other characteristics unrelated to the worth of the individual. Protection of civil rights means that government entities will take action to ensure that individuals are not discriminated against on the basis of any federal or state protected characteristic.

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, and they may include state constitutional and statutory guarantees, as well. For example, a state may have constitutional or statutory language regarding parental status.

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.

Collect-- For purposes of this document, “gather” and “collect” mean the same thing.

Computer Security-- The protection of information technology 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 appropriately use information and data under their control once it has been disclosed to them and in accordance with applicable data security laws and policies. 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

As more recently described in a November 4, 2010, Executive Order titled “Controlled Unclassified Information,” CUI is “information that requires safeguarding or dissemination controls…excluding information that is classified under Executive Order 13526 of December 29, 2009, or the Atomic Energy Act, as amended.” The November 4th Executive Order gives examples such as government-held “information that involves privacy, security, proprietary business interests, and law enforcement investigations.”

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 Activity-- A behavior, action, or omission that is punishable by criminal law.

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 activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

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

Data Breach-- The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially access PII, or (2) an authorized user accesses PII for a purpose other than the authorized purpose. The center's response to a data breach may be addressed in state law or agency policy. These data breaches may include incidents such as:

- Theft or loss of digital media upon which information is stored unencrypted and/or posting such information on the Internet;
- Unauthorized employee access to certain information;
- Moving information to a computer otherwise accessible from the Internet without proper information security precautions;
- Intentional or unintentional transfer of information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted email;
- Transfer of information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

Data Quality-- Refers to various aspects of the information, including: accuracy and actual values of the data; information structure; database repository design; completeness; currency; reliability; and context/meaning. Modern multidimensional descriptive models of data quality include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Integrity/Quality. See Appendix D.

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, or cloud technologies.

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.

Evaluation-- An assessment of the reliability of the source and accuracy of raw data.

Fair Information Practices and Fair Information Practice Principles—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, and form the basis for the subsequently-named Fair Information Practice Principles (FIPPs). They 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. Because of operational security, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (see listing, below) may be of limited applicability in intelligence operations, as fusion centers do not generally engage with individuals. That said, the STLFC, like all other integrated justice systems, endeavors to apply the FIPs and FIPPs where practicable.

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

The eight FIPPs are:

1. Purpose Specification
2. Data Quality/Integrity (see definition)
3. Collection Limitation/Data Minimization
4. Use Limitation
5. Security Safeguards (see definition)
6. Accountability/Audit
7. Openness/Trans[arency
8. Individual Participation

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

Fusion Center-- A collaborative effort of two or more federal, state, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent,

investigate, apprehend, and respond to criminal or terrorist activity. (Source: §511 of the 911 Commission Act; definition in the ISE-SAR Functional Standard, Version 1.5.5)

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

Home Agency/Organization—Refers to the actual employer of the staff member. For instance, someone may be assigned to the fusion center on a full-time basis, but be fully employed by a law enforcement agency.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002, 6 U.S.C. §482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (A) relates to a threat of terrorist activity; (B) relates to the ability to prevent, interdict, or disrupt terrorist activity; (C) which would improve 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) would improve the response to a terrorist act.

Identification—A process whereby a real-world entity is recognized and its identity established. Identity is operationalized in the abstract world of information systems as a set of information about an entity that differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a collection of data, such as a given and family name, date of birth, and address. An organization's identification process comprises the acquisition of the relevant identifying information.

Individual Responsibility—Because 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 three general areas: general data (including investigative information), tips and leads data (including suspicious activity reports), and criminal intelligence information.

Information Originator---In the context of data transfer, an information originator is an identifiable person or entity that provides data (i.e., information; see above) to the STLFC for evaluation, storage, retention, or dissemination. An anonymous, non-identifiable originator of data to the STLFC, at times, may be referred to as an

information originator, but not in the formal sense of one whom the STLFC is obliged by policy to treat as an identifiable person or entity.

Information Quality— See Data Quality, above.

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

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—An ISE-SAR is a SAR that has been determined, pursuant to a two-step process established in the ISE-SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Invasion of Privacy—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.

Joint Terrorism Task Forces (JTTFs)--The Federal Bureau of Investigation's (FBI) JTTFs are interagency task forces designed to enhance communication, coordination, and cooperation in countering terrorist threats. JTTFs combine the resources, talents, skills, and knowledge of federal, state, territorial, tribal, and local law enforcement and homeland security agencies, as well as the INtelligence Community, into a single team that deters, investigates, and/or responds to terrorist threats. JTTFs operationally execute the FBI's "lead agency" responsibility for investigating terrorist acts or threats against the United States.

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.

Lawful Permanent Resident—This term, sometimes abbreviated as “LPR,” means a foreign national who, through federal law, has been granted the privilege of permanently living and working in the United States.

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

LPRD Project---The License Plate Reader Database (LPRD) Project, an initiative of the Saint Louis Fusion Center: Terrorism Early Warning Group, consisting of an information sharing system designed to replicate, maintain, and share law enforcement license plate reader system data from participating public safety agencies within the Saint Louis UASI region, pursuant to Standard Operating Procedures which protect individual and group privacy and civil liberties/civil rights.

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.

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

Nationwide SAR Initiative (NSI) SAR Data Repository (SDR)--The NSI SDR is a single data repository, built to respect and support originator control and local stewardship of dara, which incorporates federal, state, and local retention policies. Within the SDR, hosted data enclaves extend this approach to information management and safeguarding practices by ensuring a separation of data across participating agencies.

Need to Know— As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

Non-repudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that 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.

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information, that is collected by a fusion center.

Owning Agency/Organization--The organization that owns the target associated with the suspicious activity.

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

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

Personal 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 in that it can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific 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.).

For further information about the breadth of PII and how to perform an assessment of the specific risk that an individual can be identified using certain information under consideration, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource.

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.

Preoperational Planning--Activities associated with known or particular planned criminal or terrorist operation(s). See ISE-SAR Functional Standard, v. 1.5.5.

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/k/a Privacy, Civil Rights, and Civil Liberties (P/CRCL) 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, receipt, use, analysis, maintenance, dissemination, retention, purging, 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 information collection, receipt, use, analysis, maintenance, dissemination, retention, purging, and access 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 truSaint

Privacy Protection—This is a process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health, through finding appropriate balances between privacy and multiple sometmes-competing interests, such as justice information sharing.

Protected Information—Protected information is personal data or information about individuals that is subject to information privacy or other legal protections under the U.S. Constitution and laws of the United States, including applicable federal statutes and regulations such as civil rights laws and 28 CFR Part 23, and (as applicable) the State of Missouri constitution or that of Illinois, and applicable state, local, and tribal laws and ordinances as expressly provided in this policy document. Protection may also be extended to organizations by STLFC policy or state, local, or tribal law.

Public—Public includes:

- Any individual and any for-profit or nonprofit entity, organization, or association;
- Any governmental entity for which there is no existing specific law authorizing access to the 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 center or participating entity;
- People or entities, private or governmental, who assist the agency in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the center is specified in law.

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

Purge--A term commonly used to describe methods rendering data unrecoverable in a storage space or which destroy data in a manner that it cannot be reconstituted. There are many different strategies and techniques for data purging, which is often contrasted with data deletion (i.e., made inaccessible except to system administrators or other privileged users).

Reasonably indicative--This operational concept for documenting and sharing suspicious activity takes into account the circumstances in which an observation is made which creates, in the mind of the reasonable observer, an articulable concern that the behavior may indicate preoperational planning associated with terrorism or other criminal activity. It also takes into account the training and experience of a reasonable law enforcement officer, in cases in which the officer is the observer or documenter of the observed behavior reported to a law enforcement agency.

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

Redress—Internal procedures to address complaints from persons, and laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information, regarding protected information about them that is under the agency's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

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 Know—A requirement for access to specific information to perform or assist in a lawful and authorized government function. Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity. Right to know is determined by the mission and functions of a law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity or the roles and responsibilities of particular personnel in the course of their official duties.

Right to (Information) Privacy—The right to be left alone, in the absence of some reasonable public interest in collecting, accessing, retaining, and disseminating information about an individual's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the individual or entity violating that right.

Role-Based Access Authorization—A type of access 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.

Source Agency/Organization—Defined in the ISE-SAR Functional Standard, Version 1.5.5, source agency refers to the agency or entity that originates the SAR (examples include a local police department, a private security firm handling security

for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.

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 the most common meaning in the IT industry.
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 relating to terrorism or the security of our homeland--by both the originator of the information and any recipient of the information.

Submitting Agency/Organization—The organization that actuates the push of the ISE-SAR to the NSI community. The submitting organization and the source organization may be the same.

Suspicious Activity—Suspicious activity is defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[o]bserved behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Examples of suspicious activity include: surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SAR)——Defined in the ISE-SAR Functional Standard, Version 1.5.5 as "[o]fficial documentation of observed behavior reasonably indicative of preoperational planning associated with terrorism or other criminal activity." Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the

existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53.

Terrorism-Related Information—In accordance with IRTPA, as 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 may include intelligence information.

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that 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 may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

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

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

U.S. Person—Executive Order 12333 states that a “United States person” means a United States citizen, an alien known by the intelligence element 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.

Urban Area Security Initiative (“UASI”)---In this document, this phrase/acronym refers to the eight-county, bi-state metropolitan Saint Louis region receiving federal funding managed by the Saint Louis Area Regional Response System (“STARRS”) and presently comprised of cooperating governments including those of Saint Louis, Saint Charles, Franklin, and Jefferson Counties and the City of Saint Louis in Missouri and of Saint Clair, Madison, and Monroe Counties in Illinois. (The City of Saint Louis is here counted as a separate county, as it is legally and administratively an entity independent of Saint Louis County.)

User—An individual representing a participating agency who is authorized to access or receive and use a center’s information and intelligence databases and resources for lawful purposes.

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

APPENDIX C
Applicable Federal and State Laws and Regulations

The U.S. Constitution is the primary authority that applies to federal as well as state, local, tribal, and territorial (SLTT) agencies, including the STLFC. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution, but states can broaden constitutional rights guaranteed by their own constitutions. Civil liberties protections are primarily founded in the federal Bill of Rights, which includes basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. (The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the Information Sharing Environment is discussed in a key issues guidance paper titled "Civil Rights and Civil Liberties Protection," which is available on the ODNI's website at https://www.dni.gov/index.php/nctc-who-we-are/organization/305-about/organization/information-sharingenvironment/resources/1767-privacy-civil-rights-and-civil-liberties.) In addition, statutory civil rights protections in federal laws may directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act. Federal laws, Executive Orders, regulations, and policies directly affect agencies'/centers' P/CRCL policies. While SLTT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection and sharing context, compliance may be required indirectly by funding conditions (e.g., Title VI of the Civil Rights Act of 1964; 28 CFR Parts 20, 22, and 23); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLTT agency (e.g., a memorandum of agreement or memorandum of understanding). These laws, regulations, and policies may potentially affect the sharing of information, including sharing terrorism-related information in the Information Sharing Environment (ISE). This STLFC privacy, civil rights, and civil liberties policy is primarily designed to ensure center personnel and authorized users are aware of the legal and privacy framework within which they and the center must operate. If the applicability and requirements of various laws, regulations, or sharing agreements had not been spelled out or referenced in this P/CRCL policy, staff and user accountability could be greatly diminished; mistakes could be made; privacy, civil rights, and civil liberties violations could occur; and the public's (and other agencies') confidence in the ability of the STLFC to protect information and intelligence would be compromised. Because STLFC staff members are required to know these rules and receive related ongoing training, information sharing is enhanced. Note that federal laws may use different terminology to describe information that identifies an individual (e.g., personal data, personal information, information in identifiable form). Different laws may have different statutory definitions for the terminology used. Personnel reviewing this policy should refer to the applicable statutory definition, in order to ensure that the scope of the terminology used is properly understood and implemented.

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

Additional Federal Laws, Regulations, and Guidance

Following are synopses of federal laws, regulations, and guidance. These federal laws were reviewed in developing the STLFC privacy policy. The list is arranged in alphabetical order by popular name. See also, Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0, pp. 46, et seq., at https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_pcrcl_policy_development_template_v_3.0_march_2019.pdf

1. **Brady Handgun Violence Prevention Act**, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A—The Brady Act, passed in 1993, requires background checks for purchases of firearms from federally licensed sellers. Because the act prohibits transfer of a firearm to a person who is prohibited by law from possessing a firearm, the transmission of personal data is an integral part of the regulation.

2. **Computer Matching and Privacy Act of 1988**, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget (OMB), Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000—The Computer Matching and Privacy Act of 1988 (Matching Act) amended the Privacy Act of 1974 to require that data-matching activities or programs of federal agencies that are designed to establish or verify eligibility for federal benefit programs or for recouping payments for debts under covered programs protect personal information. This is accomplished through a computer matching agreement and publication of a notice in the Federal Register. The OMB guidance requires that interagency data sharing provide protection, including provisions for notice, consent (as appropriate), redisclosure limitations, accuracy, security controls, minimization, accountability, and use of Privacy Impact Assessments. Although not directly a requirement of state, local, tribal, and territorial (SLTT) agencies, the guidance is a useful source of information on the types of protections that should be considered for all interagency data sharing programs.

3. **Confidentiality of Alcohol and Drug Abuse Patient Records**, 42 CFR Part 2, Code of Federal Regulations, Title 42: Public Health, Part 2—42 CFR Part 2 establishes minimum standards to govern the sharing of substance abuse treatment records (patient history information) in programs that are federally assisted. Generally, the sharing of such information is limited to the minimum necessary for the allowed purpose and requires consent of the patient except in specific emergency situations, pursuant to a court order or as otherwise specified. State law should also be consulted to determine whether there are additional limitations or sharing requirements.

4. **Confidentiality of Identifiable Research and Statistical Information,** 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22—28 CFR Part 22 is designed to protect the privacy of individuals whose personal information is made available for use in a research or statistical program funded under the Omnibus Crime Control and Safe Streets Act of 1968, the Juvenile Justice and Delinquency Prevention

Act of 1974, or the Victim of Crimes Act. The regulation, which may apply to SLTT agencies that conduct research or statistical programs, limits the use of such information to research or statistical purposes; limits its revelation to a need-to-know basis; provides for final disposition, transfer, and notice to/consent of data subjects; and identifies sanctions for violations. It provides useful guidance for SLTT agencies that wish to make data containing personal information available for research or statistical purposes.

5. **Crime Identification Technology**, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601—This statute authorizes the Office of Justice Programs (OJP), U.S. Department of Justice (DOJ), to support technological advances by states directed at a variety of criminal justice purposes, such as identification of certain categories of offenders, conducting background checks, and determining eligibility for firearms possession. The act defines broad categories of purposes for which funds may be used by OJP and sets forth certain eligibility criteria and assurances and other protocols that must be followed.

6. **Criminal History Records Exchanged for Noncriminal Justice Purposes**, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611—This statute provides a general overview of the Interstate Identification Index System (IIIS), an information sharing system that contains state and federal criminal history records that are also used for non-criminal justice purposes, such as governmental licensing and employment background checks. Congress recommends the creation of interstate and federal-state agreements to ensure that uniform policies are in place for records exchanges for non-criminal justice purposes and to prevent unauthorized use and disclosure of personal information due to variances in authorized users' policies. This statute is applicable to multijurisdictional information sharing systems that allow non-criminal justice-related exchanges.

7. **Criminal Intelligence Systems Operating Policies**, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23 (see text, above)—This is a guideline for law enforcement agencies that operate federally funded multijurisdictional criminal intelligence systems. The operating principles of 28 CFR Part 23 provide guidance to law enforcement regarding how to operate criminal intelligence information systems effectively while safeguarding privacy, civil rights, and civil liberties during the collection, storage, and dissemination of criminal intelligence information. The regulation governs the intelligence information systems' process, which includes information submission or collection, secure storage, inquiry and search capability, controlled dissemination, and review and purge processes.

8. **Criminal Justice Information Systems**, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20—This applies to all state and local agencies

and individuals collecting, storing, or disseminating criminal history record information processed by manual or automated operations and funded by the Omnibus Crime Control and Safe Streets Act of 1968, codified at 42 U.S.C. § 3789D. The regulation requires those criminal justice information systems to submit a criminal history information plan and provides guidance on specific areas that should have a set of operational procedures. These areas include completeness and accuracy of criminal history records and limitations on dissemination, including general policies on use and dissemination, juvenile records, audits, security, and access and review.

9. **Disposal of Consumer Report Information and Records**, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682—16 CFR Part 682 applies to information systems that maintain or possess consumer information for business purposes. The regulation provides guidance on proper disposal procedures for consumer information records to help protect against unauthorized use or access.

10. **Driver's Privacy Protection Act of 1994**, 18 U.S.C. § 2721—Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records—Collected License Plate Reader (LPR) information contains no PII that may be used to connect a license plate detection to an individual. It is only with permissible purpose that law enforcement may make this connect (using other systems), and this access is governed by the Driver's Privacy Protection Act of 1994. www.gpo.gov/fdsys/granule/USCODE-2011-title18/USCODE-2011-title18-partI-chap123- sec2721/content-detail.html

11. **E-Government Act of 2002**, Pub. L. No. 107-347, 208, 116 Stat. 2899 (2002); OMB (03-22, OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002)—OMB implementing guidance for this act requires federal agencies to perform Privacy Impact Assessments (PIA) for new information technologies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make significant changes to existing information technology that manages information in identifiable form. A PIA is an evaluation of how information in identifiable form is collected, stored, protected, shared, and managed. The purpose of a PIA is to demonstrate that system owners and developers have incorporated privacy, civil rights, and civil liberties protections throughout the entire life cycle of a system. The act requires an agency to make PIAs publicly available, except when an agency in its discretion determines publication of the PIA would raise security concerns or reveal classified (i.e., national security) information or sensitive. Although this act does not apply to SLTT partners, this tool is useful for identifying and mitigating Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0 48 privacy risks and for notifying the public what PII the SLTT agency is collecting, why PII is being collected, and how the PII will be collected, used, accessed, shared, safeguarded, and stored.

12. **Electronic Communications Privacy Act of 1986**, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508—This set of statutes prohibits a person from intentionally intercepting, trying to intercept, or asking another person to intercept or try to intercept any wire, oral, or electronic communication or trying to use information obtained in this manner. From another perspective, the law describes what law enforcement may do to intercept communications and how an organization may draft its acceptable use policies and monitor communications. Although it is a federal statute, the act does apply to state and local agencies and officials.

13. **Fair Credit Reporting Act**, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681—The Fair Credit Reporting Act regulates the collection, dissemination, and use of consumer information, including consumer credit information by consumer reporting agencies. Consumer reporting agencies include specialty agencies, such as agencies that sell information about employment history, insurance claims, check-writing histories, medical records, and rental history records, as well as credit bureaus. The law primarily deals with the rights of people about whom information has been gathered by consumer reporting agencies and the obligations of the agencies. Government agencies may obtain information from these reporting agencies and should be aware of the nature and limitations of the information, in terms of collection, retention, and error correction.

14. **Federal Civil Rights Laws**, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983—This is a federal statute that allows an individual to sue public officials in federal court for violations of the individual's civil rights. Civil rights include such things as the Fourth Amendment's prohibitions against unreasonable search and seizure, violations of privacy rights, and violations of the right to freedom of religion, free speech, and free association. It serves as a deterrent to unlawful collection, use, or sharing of information rather than providing specific authority or a prohibition to the collection, use, or sharing of information.

15. **Federal Driver's Privacy Protection Act (DPPA)**, 18 USC §§ 2721–2725—Restricts access and prohibits the release of personal information from state motor vehicle records to ensure the privacy of persons whose records have been obtained by that department in connection with a motor vehicle record unless certain criteria are met.

16. **Federal Records Act,** 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301— This chapter contains the laws governing disposal of records made or received by a federal agency in the normal course of business. It discusses procedures

and notices, if required, and the role of the federal archiviSaint The law applies only to federal agencies, but there may be similar state or local laws applicable to state and local agencies.

17. **Freedom of Information Act (FOIA)**, 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552—The federal FOIA, enacted in 1966, provides access to federal agency records or information. It does not, however, allow access to state or local government records. Nearly all states have their own public access statutes that provide access to state- and local-agency records. The interaction of federal and state FOIA laws can create complex issues. Federal statutes, in essence, provide a baseline of legal protections for individuals. While state legislatures may pass laws to supplement these federal guidelines, state laws that interfere with or are contrary to a federal law are preempted. By virtue of the Supremacy Clause of the U.S. Constitution (Article VI, Clause 2), federal law may restrict access to records otherwise available pursuant to a state's FOIA by requiring that certain information be kept confidential. Thus, federal confidentiality requirements may supersede a state FOIA statute mandating public disclosure of a record, but only when there is a specific federal statute (other than the federal FOIA) that mandates the records be kept confidential. In short, records may be available under one FOIA statute but not pursuant to another. Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0 49

18. **Health Insurance Portability and Accountability Act (HIPAA) of 1996**, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191—HIPAA was enacted to improve the Medicare and Medicaid programs and the efficiency and effectiveness of the nation's health care system by encouraging the development of a national health information system through the establishment of standards and requirements for the electronic transmission of health information. To that end, Congress directed the U.S. Department of Health and Human Services (HHS) to issue safeguards to protect the security and confidentiality of health information. To implement HIPAA's privacy requirements, HHS promulgated regulations setting national privacy standards for health information: the Standards for Privacy of Individually Identifiable Health Information (the "Privacy Rule")—42 U.S.C. §1320d-2; 45 CFR Parts 160, 164 (2003).

19. **HIPAA, Standards for Privacy of Individually Identifiable Health Information**, 45 CFR Parts 160 and 164, Code of Federal Regulations, Title 45, Parts 160 and 164—This "Privacy Rule" sets forth national standards for the privacy and security of individually identifiable health information (45 CFR Part 164, Subpart E (2003)). This rule has been described as providing a "federal floor" of safeguards to protect the confidentiality of medical information. State laws that provide stronger privacy protection will continue to apply over and above the federal privacy protection. The general rule under these standards states that a covered entity may not use or disclose protected

health information except as permitted or required by the rules (45 CFR §§ 164.502(a) and 164.103 [defining protected health information and use]). The Privacy Rule applies to the following covered entities: (1) a health plan, (2) a health care clearinghouse, and (3) a health care provider who transmits any health information in electronic form in connection with certain transactions (42 U.S.C. §1320d-1(a) (2003); 45 CFR § 160.102 (2003). Since the Privacy Rule applies only to a covered entity, a governmental body begins its inquiry by first determining whether it is a covered entity under the Privacy Rule (45 CFR § 160.103 (2003) [defining health plan, health care clearinghouse, health care provider]). If it is a covered entity, it then looks to the Privacy Rule for a permitted or required disclosure.

20. **Indian Civil Rights Act of 1968**, 25 U.S.C. § 1301 et seq., United States Code, Title 25, Chapter 15, Subchapter I—This act contains definitions of relevant terms and extends certain constitutional rights to Indian tribes exercising powers of self-government.

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

22. **National Child Protection Act of 1993**, Public Law 103-209 (December 20, 1993), 107 Stat. 2490—In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent entry. A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse. Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0 50

23. **National Crime Prevention and Privacy Compact**, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616—The compact establishes an infrastructure by which states can exchange criminal records for non-criminal justice purposes according to the laws of the requesting state and provide reciprocity among the states to share records without charging each other for the information. The Compact Council, as a national independent authority, works in partnership with criminal history record custodians, end users, and policymakers to regulate and facilitate the sharing of complete, accurate, and timely criminal history record information to noncriminal justice users in order to enhance public safety, welfare, and the security of society while recognizing the importance of individual privacy rights.

24. **National Security Act**, Public Law 235, Section 606, in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010—The National Security Act of 1947 mandated a major reorganization of foreign policy and military establishments of the U.S. government. The act created many of the institutions that U.S. Presidents found useful when formulating and implementing foreign policy, including the National Security Council and the Central Intelligence Agency. The 1947 law also caused far-reaching changes in the military establishment. The War Department and Navy Department merged into a single U.S. Department of Defense under the Secretary of Defense, who also directed the newly created Department of the Air Force. However, each of the three branches maintained its own service secretaries. On October 7, 2011, President Barack Obama signed Executive Order 13549, entitled, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information.” This order directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks that shall be consistent with appropriate protections for privacy and civil liberties. Agencies bear the primary responsibility for meeting these twin goals. These structural reforms will ensure coordinated interagency development and reliable implementation of policies and minimum standards regarding information security, personnel security, and systems security; address both internal and external security threats and vulnerabilities; and provide policies and minimum standards for sharing classified information both within and outside the federal government. These policies and minimum standards will address all agencies that operate or access classified computer networks, all users of classified computer networks (including contractors and others who operate or access classified computer networks controlled by the federal government), and all classified information on those networks.

25. **NIST Special Publication 800-53 (Appendix J) Security and Privacy Controls for Federal Information Systems and Organizations**—Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To that end, SP 800-53 Rev. 4 features eight families of privacy controls that are based on the FIPPs. The proliferation of social media, Smart Grid, mobile, and cloud computing as well as the transition from structured to unstructured information and metadata

environments have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality. The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Like their federal partners, SLTT agencies may use the privacy controls when evaluating their systems, processes, and programs.

26. **Preparing for and Responding to a Breach of Personally Identifiable Information, OMB Memorandum M-17-12 (January 2017)**—This memorandum sets forth the policy for federal agencies to prepare for and respond to a breach of PII. It includes a framework for assessing and mitigating the risk of harm to individuals potentially affected by a breach, as well as guidance on whether and how to provide notification and services to those individuals. This memorandum is intended to promote consistency in the way agencies prepare for and respond to a breach by requiring common standards and processes. Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0 51

27. **Privacy Act of 1974**, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a—The Privacy Act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies. A system of records is a group of records under the control of an agency from which information is retrieved by the name of the individual or by some identifier assigned to the individual. The Privacy Act prohibits the disclosure of a record about an individual from a system of records absent the written consent of the individual, unless the disclosure is pursuant to one of twelve statutory exceptions. The act also provides individuals with a means by which to seek access to and amendment of their records and sets agency recordkeeping requirements. In addition, the Privacy Act requires that agencies give the public notice of their systems of records by publication in the Federal Register.

28. **Privacy of Consumer Financial Information**, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313—This code oversees the treatment of nonpublic personal information about consumers by financial institutions and requires the institution to provide notice to customers about its privacy policies, the conditions under which it can disclose this information, and its opt out policies. This code also prohibits the disclosure of a consumer's credit card, deposit, or transaction account information to nonaffiliated third parties to market to the customer. The requirements for initial notice for the "opt-out" do not apply when nonpublic personal information is disclosed in order to comply with federal, state, or local laws or to comply with an authorized investigation, subpoena, or summons.

29. **Protection of Sensitive Agency Information, Office of Management and Budget Memorandum M-06-16 (June 2006)**—This memorandum provides a security checklist from the National Institute of Standards and Technology (NIST) to protect remote information removed from or accessed from outside an agency's physical location specific to PII. The NIST checklist requires that agencies verify PII in need of protection, confirm the adequacy of organization policy surrounding PII protection, and implement any necessary protections for PII transported or stored off-site or accessed remotely. In addition to the NIST checklist, the memorandum recommends implementing information encryption on all mobile devices, allowing remote access only with two factor authentication, using timeout functions on devices, and logging all computer-readable information extracts from databases with sensitive information, while verifying that each extract has either been erased within 90 days or that its use is still required.

30. **Safeguarding Customer Information**, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314—This Federal Trade Commission regulation implements Sections 501 and 505(b)(2) of the Gramm-Leach-Bliley Act. It sets forth standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information by financial institutions. While not directly applicable to government agencies, the regulation is useful in outlining the elements of a comprehensive information security program, including administrative, technical, and physical safeguards designed to (1) ensure the security and confidentiality of information, (2) protect against any anticipated threats or hazards to the security or integrity of information, and (3) protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to any individual.

31. **Sarbanes-Oxley Act of 2002**, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201—The Sarbanes-Oxley Act of 2002, Pub. L. 107-204 (July 30, 2002), commonly called Sarbanes-Oxley, is a federal law that sets new or enhanced standards for all U.S. public company boards, management, and public accounting firms. Its 11 titles include standards for public audits, internal controls, and financial disclosure. While not applicable to federal, state, local, tribal, or territorial governmental agencies, the business standards established by Sarbanes-Oxley are of value to such agencies in establishing their own policies and procedures to guide and control their business processes. Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0 52

32. **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act)**, Public Law 107-56 (October 26, 2001), 115 Stat. 272—The USA PATRIOT Act was enacted in response to the terrorist attacks of September 11, 2001. The act was designed to reduce the restrictions on law enforcement agencies' ability to gather intelligence and

investigate terrorism within the United States; expand the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and broaden the discretion of law enforcement and immigration authorities in detaining and deporting illegal immigrants suspected of terrorism-related acts. The act also expanded the definition of "terrorism" to include domestic terrorism. In 2011, the act was extended for four years, including provisions for roving wiretaps, searches of business records, and the conduct of surveillance of "lone wolves"—individuals suspected of terrorism-related activities that are not linked to terrorist groups.

33. **U.S. Constitution, First, Fourth, Fifth, Sixth, and Fourteenth Amendments**—The Bill of Rights establishes minimum standards for the protection of the civil rights and civil liberties of individuals in the United States. The First Amendment protects religious freedom, speech, the press, the right to peaceably assemble, and the right to petition the government for a redress of grievances. The Fourth Amendment protects the people from unreasonable searches and seizures and requires that warrants be issued only upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the individual or things to be seized. The Sixth Amendment establishes the right of an accused individual to a speedy and public trial by an impartial jury, to be informed of the nature and cause of the charges, to confront witnesses, to have compulsory process to obtain witnesses, and to have the assistance of legal counsel. The Fourteenth Amendment addresses citizenship rights and equal protection of the laws. Although the equal protection clause applies explicitly only to state governments, equal protection requirements apply to the federal government through the Fifth Amendment Due Process Clause.

34. **The USA FREEDOM Act of 2015** extended some provisions of the USA PATRIOT Act addressing the tracking of "lone wolves" and "roving wiretaps" of targets that communicate through multiple devices and replacing provisions related to "bulk collection" under Section 215 of the Patriot Act, with a requirement for a specific selection term used to limit the scope of tangible things sought consistent with the purpose for seeking those things in addition to showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

35. **Applicants and Recipients of Immigration Relief Under the Violence Against Women Act of 1994 (VAWA)**, Public Law 103-322, September 13, 1994, and the Victims of Trafficking and Violence Prevention Act of 2000 (T and U nonimmigrant status for victims of trafficking and other serious crimes), Public Law 106-386, Oct. 28, 2000, 8 U.S.C. § 1367, Penalties for Disclosure of Information—The governing statute prohibits the unauthorized disclosure of information about VAWA,15 T, and U cases to anyone other than an officer or employee of the U.S. Department of Homeland Security, the U.S. Department of Justice, the U.S. Department of State, or parties covered by exception when there is a need to know. This confidentiality provision is commonly

referred to as “Section 384” because it originally became law under Section 384 of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996, [5] which protects the confidentiality of victims of domestic violence, trafficking, and other crimes who have filed for or have been granted immigration relief. 8 U.S.C. § 1367 Information is defined as any information relating to aliens who are seeking or have been approved for nonimmigrant or immigrant status as (1) battered spouses, children, or parents under provisions of VAWA; (2) victims of a severe form of human trafficking who generally are cooperating with law enforcement authorities (T nonimmigrant status); or (3) aliens who have suffered substantial physical or mental abuse as the result of qualifying criminal activity and have been, are being, or are likely to be helpful in the 15 The confidentiality requirements established by VAWA are unaffected by a lapse in programmatic funding for VAWA. Fusion Center Privacy, Civil Rights, and Civil Liberties Policy Development, Version 3.0 53 investigation or prosecution of that activity (U nonimmigrant status). This includes information pertaining to qualifying family members who receive derivative T, U, or VAWA status. Because 8 U.S.C. § 1367 applies to any information about a protected individual, this includes records or other information that do not specifically identify the individual as an applicant for or a beneficiary of T nonimmigrant status, U nonimmigrant status, or relief under VAWA.

STATE OF ILLINOIS
GENERAL PROVISIONS

(5 ILCS 160/) State Records Act.

(5 ILCS 160/1) (from Ch. 116, par. 43.4)

Sec. 1. This Act may be cited as the State Records Act.
(Source: P.A. 86-1475.)

(5 ILCS 160/1.5)

Sec. 1.5. Purpose. Pursuant to the fundamental philosophy of the American constitutional form of government, it is declared to be the public policy of the State of Illinois (i) that government records are a form of property whose ownership lies with the citizens and with the State of Illinois; (ii) that those records are to be created, maintained, and administered in support of the rights of those citizens and the operation of the State; (iii) that those records are, with very few exemptions, to be available for the use, benefit, and information of the citizens; and (iv) that those records may not be disposed of without compliance to the regulations in this Act.
(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/2) (from Ch. 116, par. 43.5)

Sec. 2. For the purposes of this Act:

"Secretary" means Secretary of State.

"Record" or "records" means all books, papers, born-digital electronic material, digitized electronic material, electronic material with a combination of digitized and born-digital material, maps, photographs, databases, or other official documentary materials, regardless of physical form or characteristics, made, produced, executed, or received by any agency in the State in pursuance of State law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its successor as evidence of the organization, function, policies, decisions, procedures, operations, or other activities of the State or of the State Government, or because of the informational data contained therein. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of blank forms are not included within the definition of records as used in this Act. Reports of impaired physicians under Section 16.04 of the Medical Practice Act or Section 23 of the Medical Practice Act of 1987 are not included within the definition of records as used in this Act.

"Born-digital electronic material" means electronic material created in digital form rather than converted from print or analog form to digital form.

"Digitized electronic material" means electronic material converted from print or analog form to digital form.

"Agency" means all parts, boards, and commissions of the executive branch of the State government, including, but not limited to, State colleges and universities and their governing boards and all departments established by the Civil Administrative Code of Illinois.

"Public Officer" or "public officers" means all officers of the executive branch of the State government, all officers created by the Civil Administrative Code of Illinois, and all other officers and heads, presidents, or chairmen of boards, commissions, and agencies of the State government.

"Commission" means the State Records Commission.

"Archivist" means the Secretary of State.

(Source: P.A. 99-147, eff. 1-1-16; 100-201, eff. 8-18-17.)

(5 ILCS 160/3) (from Ch. 116, par. 43.6)

Sec. 3. Records as property of State.

(a) All records created or received by or under the authority of or coming into the custody, control, or possession of public officials of this State in the course of their public duties are the property of the State. These records may not be mutilated, destroyed, transferred, removed, or otherwise damaged or disposed of, in whole or in part, except as provided by law. Any person shall have the right of access to any public records, unless access to the records is otherwise limited or prohibited by law. This subsection (a) does not apply to records that are subject to expungement under subsections (1.5) and (1.6) of Section 5-915 of the Juvenile Court Act of 1987.

(b) Reports and records of the obligation, receipt and use of public funds of the State are public records available for inspection by the public, except as access to such records is otherwise limited or prohibited by law or pursuant to law. These records shall be kept at the official place of business of the State or at a designated place of business of the State. These records shall be available for public inspection during regular office hours except when in immediate use by persons exercising official duties which require the use of those records. Nothing in this section shall require the State to invade or assist in the invasion of any person's right to privacy. Nothing in this Section shall be construed to limit any right given by statute or rule of law with respect to the inspection of other types of records.

Warrants and vouchers in the keeping of the State Comptroller may be destroyed by him as authorized in "An Act in relation to the reproduction and destruction of records kept by the Comptroller", approved August 1, 1949, as now or hereafter amended after obtaining the approval of the State Records Commission.

(Source: P.A. 98-637, eff. 1-1-15.)

(5 ILCS 160/3.5)

Sec. 3.5. Confidentiality of foster placement records. All records concerning foster placement and foster parent identifying information shall be released only in accordance with Section 35.3 of the Children and Family Services Act.

(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/4) (from Ch. 116, par. 43.7)

Sec. 4. Any person shall have the right of access to any public records of the expenditure or receipt of public funds as defined in Section 3 for the purpose of obtaining copies of the same or of making photographs of the same while in the possession, custody and control of the lawful custodian thereof, or his authorized deputy.

(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/4a)

Sec. 4a. Arrest records and reports.

(a) When an individual is arrested, the following information must be made available to the news media for inspection and copying:

(1) Information that identifies the individual,

including the name, age, address, and photograph, when and if available.

(2) Information detailing any charges relating to the

arreSaint

(3) The time and location of the arreSaint

(4) The name of the investigating or arresting law

enforcement agency.

(5) If the individual is incarcerated, the amount of

any bail or bond.

(6) If the individual is incarcerated, the time and

date that the individual was received, discharged, or transferred from the arresting agency's custody.

(b) The information required by this Section must be made available to the news media for inspection and copying as soon as practicable, but in no event shall the time period exceed 72 hours from the arreSaint The information described in paragraphs (3), (4), (5), and (6) of subsection (a), however, may be withheld if it is determined that disclosure would:

(1) interfere with pending or actually and reasonably

contemplated law enforcement proceedings conducted by any law enforcement or correctional agency;

(2) endanger the life or physical safety of law

enforcement or correctional personnel or any other person; or

(3) compromise the security of any correctional

facility.

(c) For the purposes of this Section, the term "news media" means personnel of a newspaper or other periodical issued at regular intervals whether in print or electronic format, a news service whether in print or electronic format, a radio station, a television station, a television network, a community antenna television service, or a person or corporation engaged in making news reels or other motion picture news for public showing.

(d) Each law enforcement or correctional agency may charge fees for arrest records, but in no instance may the fee exceed the actual cost of copying and reproduction. The fees may not include the cost of the labor used to reproduce the arrest record.

(e) The provisions of this Section do not supersede the confidentiality provisions for arrest records of the Juvenile Court Act of 1987.

(f) All information, including photographs, made available under this Section is subject to the provisions of Section 2QQQ of the Consumer Fraud and Deceptive Business Practices Act.

(Source: P.A. 98-555, eff. 1-1-14; 99-363, eff. 1-1-16.)

(5 ILCS 160/5) (from Ch. 116, par. 43.8)

Sec. 5. The Secretary of State shall provide for a State Archives Division as a repository of State records. The State Archives may utilize space in the Archives Building or other buildings as may be necessary or appropriate for the purpose, in the opinion of the Secretary of State.

(Source: Laws 1957, p. 1687.)

(5 ILCS 160/6) (from Ch. 116, par. 43.9)

Sec. 6. The Secretary of State shall be the State Archivist and Records Administrator and he shall appoint such assistants, who shall be technically qualified and experienced in the control and management of archival materials and in records management practices and techniques, as are necessary to carry out his duties as State ArchiviSaint

(Source: Laws 1957, p. 1687.)

(5 ILCS 160/7) (from Ch. 116, par. 43.10)

Sec. 7. Powers and duties of the Secretary.

(1) The Secretary, whenever it appears to him to be in the public interest, may accept for deposit in the State Archives the records of any agency or of the Legislative or Judicial branches of the State government that are determined by him to have sufficient historical or other value to warrant the permanent preservation of such records by the State of Illinois.

(2) The Secretary may accept for deposit in the State Archives official papers, photographs, microfilm, electronic and digital records, drawings, maps, writings, and records of every description of counties, municipal corporations, political subdivisions and courts of this State, and records of the federal government pertaining to Illinois, when such materials are deemed by the Secretary to have sufficient historical or other value to warrant their continued preservation by the State of Illinois.

(3) The Secretary, whenever he deems it in the public interest, may accept for deposit in the State Archives motion picture films, still pictures, and sound recordings that are appropriate for preservation by the State government as evidence of its organization, functions and policies.

(4) The Secretary shall be responsible for the custody, use, servicing and withdrawal of records transferred for deposit in the State Archives. The Secretary shall observe any rights, limitations, or restrictions imposed by law relating to the use of records, including the provisions of the Mental Health and Developmental Disabilities Confidentiality Act which limit access to certain records or which permit access to certain records only after the removal of all personally identifiable data. Access to restricted records shall be at the direction of the depositing State agency or, in the case of records deposited by the legislative or judicial branches of State government at the direction of the branch which deposited them, but no limitation on access to such records shall extend more than 75 years after the creation of the records, except as provided in the Mental Health and Developmental Disabilities Confidentiality Act. The Secretary shall not impose restrictions on the use of records that are defined by law as public records or as records open to public inspection.

(5) The Secretary shall make provision for the preservation, arrangement, repair, and rehabilitation, duplication and reproduction, description, and exhibition of records deposited in the State Archives as may be needed or appropriate.

(6) The Secretary shall make or reproduce and furnish upon demand authenticated or unauthenticated copies of any of the documents, photographic material or other records deposited in the State Archives, the public examination of which is not prohibited by statutory limitations or restrictions or protected by copyright. The Secretary shall charge a fee therefor in accordance with the schedule of fees in Section 5.5 of the Secretary of State Act, except that there shall be no charge for making or authentication of such copies or reproductions furnished to any department or agency of the State for official use. When any such copy or reproduction is authenticated by the Great Seal of the State of Illinois and is certified by the

Secretary, or in his name by his authorized representative, such copy or reproduction shall be admitted in evidence as if it were the original.

(7) Any official of the State of Illinois may turn over to the Secretary of State, with his consent, for permanent preservation in the State Archives, any official books, records, documents, original papers, or files, not in current use in his office, taking a receipt therefor.

(8) (Blank).

(9) The Secretary may cooperate with the Illinois State Genealogical Society, or its successor organization, for the mutual benefit of the Society and the Illinois State Archives, with the State Archives furnishing necessary space for the society to carry on its functions and keep its records, to receive publications of the Illinois State Genealogical Society, to use members of the Illinois State Genealogical Society as volunteers in various archival projects and to store the Illinois State Genealogical Society's film collections.

(Source: P.A. 95-331, eff. 8-21-07.)

(5 ILCS 160/8) (from Ch. 116, par. 43.11)

Sec. 8. The head of each agency shall cause to be made and preserved records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency designed to furnish information to protect the legal and financial rights of the State and of persons directly affected by the agency's activities.

This Section shall not be construed to prevent the legal disposal of any records determined by the agency and by the Commission not to have sufficient value to warrant their continued preservation by the State or by the agency concerned. (Source: Laws 1957, p. 1687.)

(5 ILCS 160/9) (from Ch. 116, par. 43.12)

Sec. 9. The head of each agency shall establish and maintain an active, continuing program for the economical and efficient management of the records of the agency.

Such program:

(1) shall provide for effective controls over the

creation, maintenance, and use of records in the conduct of current business and shall ensure that agency electronic records, as specified in Section 5-135 of the Electronic Commerce Security Act, are retained in a trustworthy manner so that the records, and the information contained in the records, are accessible and usable for reference for the duration of the retention period; all computer tape or disk maintenance and preservation procedures must be fully applied and, if equipment or programs providing access to the records are updated or replaced, the existing data must remain accessible in the successor format for the duration of the approved retention period;

(2) shall provide for cooperation with the Secretary

in appointing a records officer and in applying standards, procedures, and techniques to improve the management of records, promote the maintenance and security of records deemed appropriate for preservation, and facilitate the segregation and disposal of records of temporary value; and

(3) shall provide for compliance with the provisions of this Act and the rules and regulations issued thereunder.

If an agency has delegated its authority to retain records to another agency, then the delegate agency shall maintain the same, or a more diligent, record retention methodology and record retention period as the original agency's program. If the delegate is from the legislative or judicial branch, then the delegate may use the same record retention methodology and record retention period that the delegate uses for similar records.
(Source: P.A. 99-642, eff. 7-28-16.)

(5 ILCS 160/10) (from Ch. 116, par. 43.13)
Sec. 10. Whenever the head of an agency determines that substantial economies or increased operating efficiency can be effected thereby, he may, subject to the approval of the Secretary, provide for the storage, care, and servicing of records that are appropriate therefor in a records center operated and maintained by the Secretary.
(Source: Laws 1957, p. 1687.)

(5 ILCS 160/11) (from Ch. 116, par. 43.14)
Sec. 11. Violation. All records made or received by or under the authority of or coming into the custody, control or possession of public officials of this State in the course of their public duties are the property of the State and shall not be mutilated, destroyed, transferred, removed or otherwise damaged or disposed of, in whole or in part except as provided by law. Any person who knowingly and without lawful authority alters, destroys, defaces, removes, or conceals any public record commits a Class 4 felony.
(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/12) (from Ch. 116, par. 43.15)
Sec. 12. The Secretary shall make continuing surveys of State records management and disposal practices and obtain reports thereon from agencies and their staff.
(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/13) (from Ch. 116, par. 43.16)

Sec. 13. The Secretary, with due regard to the program activities of the agencies concerned, shall make provision for the economical and efficient management of records of State agencies by analyzing, developing, promoting, coordinating, and promulgating standards, procedures, and techniques designed to improve the management of records, to insure the maintenance and security of records deemed appropriate for preservation, and to facilitate the segregation and disposal of records of temporary value. The Secretary shall aid also in promoting the efficient and economical utilization of space, equipment, and supplies needed for the purpose of creating, maintaining, storing, and servicing records.

(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/14) (from Ch. 116, par. 43.17)

Sec. 14. The Secretary shall establish standards for the selective retention of records of continuing value and assist agencies in applying such standards to records in their custody.

(Source: Laws 1957, p. 1687.)

(5 ILCS 160/15) (from Ch. 116, par. 43.18)

Sec. 15. The Secretary shall establish, maintain, and operate records centers for the storage, care, and servicing of records of State agencies pending their deposit in the State Archives or the disposition of such records in any other manner authorized by law. The Secretary may establish, maintain, and operate centralized microfilming and digital reproduction services for agencies.

(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/15a) (from Ch. 116, par. 43.18a)

Sec. 15a. The head of each agency shall establish a system for the protection and preservation of essential State records necessary for the continuity of governmental functions in the event of an emergency arising from enemy action or natural disaster and for the reestablishment of State government thereafter.

(Source: P.A. 85-414.)

(5 ILCS 160/15b) (from Ch. 116, par. 43.18b)
Sec. 15b. The head of each agency shall:
(1) Determine what records are "essential" for

emergency government operation through consultation with all branches of government, State agencies, and with the State Civil Defense Agency.

(2) Determine what records are "essential" for

post-emergency government operations and provide for their protection and preservation.

(3) Establish the manner in which essential records

for emergency and post-emergency government operations shall be preserved to ensure emergency usability.

(4) Establish and maintain an essential records

preservation program.

The Secretary may provide for security storage or relocation of essential State records in the event of an emergency arising from enemy attack or natural disaster.
(Source: P.A. 99-78, eff. 7-20-15.)

(5 ILCS 160/16) (from Ch. 116, par. 43.19)

Sec. 16. There is created the State Records Commission. The Commission shall consist of the following State officials or their authorized representatives: the Secretary of State, who shall act as chairman; the State Historian, who shall serve as secretary; the State Treasurer; the Director of Central Management Services; the Attorney General; and the State Comptroller. The Commission shall meet whenever called by the chairman, who shall have no vote on matters considered by the Commission. It shall be the duty of the Commission to determine what records no longer have any administrative, fiscal, legal, research, or historical value and should be destroyed or disposed of otherwise. The Commission may make recommendations to the Secretary of State concerning policies, guidelines, and best practices for addressing electronic records management issues as authorized under Section 37 of the Government Electronic Records Act.

(Source: P.A. 97-249, eff. 8-4-11.)

(5 ILCS 160/17) (from Ch. 116, par. 43.20)

Sec. 17. (a) Regardless of other authorization to the contrary, except as otherwise provided in subsection (b) of this Section, no record shall be disposed of by any agency of the State, unless approval of the State Records Commission is first obtained. The Commission shall issue regulations, not inconsistent with this Act, which shall be binding on all agencies. Such regulations shall establish procedures for compiling and submitting to the Commission lists and schedules of records proposed for disposal; procedures for the physical destruction or other disposition of records proposed for disposal; and standards for the reproduction of records by digital, photographic, or microphotographic processes with the view to the disposal of the original records. Such standards shall relate to the electronic digital process and format, quality of film used, preparation of the records for reproduction, proper identification matter on the records so that an individual document or series of documents can be located on the film or electronic medium with reasonable facility, and that the copies contain all significant record detail, to the end that the photographic, microphotographic, or digital copies will be adequate.

Such regulations shall also provide that the State archivist may retain any records which the Commission has authorized to be destroyed, where they have a historical value, and that the State archivist may deposit them in the State Archives or State Historical Library or with a historical society, museum or library.

(b) Upon request from a chief of police, county sheriff, or State's Attorney, if a person has been arrested for a criminal offense and an investigation reveals that the person arrested was not in fact the individual the arresting officer believed him or her to be, the law enforcement agency whose officers made the arrest shall delete or retract the arrest records of that person whom the investigation revealed as not the individual the arresting officer believed him or her to be. In this subsection (b):

"Arrest records" are as described in Section 4a of this Act.

"Law enforcement agency" means an agency of this

State which is vested by law or ordinance with the duty to maintain public order and to enforce criminal laws or ordinances.

(Source: P.A. 99-363, eff. 1-1-16.)

(5 ILCS 160/18) (from Ch. 116, par. 43.21)

Sec. 18. The head of each agency shall submit to the Commission, in accordance with the regulations of the Commission, lists or schedules of records in his or her custody and his or her proposal for the length of time each record series warrants retention for administrative, legal or fiscal purposes after it has been created or received by the agency.

(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/19) (from Ch. 116, par. 43.22)

Sec. 19. All lists and schedules submitted to the Commission shall be referred to the Archivist who shall ascertain whether the records proposed for disposal have value to other agencies of the State or whether such records have research or historical value. The Archivist shall submit such lists and schedules with his recommendations in writing to the Commission; and the final disposition of such records shall be according to the orders of the Commission.

(Source: Laws 1957, p. 1687.)

(5 ILCS 160/20) (from Ch. 116, par. 43.23)

Sec. 20. Nonrecord materials or materials not included within the definition of records as contained in this Act may be destroyed at any time by the agency in possession of such materials without the prior approval of the Commission. The Commission may formulate advisory procedures and interpretation to guide in the disposition of nonrecord materials.

(Source: Laws 1957, p. 1687.)

(5 ILCS 160/21) (from Ch. 116, par. 43.24)

Sec. 21. The Archivist shall submit to the Commission, with his recommendations in writing, disposal lists of records that have been deposited in the State Archives as provided in subsections (1), (2), and (3) of Section 7 of this Act, after having determined that the records concerned do not have sufficient value to warrant their continued preservation by the State. However, any records deposited in the State Archives by any agency pursuant to the provisions of subsection (1) of Section 7 of this Act shall not be submitted to the Commission for disposal without the written consent of the head of such agency.

(Source: Laws 1957, p. 1687.)

(5 ILCS 160/22) (from Ch. 116, par. 43.25)

Sec. 22. Upon the termination of any State agency whose function or functions have not been transferred to another agency, the records of such terminated agency shall be deposited in the State Archives. The Commission shall determine which records are of sufficient legal, historical, administrative, or fiscal value to warrant their continued preservation by the State. Records that are determined to be of insufficient value to warrant their continued preservation shall be disposed of as provided in Section 17 of this Act.

(Source: Laws 1957, p. 1687.)

(5 ILCS 160/22a) (from Ch. 116, par. 43.25a)

Sec. 22a. There is hereby created the State Archives Advisory Board consisting of 12 voting members and 2 nonvoting members.

The voting members shall be appointed by the Secretary of State as follows: A member of the State Records Commission, a member of a Local Records Commission, a member of a local historical society or museum, a university archivist, a person in the field of education specializing in either history or political science, a genealogist, a research or reference librarian, a person who is employed or engaged as an archivist by a business establishment and 4 public members.

The nonvoting members shall be the Director of the State Library and the State Historian who shall serve ex-officio.

Four of the initial appointees shall serve a 1-year term; four shall serve 2-year terms; and the remaining 4 shall serve 3-year terms. The terms of the initial appointees shall be specified by the Secretary of State at the time of appointments. Subsequent to the initial appointments all members shall hold office for a period of 3 years. Vacancies shall be filled by appointment of the Secretary of State for the unexpired balance of the term. No person shall serve for more than 2 consecutive 3-year terms.

The State Archives Advisory Board shall elect from its own members one chairman and one vice chairman.

The members appointed to the Board shall serve without compensation but shall be reimbursed for necessary expenses incurred in the performance of their duties.

(Source: P.A. 83-523.)

(5 ILCS 160/22b) (from Ch. 116, par. 43.25b)

Sec. 22b. The State Archives Advisory Board shall meet at the call of the chairman, but not less than 3 times in each calendar year, and shall make recommendations to the State Archivist on such matters as: general policies regarding the operation of the State archives; budget policies relative to annual appropriations by the General Assembly; and policies for federal funded archives programs.

(Source: P.A. 83-523.)

(5 ILCS 160/22c) (from Ch. 116, par. 43.25c)

Sec. 22c. The State Archives Advisory Board shall also serve as the Illinois State Historical Records Advisory Board. This Board shall:

(1) serve as the State advisory body required by

federal agencies to approve historical record grant applications;

(2) promote the identification, preservation, access

to, and use of historical records in Illinois; and

(3) meet at least once each year.

The Director of the State Archives shall serve as the coordinator of this Board and assist the Board in its functions. The Secretary may appoint additional assistants, who must be technically qualified and experienced in records management and historic records preservation, as necessary to carry out the functions of this Board.

(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/23) (from Ch. 116, par. 43.26)

Sec. 23. "An Act creating the State Records Commission and defining its powers and duties," approved July 23, 1943, as amended, is repealed, but all orders heretofore issued by the State Records Commission created by said Act shall stand and continue to be in full force and effect.

(Source: Laws 1957, p. 1687.)

(5 ILCS 160/24) (from Ch. 116, par. 43.27)

Sec. 24. Auditor General. The Auditor General shall audit agencies for compliance with this Act when conducting compliance audits and shall report his or her findings to the agency and the Secretary.

Any officer or employee who violates the provisions of subsection (b) of Section 3 of this Act is guilty of a Class B misdemeanor.

(Source: P.A. 92-866, eff. 1-3-03.)

(5 ILCS 160/25) (from Ch. 116, par. 43.28)

Sec. 25. The invalidity of any section or part or portion of this act shall not affect the validity of the remaining sections or parts thereof.

(Source: Laws 1957, p. 1687.)

"Personal identifying information" means any of the following information:

(1) A person's name.

(2) A person's address.

(3) A person's date of birth.

(4) A person's telephone number.

(5) A person's driver's license number or State of Illinois identification card as assigned by the Secretary of State of the State of Illinois or a similar agency of another state.

(6) A person's social security number.

(7) A person's public, private, or government employer, place of employment, or employment identification number.

(8) The maiden name of a person's mother.
(9) The number assigned to a person's depository account, savings account, or brokerage account.
(10) The number assigned to a person's credit or debit card, commonly known as a "Visa Card", "MasterCard", "American Express Card", "Discover Card", or other similar cards whether issued by a financial institution, corporation, or business entity.

(11) Personal identification numbers.
(12) Electronic identification numbers.
(13) Digital signals.
(14) User names, passwords, and any other word, number, character or combination of the same usable in whole or part to access information relating to a specific individual, or to the actions taken, communications made or received, or other activities or transactions of a specific individual.

(15) Any other numbers or information which can be used to access a person's financial resources, or to identify a specific individual, or the actions taken, communications made or received, or other activities or transactions of a specific individual.

(Source: P.A. 97-597, eff. 1-1-12; incorporates 97-388, eff. 1-1-12; 97-1109, eff. 1-1-13.)

Missouri Revised Statutes

Chapter 610
Governmental Bodies and Records
Section *610.021*

August 28, 2018

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, policies and specific response plans 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. Financial records related to the procurement of or expenditures relating to operational guidelines, policies or plans purchased with public funds shall be open. 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;

(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 intereSaint If retention is not necessary, the documents shall be returned to the nonpublic governmental body or destroyed;

(20) The portion of a record that identifies security systems or access codes or authorization codes for security systems of real property;

(21) 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 [sic] paid by, or on behalf of, a public governmental body for such computer, computer system, computer network, or telecommunications network shall be open;

(22) 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;

(23) Records submitted by an individual, corporation, or other business entity to a public institution of higher education in connection with a proposal to license intellectual property or perform sponsored research and which contains sales projections or other business plan information the disclosure of which may endanger the competitiveness of a business; and

(24) Records relating to foster home or kinship placements of children in foster care under section 210.498.

(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, A.L. 2013 H.B. 256, 33 & 305, A.L. 2018 S.B. 819)

See also, R.S. Mo. Sections 109.180 (public records open to inspection, except as otherwise provided; penalty for refusal), 109.190 (right of person to photograph public records), and 407.1500 (definitions and required notice of breach of security).

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

1. Background and Applicability.

a. Background. Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) calls for the issuance of guidelines to protect privacy and civil liberties in the development and use of the "information sharing environment" (ISE). Section 1 of Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, provides that, "[t]o the maximum extent consistent with applicable law, agencies shall … give the highest priority to … the interchange of terrorism information among agencies … [and shall] protect the freedom, information privacy, and other legal rights of Americans in the conduct of [such] activities …." These Guidelines implement the requirements under the IRTPA and EO 13388 to protect information privacy rights and provide other legal protections relating to civil liberties and the legal rights of Americans in the development and use of the ISE.
b. Applicability. These Guidelines apply to information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and Federal laws of the United States ("protected information"). For the intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. Government expressly determines by Executive Order, international agreement, or other similar instrument, should be covered by these Guidelines.

2. Compliance with Laws.
a. General. In the development and use of the ISE, all agencies shall, without exception, comply with the Constitution and all applicable laws and Executive Orders relating to protected information.
b. Rules Assessment. Each agency shall implement an ongoing process for and assessing the laws, Executive Orders, policies, and procedures that apply to the protected information that it will make available or access through the ISE. Each agency shall identify, document, and comply with any legal restrictions applicable to such information. Each agency shall adopt internal policies and procedures requiring it to:

(i) only seek or retain protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency; and

(ii) ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.
c. Changes. If, as part of its rules assessment process, an agency:
(i) identifies an issue that poses a significant risk to information privacy rights or other legal protections, it shall as appropriate develop policies and procedures to provide protections that address that issue;
(ii) identifies a restriction on sharing protected information imposed by internal agency policy, that significantly impedes the sharing of terrorism information, homeland security information, or law enforcement information (as defined in Section 13 below) in a manner that does not appear to be required by applicable laws or to protect information privacy rights or provide other legal protections, it shall review the advisability of maintaining such restriction;
(iii) identifies a restriction on sharing protected information, other than one imposed by internal agency policy, that significantly impedes the sharing of information in a manner that does not appear to be required to protect privacy rights or provide other legal protections, it shall review such restriction with the ISE Privacy Guidelines Committee (described in Section 12 below), and if an appropriate internal resolution cannot be developed, bring such restriction to the attention of the Attorney General and the Director of National Intelligence (DNI). The Attorney General and the DNI shall review any such restriction and jointly submit any recommendations for changes to such restriction to the Assistant to the President for Homeland Security and Counterterrorism, the Assistant to the President for National Security Affairs, and the Director of the Office of Management and Budget for further review.

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

4. Identification of Protected Information to be Shared through the ISE.
a. Identification and Prior Review. In order to facilitate compliance with these Guidelines, particularly Section 2 (Compliance with Laws) and Section 3 (Purpose Specification), each agency shall identify its data holdings that contain protected information to be shared through the

ISE, and shall put in place such mechanisms as may be reasonably feasible to ensure that protected information has been reviewed pursuant to these Guidelines before it is made available to the ISE.

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

(i) the information pertains to a United States citizen or lawful permanent resident;

(ii) the information is subject to specific information privacy or other similar restrictions on access, use or disclosure, and if so, the nature of such restrictions; and

(iii) there are limitations on the reliability or accuracy of the information.

5. Data Quality.

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

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

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

(i) take appropriate steps, when merging protected information about an individual from two or more sources, to ensure that the information is about the same individual;

(ii) investigate in a timely manner alleged errors and deficiencies and correct, delete, or refrain from using protected information found to be erroneous or deficient; and

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

6. Data Security.

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

7. Accountability, Enforcement and Audit.

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

(i) have and enforce policies for reporting, investigating, and responding to violations of agency policies relating to protected information, including taking appropriate action when violations are found;

(ii) provide training to personnel authorized to share protected information through the ISE regarding the agency's requirements and policies for collection, use, and disclosure of protected information, and, as appropriate, for reporting violations of agency privacy-protection policies;

(iii) cooperate with audits and reviews by officials with responsibility for providing oversight with respect to the ISE; and

(iv) designate each agency's ISE privacy official to receive reports (or copies thereof if the agency already has a designated recipient of such reports) regarding alleged errors in protected information that originate from that agency.

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

8. Redress.

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

9. Execution, Training, and Technology.

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

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

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

10. Awareness.

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

.

11. Non-Federal Entities.

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

12. Governance.

a. ISE Privacy Officials. Each agency's senior official with overall agency-wide responsibility for information privacy issues (as designated by statute or executive order, or as otherwise

identified in response to OMB Memorandum M-05-08 dated February 11, 2005), shall directly oversee the agency's implementation of and compliance with these Guidelines (the "ISE privacy official"). If a different official would be better situated to perform this role, he or she may be so designated by the head of the agency. The ISE privacy official role may be delegated to separate components within an agency, such that there could be multiple ISE privacy officials within one executive department. The ISE privacy official shall be responsible for ensuring that (i) the agency's policies, procedures, and systems are appropriately designed and executed in compliance with these Guidelines, and (ii) changes are made as necessary. The ISE privacy official should be familiar with the agency's activities as they relate to the ISE, possess all necessary security clearances, and be granted the authority and resources, as appropriate, to identify and address privacy and other legal issues arising out of the agency's participation in the ISE. Such authority should be exercised in coordination with the agency's senior ISE official.

b. ISE Privacy Guidelines Committee. All agencies will abide by these Guidelines in their participation in the ISE. The PM shall establish a standing "ISE Privacy Guidelines Committee" to provide ongoing guidance on the implementation of these Guidelines, so that, among other things, agencies follow consistent interpretations of applicable legal requirements, avoid duplication of effort, share best practices, and have a forum for resolving issues on an inter-agency basis. The ISE Privacy Guidelines Committee is not intended to replace legal or policy guidance mechanisms established by law, executive order, or as part of the ISE, and will as appropriate work through or in consultation with such other mechanisms. The ISE Privacy Guidelines Committee shall be chaired by the PM or a senior official designated by the PM, and will consist of the ISE privacy officials of each member of the Information Sharing Council. If an issue cannot be resolved by the ISE Privacy Guidelines Committee, the PM will address the issue through the established ISE governance process. The ISE Privacy Guidelines Committee should request legal or policy guidance on questions relating to the implementation of these Guidelines from those agencies having responsibility or authorities for issuing guidance on such questions; any such requested guidance shall be provided promptly by the appropriate agencies. As the ISE governance process evolves, if a different entity is established or identified that could more effectively perform the functions of the ISE Privacy Guidelines Committee, the ISE Privacy Guidelines Committee structure shall be modified by the PM through such consultation and coordination as may be required by the ISE governance process, to ensure the functions and responsibilities of the ISE Privacy Guidelines Committee remain priorities fully integrated into the overall ISE governance process.

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

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

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

“Terrorism information,” consistent with section 1016(a)(4) of IRTPA, means all information relating to (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations, (C) communications of or by such groups or individuals, or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

“Homeland security information,” as derived from section 482(f)(1) of the Homeland Security Act of 2002, means any information possessed by a Federal, State, local, or tribal agency that relates to (A) a threat of terrorist activity, (B) the ability to prevent, interdict, or disrupt terrorist activity, (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization, or (D) a planned or actual response to a terrorist act.

“Law enforcement information” for the purposes of the ISE means any information obtained by or of interest to a law enforcement agency or official that is (A) related to terrorism or the security of our homeland and (B) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of, or response to, criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.
b. The treatment of information as “protected information” under these Guidelines does not by itself establish that the individual or entity to which such information pertains does in fact have information privacy or other legal rights with respect to such information.
c. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide the cooperation, assistance, and information necessary for the implementation of these Guidelines.

d. These Guidelines:

(i) shall be implemented in a manner consistent with applicable laws and executive orders, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;

(ii) shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;

(iii) shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

(iv) are intended only to improve the internal management of the Federal Government and are not intended to, and do not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies….

https://www.dni.gov/files/ISE/documents/DocumentLibrary/PrivacyGuidelines20061204_1.pdf

APPENDIX D

OECD Privacy Principles

The Organization for Economic Cooperation and Development (OECD) privacy guidelines, the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, became applicable on September 23, 1980.*

The eight principles set out by the OECD are:

Collection Limitation Principle--There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle--Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.

Purpose Specification Principle--The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle--Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.

Security Safeguards Principle--Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

Openness Principle--There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle--An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle--A data controller should be accountable for complying with measures, which give effect to the principles stated above.

[*See*, generally and for commentary and guidance regarding these principles: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html]

See also, for general guidance, the LEIU File Guidelines posted at <http://it.ojp.gov/documents/LEIU_Crim_Intel_File_Guidelines.pdf>

Fair Information Practice Principles

December 29, 2008 PRIVACY POLICY GUIDANCE MEMORANDUM Memorandum Number: 2008-01 FROM: Hugo Teufel III Chief Privacy Officer SUBJECT: The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security

I. PURPOSE This Memorandum memorializes the Fair Information Practice Principles (FIPPs) as the foundational principles for privacy policy and implementation at the Department of Homeland Security (DHS). [... IV. ...] The FIPPs provide the foundation of all privacy policy development and implementation at the Department and must be considered whenever a DHS program or activity raises privacy concerns or involves the collection of personally identifiable information from individuals, regardless of their status.

V. THE FAIR INFORMATION PRACTICE PRINCIPLES • **Transparency**: DHS should be transparent and provide notice to the individual regarding its collection, use, dissemination, and maintenance of personally identifiable information (PII). • **Individual Participation**: DHS should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. DHS should also provide mechanisms for appropriate access, correction, and redress regarding DHS's use of PII. • **Purpose Specification**: DHS should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
6 http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.Fil e.v1.1 7 Homeland Security Act of 2002, as amended, 6 U.S.C. § 142. Privacy Policy: Fair Information Practice Principles December 29, 2008 Page 4 • **Data Minimization**: DHS should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s). • **Use Limitation**: DHS should use PII solely for the purpose(s) specified in the notice. Sharing PII outside the Department should be for a purpose compatible with the purpose for which the PII was collected. • **Data Quality and Integrity**: DHS should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete. • **Security**: DHS should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure. • **Accountability and Auditin**g: DHS should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.

The DHS Privacy Office, therefore, has adopted the FIPPs as its privacy policy framework and seeks to apply them to the full breadth and diversity of DHS programs and activities. Any questions regarding the application or implementation of these principles should be directed to the DHS Privacy Office at privacy@dhs.gov or (703) 235-0780.