Kansas City Regional Fusion Center

Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy
April 15, 2019

Kansas City Regional Fusion Center
Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy

A. Purpose Statement

1. The mission of the Kansas City Regional Fusion Center (KCRFC), herein also referred to as "the center", is to bring federal, state, and local representatives together with public and private sector partners to increase safety and security within our area of responsibility by combating international and domestic terrorism, assisting in the protection of critical infrastructure and key resources, and mitigating threats of school violence, workplace violence, and incidents involving potential mass casualties as well as any other related criminal acts. This will be accomplished through collecting, evaluating, analyzing, and disseminating information and intelligence data (records) regarding criminal and terrorist activity in a timely, effective, and appropriately secure manner. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the federal Privacy Act of 1974, as amended, to ensure that information privacy and other legal rights of individuals and organizations are protected (see definitions of "Fair Information Practice Principles" [FIPPs] and "Protected Information" in Appendix A, Terms and Definitions and the FIPP's in Appendix C, Fair Information Practice Principles).

2. The purpose of this P/CRCL protection policy is to articulate the KCRFC's position on how it handles the personally identifiable information (PII) (see Appendix A, Terms and Definitions) and other personal, sensitive information about individuals and organizations that it seeks, collects, receives, maintains, uses, accesses, archives, or discloses in the normal course of business and to promote KCRFC and user conduct that complies with applicable federal, state, local, tribal, and territorial laws and that assists the center and its users in:

    a. Increasing public safety and improving national security.

    b. Minimizing the threat and risk of injury to specific individuals.

    c. Minimizing the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health.

    d. Minimizing the threat and risk of damage to real or personal property.

    e. Protecting individual privacy, civil rights, civil liberties, and other protected interests.

    f. Protecting the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information.

    g. Minimizing the reluctance of individuals or groups to use or cooperate with the justice system.

    h. Supporting the role of the justice system in society.

i. Promoting governmental legitimacy and accountability.

j. Not unduly burdening the ongoing business of the justice system.

k. Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

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

2. The KCRFC will provide a printed or electronic copy of this policy to all center personnel, non-center personnel who routinely work at the center and participating agency personnel. The KCRFC will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

3. All KCRFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable laws protecting P/CRCL, (see Appendix B, "Federal, State, Local, Tribal, and Territorial Laws, Regulations, and Guidance Relevant to Seeking, Retaining, and Disseminating Justice Information").

4. The KCRFC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to those listed in Appendix B, "Federal, State, Local, Tribal, and Territorial Laws, Regulations, and Guidance Relevant to Seeking, Retaining, and Disseminating Justice Information".

Information which furthers an administrative or other non-analytical purpose (such as personnel files or information regarding fiscal, regulatory, or other matters associated with the operation of the KCRFC as a governmental entity) or which does not identify an individual or organization will be handled in a manner which complies with all applicable privacy laws and regulations but will not be subject to the provisions of this policy.

C. Governance and Oversight

1. Primary responsibility for the operation of the KCRFC**;** its justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, data quality,

analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the Director of the center.

2. The KCRFC Privacy Officer will periodically review and update the P/CRCL policy in response to changes in law and implementation experience.

3. The KCRFC's Privacy Officer is appointed by the Director of the center. The Privacy Officer may receive reports regarding alleged errors and violations of the provisions of this policy, may coordinate complaint processing with the Kansas City, Missouri Police Department (KCPD) Office of Community Complaints, serving as the liaison for the center and ensure that P/CRCL protections are implemented through KCRFC practices and policies. The Privacy Officer can be contacted at 635 Woodland, Suite 2105B, Kansas City, Missouri 64106 or KCRFC@kcpd.org.

4. The KCRFC's Privacy Officer ensures that enforcement procedures and sanctions outlined in Section N are adequate and enforced.

D. Definitions

For examples of primary terms and definitions used in this policy, refer to Appendix A, Terms and Definitions.

E. Information

1. The KCRFC will seek or retain information (including "protected attributes," subject to conditions articulated in Section E.2.) that:

   a. Is based on a possible threat to public safety, public order, or the enforcement of criminal law, or

   b. Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in supporting 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

   c. 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

   d. Is useful in crime or threat analysis or in the administration of criminal justice, force deployment and public safety, anti-terrorism, counter-terrorism or homeland security responsibilities (including topical searches), and

   e. The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and

   f. The information was collected in a fair and lawful manner.

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

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

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

3. The KCRFC applies labels to center-originated information or ensures that the originating agency has applied labels to indicate to the accessing authorized user that:

   a. The information is protected information (as defined by the ISE Privacy Guidelines and) to the extent expressly provided in this policy, includes organizational entities. Specifically information that pertains to a United States citizen or lawful permanent resident.

   b. The information is subject to Chapter 45 of the Kansas Statutes Annotated (Kansas Open Records Act [KORA] and Kansas Open Meetings Act [KOMA]) and Chapter 610 of the Revised Statutes of Missouri (Missouri Sunshine Laws) restricting access, use, and disclosure.

4. The KCRFC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. The information may consist of tips and leads (including SAR data), law enforcement information/case support, intelligence or other information.

   Information included in the Tips and Leads category will additionally be labeled as to:

      a. The nature of the source as it affects veracity (e.g., anonymous tip, law enforcement, public agencies or private sector).

      b. The reliability of the source (e.g., reliable, unreliable or unknown).

      c. The validity of the content (e.g., confirmed/substantiated, partially confirmed, not confirmed/unsubstantiated or unable to confirm).

   These requirements do not apply to analytical products and other information obtained from or originated by a federal, state, local, tribal, or territorial entity that has itself

evaluated the validity and reliability of information in accordance with their principles or the conventions of the intelligence and law enforcement communities.

5. KCRFC personnel are required to adhere to practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads (including SAR information). Center personnel will:

    a. Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been subjected to an evaluation or screening process to determine its credibility and value. Categorize the information as unsubstantiated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use standard reporting formats and data collection codes (see Information Sharing Environment Functional Standard Suspicious Activity Reporting Version 1.5.5, Section IV: ISE-SAR Exchange Data Model) for SAR information.

    b. Forward the information to the proper agency for further evaluation or investigation of the tip, lead or report in accordance with applicable procedures and direction provided by the KCRFC leadership.

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

    d. 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 (e.g., "need-to-know" and "right-to-know" access or dissemination for PII).

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

    f. Retain PII and other sensitive personal information for one (1) year in order to work an un-validated tip or lead or a suspicious activity report, to determine its credibility and value or assign a "disposition" label (e.g., Open, Under Investigation, Cleared by Arrest, Cleared Other, Information Only, Unfounded, Unverified, Already Known, No Disposition Received, Other or N/A) 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.

    g. Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or

similar to the system that secures data that rises to the level of reasonable suspicion.

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

7. The KCRFC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the ISE. Further, the center will provide notice mechanisms, including but not limited to metadata or data 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.

8. The KCRFC 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:

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

    b. The title and contact information for the person to who questions regarding the information should be directed.

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

10. The KCRFC will keep a record of the source of all information sought and collected by the center. In this context, "source" refers to the individual or entity which provided the information to the KCRFC. If the source is an agency, governmental entity, or other organization, such as a corporation or association, this requirement can be met by maintaining the name of the agency, governmental entity, or organization, as long as the specific unit of that agency, governmental entity, or organization which provided the information is identified.

F. Acquiring and Receiving Information

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

    a. 28 CFR Part 23 regarding "criminal intelligence information," as applicable.

b. FIPPs, see Appendix C, (but note that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy).
c. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP) (Ver. 2).

d. Constitutional provisions; Chapter 45 of the Kansas Statutes Annotated (KORA and KOMA) and Chapter 610 of the Revised Statutes of Missouri (Missouri Sunshine Laws) and administrative rules as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

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

3. The KCRFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, ethnicity, national origin, religion, etc.) and civil liberties (speech, assembly, association, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared. (See Sections E.2 and F.2).

4. Information-gathering and investigative techniques used by the KCRFC will (and those used by originating agencies should) be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access the KCRFC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

6. The KCRFC will contract only with commercial database entities that provide an assurance that their methods for gathering PII comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

7. The KCRFC will not directly or indirectly receive, seek, accept, or retain information from:

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

   b. An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. Data Quality Assurance

1. The KCRFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources, is accurate, current, complete, including the relevant context in which it was sought or received and other related information.

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

3. At the time of retention, when applicable, the information will be labeled regarding its level of quality (e.g., Accurate, Complete, Current, Verifiable or Reliable).

4. The KCRFC corrects, in a timely manner, any discovered errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

H. Collation and Analysis

1. Information acquired or received by the KCRFC or accessed from other sources will be analyzed only by qualified and properly trained individuals who have successfully completed a background check and possess the appropriate security clearance.

2. Information subject to collation and analysis is information as defined and identified in Section E of this policy.

3. Information acquired or received by the KCRFC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

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

    b. 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.

I. Merging Records

The KCRFC does not currently merge records.

J. Sharing and Disclosure

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

a. The information to which a particular group or class of users can have access based on the group or class.

b. The information a class of users can receive.

c. To whom, individually, the information can be disclosed and under what circumstances.

2. The KCRFC adheres to the current version of the ISE-SAR Functional Standard for its SAR process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially associated with terrorism.

3. Access to or disclosure of records retained by the KCRFC will be provided only to persons within the center or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the center for a reasonable period of time.

4. The KCRFC notifies agencies external to the KCRFC that they may not freely disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

5. Records retained by the KCRFC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center for a reasonable period of time.

6. Information gathered or collected and records retained by the KCRFC 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 center; the nature of the information requested, accessed, or received; and the specific purpose will be kept by the center for a reasonable period of time.

7. Information gathered or collected and records retained by the KCRFC 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 center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center 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 center and the nature of the information accessed will be kept by the center**.**

8. Information gathered or collected and records retained by the KCRFC will not be:

    a. Sold, published, exchanged, or disclosed for commercial purposes.

    b. Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency or specifically authorized by the originating agency.

    c. Disseminated to persons not authorized to access or use the information.

9. There are several categories of records that will ordinarily not be provided to the public:

    a. Records that may be kept confidential by law are exempt from disclosure requirements under Chapter 45 of the Kansas Statutes Annotated (KORA and KOMA) and Chapter 610 of the Revised Statutes of Missouri (Missouri Sunshine Laws).

    b. Information determined by the federal government to meet the definition of "classified information" as defined in the National Security Act, Public Law 235, Section 606, and in accordance with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

    c. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under applicable law. However, certain law enforcement records must be made available for inspection and copying under applicable law.

    d. A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under 6 U.S.C. § 482. By way of example, this may include a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under applicable law or an act of agricultural terrorism under applicable law, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

    e. Protected federal, state, local, tribal, or territorial records, which may include records originated and controlled by another agency that cannot, under applicable law, be shared without permission.

    f. A record or part of a record that constitutes trade secrets or information that is commercial, financial, or otherwise subject to a nondisclosure agreement that was obtained from a person and is privileged and confidential under applicable law.

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

K. Redress

1. Disclosure

a. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in K., Redress, 2., Corrections, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the KCRFC. The individual may obtain a copy of the information. The center's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual.

b. The existence, content, and source of the information will not be made available by the KCRFC to an individual when restricted under Chapter 45 of the Kansas Statutes Annotated (KORA and KOMA) and Chapter 610 of the Revised Statutes of Missouri (Missouri Sunshine Laws)**.** Examples may include:

1) Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.

2) Disclosure would endanger the health or safety of an individual, organization, or community.

3) The information is in a criminal intelligence information system subject to 28 CFR Part 23.

4) The information relates to 6 U.S.C. § 482 or other applicable law.

5) The information source does not reside with the center.

6) The center did not originate and does not have a right to disclose the information.

7) Other authorized basis for denial.

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

2. Corrections

If an individual requests correction of information originating with the KCRFC that has been disclosed, the center's Privacy Officer or designee will inform the individual of the procedure for requesting a review of the information and considerations of corrections. If the requested corrections are denied in whole or in part, the individual may file a complaint as provided in Section K.3. A record will be kept of all requests for corrections and the resulting action, if any.

3. Complaints

The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Privacy Officer, 635 Woodland, Suite 2105B, Kansas City, Missouri 64106, KCRFC@kcpd.org or by the KCPD Office of Citizen Complaints. 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 center, the Privacy Officer will notify the originating agency in writing or electronically, and ask that they handle the dispute. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

L. Security Safeguards

1. The KCRFC's Security Liaison is designated and trained to serve as the center's security officer.

2. The center will comply with generally accepted industry or other applicable standards for security, in accordance with KCRFC Standard Operating Procedure for the Protection and Safeguarding of Classified National Security Information (CNSI). Security safeguards will cover any type of medium (printed and electronic) or technology (e.g., physical servers, virtual machines or mobile devices) used in a work-related KCRFC activity.

   The KCRFC will operate in a secure facility protected from external intrusion. The center will utilize secure internal and external safeguards against network intrusions. Access to the center's databases from outside the facility will be allowed only over secure networks.

3. The KCRFC will secure tips, leads, and SAR information in a 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.

4. The KCRFC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by personnel authorized to take such actions.

5. Access to KCRFC information will be granted only to center personnel whose positions and job duties require such access; who have successfully completed a background

check and possess an appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

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

7. The KCRFC will utilize email logs and spreadsheets to maintain audit trails of requested and disseminated information.

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

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

10. In the event of a data breach, the KCRFC's host agency, KCPD, utilizes protocols established by the Criminal Justice Information Services (CJIS) and the Missouri Uniform Law Enforcement System (MULES).

M. Information Retention and Destruction

1. All criminal intelligence information, as that term is defined in 28 CFR Part 23, will be reviewed for record retention (validation or purge) by KCRFC at least every five (5) years, in accordance with 28 CFR Part 23. For other information or intelligence, the record retention will be established by state law or local ordinance, or in accordance with a retention schedule established by the KCPD**.**

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

3. The KCRFC may delete information or return it to the originating agency once its retention period has expired as provided by this policy.

4. No approval will be required from the originating agency before information held by the KCRFC is destroyed or returned in accordance with this policy.

5. Notification of proposed destruction or return of records may or may not be provided to the originating agency by the KCRFC.

N. Accountability and Enforcement

1. Information System Transparency

a. The KCRFC will be open with the public in regard to information and intelligence collection practices. The center's P/CRCL policy will be provided to the public for review, made available upon request, and posted on the center's website (www.KCRFC.org).

b. The Privacy Officer may receive reports regarding alleged errors and violations of the provisions of this policy, may coordinate complaint processing with the Kansas City Missouri Police Department, KCPD, Office of Community Complaints, serving as the liaison for the center and ensure that P/CRCL protections are implemented through KCRFC practices and policies. The Privacy Officer can be contacted at 635 Woodland, Suite 2105B, Kansas City, Missouri 64106 or KCRFC@kcpd.org.

2. Accountability

a. KCRFC's documentation of queries made to the KCRFC will identify the user initiating the query.

b. The KCRFC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

c. The KCRFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance with the provisions of this policy and applicable law.

d. The KCRFC's personnel or other authorized users shall report errors and suspected or confirmed violations of center policies relating to protected information to the center's Privacy Officer.

e. The KCRFC's Privacy Officer, will review and update the provisions protecting P/CRCL contained in this policy periodically and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

3. Enforcement

a. If any center personnel, participating agency personnel, or 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 KCRFC will:

1) Suspend or discontinue access to information until the matter has been investigated and resolved.

2) If violations are found, report such violations to the user's chain of command for disciplinary review.

3) If the authorized user is from an agency external to the center, request that the user's employer enforce their agencies pertinent disciplinary provisions.

4) Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy, if appropriate.

b. The KCRFC reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the center's P/CRCL policy.

O. Training

1. The KCRFC will require the following individuals to participate in training programs regarding implementation of and adherence to the privacy, civil rights, and civil liberties policy:

    a. All center personnel.

    b. Participating agency personnel.

    c. Personnel providing information technology services to the center.

2. The KCRFC will provide special training regarding the center's requirements and policies for collection, use, and disclosure of protected information to personnel authorized to share protected information through the ISE.

3. The KCRFC's P/CRCL policy training program will cover:

    a. Purposes of the P/CRCL protection policy.

    b. Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.

    c. How to implement the policy in the day-to-day work of the user, whether a paper or systems user.

    d. The potential impact of violations of the agency's P/CRCL policy.

    e. Mechanisms for reporting violations of center P/CRCL protection policies and procedures.

    f. How to identify, report, and respond to a suspected or confirmed breach of PII.

    g. Updates to the P/CRCL policy, if any, in response to changes in law and implementation experience.

4. Subject to course availability, the Privacy Officer of the KCRFC will also take courses offered by the U.S. Department of Homeland Security addressing:

    a. P/CRCL training of trainers.

    b. Derivative classification markings.

    c. Any other applicable training.

Appendix A: Terms and Definitions

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

Access—Information access is being able to get to (usually having permission to use) particular information on a computer. Web access means having a connection to the Internet through an access provider or an online service provider.

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

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.

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

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

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

Authorization—The process of granting a person, a computer process, or a device access to certain information, services, or functionality. Authorization is derived from the identity of the person, the computer process, or the device requesting access, which is verified through authentication. See Authentication.

Biometrics—A general term used alternatively to describe a characteristic or a process. (1) As a characteristic: a measureable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. (2) As a process: automated methods of recognizing an individual based on measureable biological (anatomical and physiological) and behavioral characteristics. See Glossary, Facial Identification Scientific Working Group (FISWG), version 1.1, February 2, https://www.fiswg.org/FUSWG_Glossary_v1.1_2012_02_02.pdf.

Center- Refers to the Kansas City Regional Fusion Center (KCRFC) and all participating state agencies of the KCRFC.

Civil Liberties—According to the U.S. Department of Justice's Global Justice Information Sharing Initiative, the term "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.[1] 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.

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, gender, national origin, religion, 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 federally or state protected characteristic. For example, a state may have constitutional or statutory language regarding parental status. Generally, the term "civil rights" involves positive (or affirmative) government action to protect against infringement, while the term "civil liberties" involves restrictions on government.[2]

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—Refers to the obligations of individuals and institutions to appropriately use information and data under their control once they have been disclosed to them and in accordance with applicable data security laws and policies.

---

[1] Civil Rights and Civil Liberties Protections Guidance, at 4 (August 2008), available at https://www.ise.gov/sites/default/files/CR-CL_Guidance_08112008.pdf.

[2] The definition of "civil rights" is a modified version of the definition contained in the National Criminal Intelligence Sharing Plan (NCISP), at pp. 5–6, and Civil Rights and Civil Liberties Protections Guidance, at 5, available at https://www.ise.gov/sites/default/files/CR-CL_Guidance_08112008.pdf.

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

Criminal Activity— A behavior, an action, or an omission that is punishable by criminal law.

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

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

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

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

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, receipt, use, dissemination, retention, purging, and protection of information.

Data Quality—Refers to various aspects of the information: the accuracy and validity of the actual values of the data, information structure, and database/information repository design. Traditionally, the basic elements of data quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, data quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy. This concept is also addressed as one of the Fair Information Practice Principles (FIPPs), Data Quality/Integrity. See Appendix C for further background on the FIPPs.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of PII in any manner—electronic, verbal, or in writing—to an individual, agency, or an organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information

which may be available only to certain people for certain purposes but which is not available to everyone.

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, compact disc 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, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or 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 the raw data.

Fair Information Practice Principles (FIPPs)—FIPPs are a set of internationally recognized principles that inform information privacy policies both within government and the private sector. Although specific articulations of the FIPPs vary and have evolved since their genesis in the 1970s, core elements are consistent among nations, states, and economic sectors. These core elements are incorporated into information privacy laws, policies, and governance documents around the world. They provide a straightforward description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done with regard to privacy in integrated justice systems. Because of operational necessity, it may not always be possible to apply all of the principles equally. For example, the Individual Participation Principle (#8) may be of limited applicability in intelligence operations, as fusion centers do not generally engage with individuals. That said, fusion centers and all other integrated justice systems should endeavor to apply the FIPPs where practicable.
The eight principles 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/Transparency
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—Defined in the ISE-SAR Functional Standard 1.5.5 as "[a] collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combines resources, expertise, or information with the goal of maximizing the ability of such agencies to detect, prevent, investigate, apprehend, and respond to criminal or terrorist activity." (Source: Section 511 of the 9/11 Commission Act). State and major urban area fusion centers serve as focal points within the State and local environment for the receipt, analysis,

gathering, and sharing of threat-related information between the federal government and SLTT and private sector partners.

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

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

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

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

Information 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).

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather

and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Invasion of Privacy—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. They 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 investigates and/or responds to terrorist threats. The JTTFs execute the FBI's lead federal agency responsibility for investigating terrorist acts or terrorist threats against the United States.

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

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

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

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

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

Maintenance of Information—Applies to all forms of information storage. This includes 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 to 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 aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

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

Nationwide SAR Initiative (NSI) SAR Data Repository (SDR)—The NSI SDR consists of a single data repository, built to respect and support originator control and local stewardship of data, 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 to perform or assist in a law enforcement, homeland security, or counterterrorism activity or other lawful and authorized government activity, such as to further an investigation or meet another law enforcement requirement.

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

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

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.

Privacy, Civil Rights, and Civil Liberties (P/CRCL) Policy—A printed, published statement that articulates the policy position of an organization on how it handles the PII that it maintains and uses in the normal course of business. The policy should include information relating to the processes of information collection, receipt, access, use, dissemination, retention, and purging. It is likely to be informed by the Fair Information Practice Principles (FIPPs). The purpose of the P/CRCL policy is to articulate that the center will adhere to those legal requirements and center policy determinations that enable collection, receipt, access, use, dissemination, retention, and purging of information to occur in a manner that protects personal privacy interests. A well-developed and implemented P/CRCL policy uses justice entity resources wisely and effectively; protects the center, the individual, and the public; and promotes public trust.

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

Personally Identifiable Information—Information that 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." [3]

Preoperational Planning—As defined in ISE-SAR Functional Standard 1.5.5, "preoperational planning describes activities associated with a known or particular planned criminal operation or with terrorist operations generally."

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of PII. 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); and to avoid being seen or overheard in particular contexts.

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Protected Information—For the nonintelligence community, protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under the Constitution and laws of the United States.

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

---

[3] 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 the information, see Revision of Office of Management and Budget Circular A-130: Managing Information as a Strategic Resource, July 2016, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

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

Public—Public includes:

- Any individual and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the center's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the center or participating agency.

Public does not include:

- Any employees of the center or participating entity.
- People or entities, private or governmental, who assist the center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the center is specified in law.

Public Access—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 that is commonly used to describe methods that render data unrecoverable in a storage space or to 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 (e.g., 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 that observation is made which creates in the mind of the reasonable observer, including a law enforcement officer, 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 an 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 PII and is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Redress—Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the center'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 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 an individual's privacy.

Right to Know—A requirement for access to specific information to perform or assist in a lawful and authorized governmental function. 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.

Role-Based Access—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—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of information 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 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:

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

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information—including 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—Defined in the ISE-SAR Functional Standard 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 sensitive infrastructure facilities, site breach or physical intrusion, cyberattacks, testing of security, etc.

Suspicious Activity Report (SAR)—Defined in the ISE-SAR Functional Standard 1.5.5 as "official 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.

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

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside a law enforcement agency that allege or indicate some form of

possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information. However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data. Tips and leads information should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.
A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

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

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.

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 B: Federal and SLTT Laws, Regulations, and Guidance Relevant to Seeking, Retaining, and Disseminating Justice Information

The U.S. Constitution is the primary authority that applies to federal as well as state, local, tribal, and territorial (SLTT) agencies. 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 Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc.[4]

In addition, statutory civil rights protections in the U.S. Constitution 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). When relevant or possibly relevant, agencies/centers are advised to list these laws, regulations, and policies within their privacy, civil rights, and civil liberties (P/CRCL) policies, noting those that may potentially affect the sharing of information, including sharing terrorism-related information in the Information Sharing Environment (ISE).

The development of a privacy, civil rights, and civil liberties policy is primarily designed for center personnel and authorized users to ensure that they 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 are not spelled out or referenced in a center P/CRCL policy, staff and user accountability is greatly diminished; mistakes are made; privacy, civil rights, and civil liberties violations occur; and the public's (and other agencies') confidence in the ability of the center to protect information and intelligence is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, information sharing is enhanced.

It is important to note that federal laws may use different terminology to describe information that identifies an individual (e.g., personal data, personal information, information in identifiable

[4] The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the Information Sharing Environment is explored in a key issues guidance paper titled *Civil Rights and Civil Liberties Protection*, which is available on the ODNI's Office of Partner Engagement-Information Sharing Environment (PE-ISE) website at www.ise.gov.

form). Different laws may have different statutory definitions for the terminology used. Personnel who are charged with developing or updating their center's P/CRCL policy should refer to the applicable statutory definition, in order to ensure that the scope of the terminology used is properly understand and implemented.

A. Federal Laws, Regulations, and Guidance

Following are synopses of federal laws, regulations, and guidance that a center should review and, when appropriate, cite within the policy when developing a P/CRCL policy for a justice information system. The list is arranged in alphabetical order by popular name.

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—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 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 archivist. 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.

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 Part 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 Part 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 Part 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.

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.

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.

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, 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 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

.

B. State, Local, Tribal, and Territorial Laws, Regulations, and Guidelines

The following list provides synopses of SLTT laws, regulations, and guidance that a center should review and, when appropriate, cite within the policy when developing a P/CRCL policy for a justice information system. The list is arranged in alphabetical order by popular name.

[Summarize and provide a citation to applicable SLTT laws, regulations, and guidance and insert below.]

Chapter 45 of the Kansas Statutes Annotated (Kansas Open Records Act [KORA] and Kansas Open Meetings Act [KOMA])

Chapter 610 of the Revised Statutes of Missouri (Missouri Sunshine Laws)

Appendix C: Fair Information Practice Principles

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

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

- At the heart of the Privacy Act of 1974, which applies these principles to U.S. federal agencies.[5]
- Mirrored in many states' laws and in fusion centers' privacy policies.
- In the ISO/IEC 29100 Privacy Framework, which has been adopted by numerous foreign countries and international organizations.

The following formulation of the FIPPs is used and implemented for the Information Sharing Environment (ISE) by the U.S. Department of Homeland Security (DHS).[6] Note, however, that under certain circumstances, the FIPPs may be superseded by authorities paralleling those provided in the federal Privacy Act; state, local, tribal, or territorial law; or center policy.

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

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

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

2. Data Quality/Integrity—PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up to date.

Implementing the Data Quality/Integrity Principle—One important way to minimize potential

[5] 5 U.S.C. § 552a.
[6] 6 U.S.C. § 142.

downstream P/CRCL concerns is to ensure that any information collected, stored, and disseminated is accurate. This includes ensuring that the information provides sufficient context for any PII. Possible approaches include:

- Properly labeling PII.
- Determining a policy for safeguarding PII if there are "mixed" databases (i.e., those databases with PII on U.S. individuals and others, regardless of nationality).
- Instituting a source verification procedure to ensure reporting is based only on authorized data.
- Reconciling and updating PII whenever new relevant information is collected.
- Developing a protocol for ensuring data corrections are passed to those entities with which
- information has been shared.
- Creating a documented process for identifying and addressing situations in which data has been erroneously received, is inaccurate or has been expunged.

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

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

4. Use Limitation—PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law.

Implementing the Use Limitation Principle—Sharing information should be tempered by adherence to key principles such as "authorized access." Use limitation may be implemented by:

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

- receive the information.
-

5. Security/Safeguards—Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure.

Implementing the Security/Safeguards Principle—This principle can be implemented by:

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

6. Accountability/Audit—Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.

Implementing the Accountability/Audit Principle—Strong policies must not only be in place but also be effectively implemented. Accountability can be demonstrated by:

- Ensuring that upon entry for duty, all staff take an oath to adhere to the privacy and civil liberties protections articulated in the center's or host agency's mission, core values statements, other key documents, and/or the U.S. Constitution.
- Conducting effective orientation and periodic refresher training, including P/CRCL protections, for all individuals handling PII.
- Tailoring training to specific job functions, database access, or data source/storage requirements.
- Conducting regular audits of all systems in which records are kept to ensure compliance with the P/CRCL policies and all legal requirements.
- Following a privacy incident handling procedure for any data breaches or policy violations.
- Denying database access to individuals until they have completed mandatory systems access

- training (including training for handling of PII), show a mission need for access, and have any
- necessary clearances.
- Developing targeted and consistent corrective actions whenever noncompliance is found.

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

Implementing the Openness/Transparency Principle—Agencies can implement the Openness/Transparency principle by:

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

8. Individual Participation—To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII.

Implementing the Individual Participation Principle—To the extent appropriate, agencies can implement the Individual Participation principle by:

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