Louisiana State Analytic & Fusion Exchange

PRIVACY POLICY

Revised 05.24.2023

A. PURPOSE STATEMENT

1. The Louisiana State Analytical & Fusion Exchange (LA-SAFE) mission is to collect, evaluate, analyze, and disseminate information and intelligence data (records) regarding criminal and terrorist activity in Louisiana while protecting privacy, civil rights, civil liberties, and other protected interests. This includes implementing appropriate privacy and civil liberties safeguards as outlined in the principles of the Privacy Act of 1974, as amended, to ensure that the 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).

   The purpose of this privacy, civil rights, and civil liberties (P/CRCL) protection policy is to promote LA-SAFE and user conduct that complies with applicable federal, state, local, tribal, and territorial law (see Appendix A, Terms and Definitions) and assists the center and its users in:

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

B. POLICY APPLICABILITY AND LEGAL COMPLIANCE

1. All LA-SAFE personnel, participating agency personnel, personnel providing information technology services to the center, staff members in other public agencies, private contractors providing services to the center, and other authorized users not employed by the center or a contractor will comply with the center'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. LA-SAFE will provide a printed or electronic copy of this policy to all center personnel, non-center personnel who provide services to the center, and to participating and individual users. LA-SAFE will require all LA-SAFE personnel to comply with this policy and the applicable provisions in written acknowledgment, a read receipt, or an electronic signature acknowledging receipt of this policy, in addition to a written agreement.

3. All LA-SAFE personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, agencies from which center information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to Code of Federal Regulations (28 CFR Part

23), Louisiana Constitution Article 1, Section 5, Louisiana Constitution Article 12, Section 3 and Louisiana Revised Statute 44:1 et seq.

4. LA-SAFE has adopted internal operating policies that comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, the Code of Federal Regulations (28 CFR Part 23), Louisiana Constitution Article 1, Section 5, Louisiana Constitution Article 12, Section 3, and Louisiana Revised Statue 44:1 et seq. (see Appendix B, "Federal, State, Local, Tribal, and Territorial Laws, Regulations, and Guidance Relevant to Seeking, Retaining, and Disseminating Justice Information.")

C. GOVERNANCE AND OVERSIGHT

1. Primary responsibility for the operation of LA-SAFE; its justice systems, processes, 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. LA-SAFE is guided by a designated privacy oversight committee that ensures privacy, civil rights, and civil liberties are protected as provided in this policy and by the center's information-gathering and collection, retention, and dissemination processes and procedures.

   The committee will annually review and update the privacy policy in response to changes in law and implementation experience, including the results of audits and inspections. It will solicit input from stakeholders on the development of or proposed updates to the policy.

3. LA-SAFE's privacy committee is guided by a trained Privacy Officer, the center's Director. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the center's redress policy, and serves as the liaison for the center (and for the Information Sharing Environment), ensuring that privacy, civil rights, and civil liberties protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies. The Privacy Officer can be contacted at the following address: lafusion.center@la.gov.

4. LA-SAFE's Privacy Officer ensures that enforcement procedures and sanctions outlined in Section N.2, Enforcement 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. LA-SAFE will seek or retain information (including "protected attributes") subject to conditions articulated in Section E.2. that:

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

- Is useful in crime analysis or the administration of criminal justice and public safety (including topical searches), and
- The source of the information is reliable and verifiable, or limitations on the quality of the information are identified, and
- The information was collected fairly and lawfully, with the knowledge and consent of the individual, if appropriate.

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. Per applicable laws, guidance, and regulations, LA-SAFE will not seek or retain and will inform information-originating agencies not to submit information about individuals or organizations solely based on their religious, political, or social views or activities; their participation in a particular non-criminal 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 (SAR) 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. LA-SAFE applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

   - The information is protected (as defined by the center to include personally identifiable information "PII" on any individual) and includes organizational entities to the extent expressly provided in this policy.
   - The information is subject to [local, state, or federal] laws restricting access, use, or disclosure.

4. At the time LA-SAFE decides to retain information, it will be labeled (by the record, data set, or system of records), to the maximum extent feasible, under applicable limitations on access and sensitivity to disclosure to:

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

5. LA-SAFE personnel must adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads (including SAR information.) Center personnel will:

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

- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, “need-to-know” and “right-to-know” access or dissemination for PII).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain information for five years to work an unvalidated tip or lead to determine its credibility and value or assign a “disposition” label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center’s physical, administrative, and technical security measures to protect tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is similar to the system that secures data that rises to reasonable suspicion.

6. LA-SAFE 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 current policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

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

7. LA-SAFE will take necessary measures to secure access to the center’s information and intelligence resources. Unauthorized access or use of the resources is forbidden. The privacy oversight committee reserves the right to restrict the qualifications and number of personnel having access to the center and to suspend or withhold service to any individual violating this Privacy Policy. The Committee, or persons acting on its behalf, further reserves the right to conduct inspections concerning the proper use and security of the information received from the center.

8. Information disseminated by LA-SAFE will be authorized on a “need to know” and “right to know” basis and will be provided in accordance with applicable laws, rules, and regulations. Furthermore, all personnel receiving, handling, or accessing the center’s data will be trained on those regulations. All personnel having access to LA-SAFE data agree to abide by the following rules:

   - Access to and disclosure of records retained by the center will be provided to those responsible for public protection, safety, or public health.
   - The center’s data will be used only in support of specific purposes as authorized by law and only for those users and purposes specified in the law.
   - Individual passwords will not be disclosed to any other person.
   - Individual passwords will be changed if the password is compromised or improperly disclosed.

- Only personnel assigned to LA-SAFE that have undergone a background check and appropriate security clearance, if applicable, and who have been selected, approved, and trained accordingly will have direct access to the center's acquired or received information.
- Use of the center's data in an unauthorized or illegal manner will subject the requestor to suspension or termination of user privileges, discipline by the requestor's employing agency, and/or criminal prosecution.

9. The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following:

    - Date of birth
    - Law enforcement or corrections system identification number
    - Individual identifiers
        - Fingerprints
        - Photographs
        - Physical description
        - Height / Weight
        - Eye and hair color
        - Race / Ethnicity
        - Tattoos or scars
    - Social security number
    - Driver's license number
    - Other biometrics
        - DNA
        - Retinal scan
        - Facial recognition

10. When combined, the identifiers or characteristics that could establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

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

12. The LA-SAFE Director or his designee reserves the right to deny access to any center user who fails to comply with the applicable restrictions and limitations of the center's policy.

F. ACQUIRING AND RECEIVING INFORMATION

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

    - 28 CFR Part 23 regarding "criminal intelligence information," as applicable.
    - The FIPPs; see Appendix C, "Fair Information Practice Principles," 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.
    - Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Crime Intelligence Sharing Plan* (NCISP) (Ver. 2).
    - Constitutional provisions; Louisiana Constitution Article 1, Section 5, Louisiana Constitution Article 12, Section 3, and Louisiana Revised Statute 44:1 et seq.,

administrative rules, regulations, and policies that apply to multijurisdictional intelligence and information databases.

2. LA-SAFE's SAR process provides for human review and vetting to ensure that information is gathered in an authorized and lawful manner and, when applicable, determined to have a potential terrorism nexus. Law enforcement officers, appropriate center, and participating agency staff members will be trained to recognize behaviors and incidents indicative of criminal activity associated with terrorism.

3. LA-SAFE's SAR process includes safeguards to ensure, to the most significant degree, that only information regarding individuals involved in activities determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards 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. [Refer to policy Sections E.2 and F.2]

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

5. External agencies that access LA-SAFE'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. LA-SAFE will contract only with commercial database entities that assure 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. LA-SAFE will not directly or indirectly receive, seek, accept, or retain information from:
    - An individual or nongovernmental entity that may receive a fee or benefit from providing the information, except as expressly authorized by law or center policy.
    - An individual or information provider legally prohibited from obtaining or disclosing the information.

8. Stakeholder agencies are responsible for ensuring the legal validity of gathered information to include the following minimal guidelines.
    - Information supports reasonable suspicion the individual or organization is involved in criminal conduct, and the information is relevant to that conduct.
    - Information is collected fairly and lawfully, with the knowledge and consent of the individual, if appropriate.
    - LA-SAFE will not seek or retain information about individuals or organizations solely based on their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

9. LA-SAFE will abide by daily operating procedures for the initial collection and verification of information, including the screening process by an Investigative Specialist / call taker and the subsequent review by supervisory personnel.

10. LA-SAFE is maintained for developing information and intelligence for and by participating stakeholder agencies. The decision of agencies to join with LA-SAFE and to decide which databases to provide for center access is voluntary and governed by the laws and rules governing those individual agencies, as well as by applicable federal laws to ensure compliance with

constitutional and statutory laws listed above in protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, and destruction of information.

11. LA-SAFE will seek or retain information that:

    - Is based on a criminal predicate or threat to public safety; or
    - Is based on a reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity; or
    - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or
    - Is useful in crime analysis or the administration of criminal justice and public safety; and
    - The source of the information is reliable and verifiable, or limitations on the quality of the information are identified; and
    - The information was collected fairly and lawfully, with the knowledge and consent of the individual, if appropriate.
    - LA-SAFE may retain information based on a level of suspicion that is less than 'reasonable suspicion,' such as tips, leads, or suspicious activity reports (SARs), subject to the policies and procedures specified in Section IV.

12. Information subject to collation and analysis is defined and identified in Section IV.

13. Prohibited Information for Collection / Reporting:

    - Information on an individual or group merely on the basis that such individuals or group supports unpopular causes;
    - Information on an individual or group based on ethnic background;
    - Information on an individual or group merely based on religious or political affiliations;
    - Information on an individual or group merely based on non-criminal personal habits, actions, or lifestyle;
    - Criminal History Record Information if this information is subject to audit and dissemination restrictions.

14. Information is not to be collected on a person because of race, religion, national origin, political affiliation, support of unpopular causes, social views or activities, participation in a particular non-criminal organization or lawful event, citizenship, age, ethnicity, place of origin, disability, gender, or sexual orientation. Unless directly related to criminal activity, a group or individual's tendencies are not a law enforcement concern.

15. LA-SAFE personnel will assess the information's nature, usability, and quality. Personnel will assign categories to the information to reflect the assessment, such as:

    - Whether the information consists of tips and leads, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, or case progress;
    - The nature of the source as it affects veracity. (Anonymous tip, trained interviewer, public record, private sector);
    - The reliability of the source;
    - The validity of the content.

16. Non-criminal information may be entered into the Records Management System (RMS) and/or organizations that meet the criteria of Section E.

17. Non-criminal information must be clearly labeled as "Non-Criminal Identifying Information." This makes it obvious to any reader of the Intelligence Report that the information is not criminal but is used to identify the individual and/or organization/entity with a criminal nexus. Information shall be entered into the RMS pursuant to applicable limitations on access and sensitivity of disclosure to:

    - Protect confidential sources and police undercover techniques and methods;
    - Not interfere with or compromise pending criminal investigations;
    - Protect an individual's right to privacy, civil rights, and civil liberties; and
    - Provide legally required protection based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

18. LA-SAFE will keep a record of the source of all information sought and collected by the center.

19. LA-SAFE adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting process, including using a standard reporting format, commonly accepted indicators/behaviors, and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity related to terrorism and other crimes. LA-SAFE personnel must adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads, and SARs information. LA-SAFE personnel will:

    - Before allowing access to or dissemination of the information, attempt to validate or refute the information and assess it for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information fail. LA-SAFE will use a standard reporting format and commonly accepted indicators and behaviors for SAR information.
    - Store the information using the same storage method used for data that rises to the level of reasonable suspicion. It includes an audit and inspection process, supporting documentation, and data labeling to delineate it from other information.
    - Allow access to or disseminate the information using the same access or dissemination method used for data that rises to the level of reasonable suspicion (need to know / right to know).
    - Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, public safety, and analytical purposes or when credible information indicates potential imminent danger to life or property.
    - Retain information for a period of time sufficient to work an invalidated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
    - Adhere to LA-SAFE's physical, administrative, and technical security measures that are in place to protect and secure all its information. All information will be secured in a system that is the same or similar to the system that secures data that rises to the level of reasonable suspicion.

20. LA-SAFE incorporates the gathering, processing, reporting, analyzing, and sharing of criminal and terrorism-related suspicious activities and incidents (SAR process) into current 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.

21. LA-SAFE's SAR process provides for human review and vetting to ensure that information is legally gathered and, where applicable, determined to have a potential criminal or terrorism nexus. Law enforcement officers, appropriate center, and participating agency staff will be trained to recognize those behaviors and incidents indicative of criminal activity related to terrorism or other crimes.

22. LA- SAFE's SAR process includes safeguards to ensure, to the greatest degree, that only information regarding individuals involved in activities that are consistent with criminal activities associated with terrorism or other crimes will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

G. DATA QUALITY ASSURANCE

1. LA-SAFE will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.
2. LA-SAFE will implement a process for additional face development during the vetting process where a SAR includes PII and is based on behaviors that are not inherently criminal. LA-SAFE 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. LA-SAFE investigates, in a timely manner, alleged 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.
4. The labeling of retained information will be reevaluated by LA-SAFE or the originating agency when new information is gathered that impacts the confidence (source reliability and content validity) in previously retained information.
5. LA-SAFE will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to collect the information (except when the center's information source did not act as the agent of the center in gathering the information).
6. Originating agencies external to LA-SAFE are responsible for reviewing the quality and accuracy of the data accessed by or provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing, electronically, or by phone, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date or unverifiable.
7. LA-SAFE will use written or documented electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center

because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

8. Information acquired or received by LA-SAFE or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
   - Further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives and priorities established by the center, and
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged or engaging in criminal (including terrorist) activities.
9. The agencies participating in LA-SAFE remain the owners of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by LA-SAFE. Inaccurate personal information can have a damaging impact on the person concerned and the integrity and functional value of the center. LA-SAFE personnel will endeavor to ensure the accuracy of information received through database searches by crosschecking other data systems and open-source information. To maintain the center's integrity, any information obtained through the center will be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken. Any third-party information obtained by LA-SAFE will not be further disseminated without approval from the originator of the information. User agencies and individual users are responsible for compliance with the use and further dissemination of such information and the purging and updating the data.

H. COLLATION AND ANALYSIS

1. Only qualified and properly trained individuals who have successfully completed a background check and possess the appropriate security clearance will analyze information acquired or received by LA-SAFE or accessed from other sources.
2. Information subject to collation and analysis is defined and identified in Section E, Information.
3. Information acquired or received by LA-SAFE or accessed from other sources is analyzed according to priorities and needs and will be analyzed to:
   - Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
   - 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.

   LA-SAFE requires all analytical products to be reviewed and approved by the privacy oversight committee to ensure they provide appropriate privacy, civil rights, and civil liberties protections before dissemination or sharing by the center.

I. MERGING RECORDS

1. Information will be merged only by qualified individuals who have successfully completed a background check and possess the appropriate security clearance, if applicable, and have been selected, approved, and trained accordingly.
2. The set of identifying information sufficient to allow merging by LA-SAFE may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as

DNA, retinal scan, or facial recognition. When combined, the identifiers or characteristics that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

J. SHARING AND DISCLOSURE

1. Authorized persons:

    - For purposes of this policy, authorized persons are assigned to LA-SAFE or other government 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.
    - Authorized users may disseminate LA-SAFE data to authorized persons as defined in this section only per the dissemination rules of this policy.

2. Authorized users

    - For purposes of this policy, authorized users are assigned to LA-SAFE, commissioned police officers, and other criminal justice administrative personnel, who:
        - Are approved for LA-SAFE access by the LSP; and
        - Meet, at a minimum, the certification requirements for LA-SAFE access; and
        - Undergo training regarding the system's capabilities and the appropriate use and sharing of data accessed through LA-SAFE.

3. The data maintained by LA-SAFE is obtained through participating stakeholder agencies, federal agencies, and open-source resources. Individual users of the center's information are solely responsible for the interpretation, further dissemination, and use of information developed in the research process. Additionally, the user's accountable for ensuring the accuracy, validity, and completeness of all intelligence information obtained before official action is taken in whole or in part.

4. Credentialed, role-based access criteria will be used by LA-SAFE, as appropriate, to control:

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

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

6. Access to or disclosure of records retained by LA-SAFE 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 identify individuals who access information retained by the center and the nature of the information accessed will be kept by the center.

7. Agencies external to LA-SAFE may only share information accessed or disseminated from the center with approval from the center or other originators of the information.

8. Records retained by LA-SAFE may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public security, public safety, or public health purposes and only in the performance of official duties under applicable laws and procedures. An audit trail sufficient to identify each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

9. Information gathered or collected and records retained by LA-SAFE 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 and the Louisiana State Police for this type of information or when there is a legitimate need. All requests will be forwarded to the Department of Public Safety Legal Section for review and compliance. The Legal Section will send an acknowledgment letter to the requestor within three days of receipt of the written request stating that their request has been received and they will receive a response to their request within 30 days. LA-SAFE shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive it. An audit trail will be kept of all requests and of what information is disclosed to a member of the public.

10. The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the center or originating agency. The individual will also be informed of the procedure for appeal when the center or originating agency has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

11. Information gathered or collected and records retained by LA-SAFE will not be:

    - Sold, published, exchanged, or disclosed for commercial purposes;
    - 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 authorized explicitly by the originating agency; or
    - Disseminated to persons not authorized to access or use the information.

12. Several categories of records that will ordinarily not be provided to the public:

    - Records required to be kept confidential by law are exempted from disclosure requirements under **LRS 44:3.**
    - 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.
    - Investigatory records of law enforcement agencies exempted from disclosure requirements under **LRS 44:3**. However, certain law enforcement records must be made available for inspection and copying under **LRS 44:31**.
    - 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 a terrorist attack is exempted from disclosure requirements under **LRS 44:3**. By way of example, this *may include* a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under **LRS 14:128.1**, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

- A record, or part of a record that constitutes trade secrets or information that is commercial, financial, or otherwise subject to a nondisclosure agreement obtained from a person and is privileged and confidential **LRS 44:3.2 and LRS 51:710.2.**

13. LA-SAFE 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

K.1 DISCLOSURE

LA-SAFE and participating agencies intend to be open with the public concerning data collection practices when such openness does not jeopardize ongoing criminal investigative activities. LA-SAFE and its participating agencies will refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality when this can be done without compromising an active inquiry or investigation. All freedom of information act (FOIA) requests are sent to the Louisiana State Police Legal Affairs Section for review and processing. LA-SAFE does not directly respond to any request for information.

1. The existence, content, and source of the information will not be made available to an individual when LRS 44.3 and LRS 44.3.1 applies or any of the following:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
   - Disclosure would endanger the health or safety of an individual, organization, or community.
   - The information is in a criminal intelligence information system subject to 28 CFR Part 23.
   - The information relates to LRS 44.3.1.
   - The information source does not reside with the center.
   - LA-SAFE did not originate or has no right to disclose the information.
   - Other authorized basis for denial.
2. Research of LA-SAFE's data sources is limited to individuals selected, approved, and trained accordingly. Access to the information within the center will be granted only to fully authorized personnel screened with state and national fingerprint-based background checks and any additional background standards established by the LA-SAFE Privacy Oversight Committee with the approval of the Deputy Secretary of Public Safety.
3. LA-SAFE's privacy policy will be posted at LA-SAFE.org for public review and will be made available upon request.

K.2 CORRECTIONS

1. If an individual has complaints or objections to the accuracy or completeness of information about them originating with LA-SAFE, LA-SAFE will inform the individual to submit a written request of the complaint or request correction along with documentation. The Information Security Officer will record of all complaints and requests for corrections and the resulting action, if any.
2. If an individual has complaints or objections to the accuracy or completeness of information about them that originates with another agency, LA-SAFE will notify the source agency of the complaint or request for correction and coordinate with the source agency to ensure that the individual is provided with applicable complaint submission or corrections procedures. A record will be kept of all such complaints and requests for corrections and the resulting action taken, if any, by the Information Security Officer.

3. If an individual has complaints or objections to the accuracy or completeness of protected information that has been disclosed to them that is shared through the Information Sharing Environment (ISE), LA-SAFE will notify the originating ISE participating agency of the complaint or request for correction and coordinate with them to ensure the individual is provided with complaint submission or corrections procedures.

4. LA-SAFE does not directly respond to any public requests for information. All requests and responses are processed through the Louisiana State Police Legal Affairs Section.

K.3 APPEALS

1. The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied on behalf of LA-SAFE or the originating agency. The individual will also be informed of the procedure for appeal when the LSP Legal Affairs Section or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

K.4 COMPLAINTS

1. LA-SAFE's Director will receive and forward all inquiries and complaints about privacy, civil rights, and civil liberties protection in the information system to the LSP Legal Affairs Section for review. The Director or inquiries can be forwarded to the following address: lafusion.center@la.gov.

2. The LA-SAFE Privacy Oversight Committee will be advised of the complaint and will notify the LSP Legal Affairs Section. No personnel from LA-SAFE will confirm or deny the existence or nonexistence of the information to the complainant unless otherwise required by law. The LSP Legal Affairs Section will handle all notifications and responses from that point forward. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency in correcting any identified data/record deficiencies, purging the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed by Legal and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. The center will not share information until the complaint has been resolved or Legal advises or directs. The Privacy Officer will keep a record at the center of all complaints and the resulting action taken in response to the complaint.

L. SECURITY SAFEGUARDS

1. LA-SAFE is committed to protecting privacy and maintaining the integrity and security of personal information. LA-SAFE and the Department of Public Safety, Office of Technology Services, shall be responsible for implementing the following security requirements for its intelligence systems.

2. Firewalls are in place to prevent unauthorized agencies or entities from accessing LA-SAFE resources.

3. LA-SAFE utilizes various levels of Role-Based User Access.

    - Each user's role shall determine the types of information accessible to the user.
    - Each user's role contains specific permissions to modify or delete records.

- Security Breach and Notifications – LA-SAFE and the Department of Public Safety, Office of Technology Services, will monitor and respond to security breaches or breach attempts.
    - If LA-SAFE personnel become aware of a breach of the security of unencrypted personal information, LA-SAFE will notify any individual whose personal information was or is believed to have been obtained by an unauthorized person and access to which threatens the physical or financial harm to the person.
    - Any necessary notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and if necessary, to reasonably restore the integrity of any information system affected by this release.
- Physical Safeguards – LA-SAFE systems shall be located in a physically secured area restricted to designated authorized personnel.
    - Only designated, authorized personnel will have access to information stored in LA-SAFE data systems.
    - Regardless of agency, all authorized visitors must register with designated authorized personnel before gaining admission to the facility.
    - Designated authorized personnel will escort all authorized registered visitors.
- The LA-SAFE Director, or his designee, will identify technical resources to establish a secure facility for center operations with restricted electronic access and alarm systems to guard against external breaches of the facility. In addition, the LA-SAFE Director, or his designee, will identify technological support to develop certain internal and external safeguards against network intrusion of the center's data systems. Access to the center's databases from outside the facility will only be allowed over secure network lines.
- Disaster Recovery – The Department of Public Safety, Office of Technology Services, has appropriate disaster recovery procedures for LA-SAFE data outlined in their Information and Technology Command Disaster Recovery Plan.
- Information Security Officers – Federal agencies housed at LA-SAFE each have a dedicated information security officer. The Department of Public Safety, Office of Technology Services, will be the Information Security Officer for LA-SAFE. They shall be trained to handle network access/security.
- LA-SAFE will secure tips, leads, and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

M. INFORMATION RETENTION AND DESTRUCTION

1. All applicable information will be reviewed for record retention (validation or purge) every five years, as provided by 28 CFR Part 23. Misleading, obsolete, or otherwise unreliable information will be purged, destroyed, deleted, or returned to the submitting source. Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time. Notification of proposed destruction or return of records may or may not be provided to the contributor, depending on the relevance of the information and any agreement with the providing agency.

2. Criminal intelligence information and requests for information will be deleted (purged) from the RMS periodically if no updated criminal activity has been documented after holding the information for five years.

3. Each entry into the RMS will be evaluated on its content and may be retained if it is the supervisor's opinion that retention of the information serves a valid law enforcement purpose and the information has been updated to comply with the retention schedule.

4. A record of information to be reviewed for retention will be maintained by the Department of Public Safety's Information Technology Section. Before purging intelligence information, an electronic copy of the information will be sent to the originating unit supervisor 90 days before purging, advising that the information will be purged from the RMS. If this supervisor has intelligence information indicating that the subject is currently involved in criminal activity, an updated intelligence submission will authorize LA-SAFE or the Investigative Support Section to maintain the information for an additional five years.

N. ACCOUNTABILITY AND ENFORCEMENT

N.1 ACCOUNTABILITY

1. Queries made to LA-SAFE data applications will be logged into the center's data system identifying the user initiating the query. When such information is disseminated outside the originating agency, prior approval from the originating agency shall be obtained before its release.

2. An electronic audit log is produced for all inquiries into LA-SAFE's record management system. LA-SAFE and the Department of Public Safety, Office of Technology Services will maintain an audit trail of accessed, requested or disseminated information. An audit trail will be kept for a minimum of five years of requests for access to information for specific purposes and of what information is disseminated to each person in response to a request.

3. Secondary dissemination of information can only be to a law enforcement agency for investigative purposes or to other agencies as provided by law. The agency from which the information is requested will maintain a record of any secondary dissemination of information. This record should reflect, at a minimum:

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

4. With the concurrence of the Deputy Secretary of Public Safety, the LA-SAFE Governance Board will be responsible for conducting or coordinating internal or special audits and for investigating misuse of the center's information systems.

5. LA-SAFE will conduct an annual audit and inspection of its information to include, but not limited to, contracts, databases, and policies. In addition, an independent panel will be designated to conduct its inspections. This independent panel can conduct a random audit, without announcement, at any time and without prior notice to LA-SAFE. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the RMS.

6. LA-SAFE personnel or other authorized users shall report violations or suspected violations of center policies relating to protected information through LA-SAFE to the Deputy Secretary of Public Safety, or his designee

7. LA-SAFE will identify and review protected information that originates from the center before sharing that information through the Information Sharing Environment. Further, LA-SAFE will provide notice mechanisms, including but not limited to metadata or data field labels, that will

enable ISE-authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

8. To delineate ISE information from other data, LA-SAFE maintains records of the ISE-originating agencies the center has access to and audit logs and employs system mechanisms whereby the source is identified within the information record.
9. LA-SAFE requires certain basic descriptive information to be entered and electronically associated with data or content for which special laws, rules, or policies regarding access, use, and disclosure exist.
10. LA-SAFE's privacy officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained within this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

N.2 ENFORCEMENT

1. All confirmed or suspected violations of LA-SAFE policies will be reported through LA-SAFE to the Deputy Secretary of Public Safety or his designee. Individual users of LA-SAFE information remain responsible for appropriately using center information. Each user of the center and participating agency within LA-SAFE must abide by this Privacy Policy in disseminating information. Failure to abide by the restrictions for the use of LA-SAFE data may result in the following:
    - The suspension or termination of user privileges;
    - Suspension, demotion, transfer, or termination of center personnel, as permitted by applicable personnel policies;
    - Discipline imposed by the user's employing agency;
    - Criminal prosecution;
2. LA-SAFE reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service to any person violating the privacy policy. LA-SAFE reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of LA-SAFE's privacy policy.

O. TRAINING

1. LA-SAFE will require the following individuals to participate in training programs regarding the implementation of and adherence to the privacy, civil rights, and civil liberties policy:
    - All center personnel.
    - Participating agency personnel.
    - Personnel providing information technology services to the center.
    - Staff members in other public agencies or private contractors providing services to the center.
    - Authorized users who the center or a contractor does not employ.
2. LA-SAFE will provide special training to personnel authorized to share criminal intelligence information in the Information Sharing Environment regarding the requirements and policies for collecting, using, and disclosing criminal intelligence information.
3. The training program will address the following:
    - Purpose of this policy;

- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of criminal intelligence information and tips and leads information;
- Implementation of this policy in the day-to-day work of the user (either paper or systems user);
- Impact of policy violations upon citizens and the agency;
- Penalties for policy violations;
- Originating and participating agency responsibilities and obligations under applicable law and policy;
- Mechanisms for reporting violations of center P/CRCL protection policies and procedures;
- How to identify, report, and respond to a suspected or confirmed breach of PII;
- Updates to the P/CRCL policy, if any, in response to changes in law and implementation experience; and
- ISE Core Awareness Training, if available, at ise.gov.

Appendix A
Terms and Definitions

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

Regarding the Information Sharing Environment (ISE), access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, including 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—How an ISE participant obtains information by exercising authority; for example, through human intelligence collection or from a foreign partner. For this definition, acquisition does not refer to obtaining information widely available to other ISE participants through, for example, news reports or obtaining 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 about 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 detail each user's activity—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 to assist with information recovery in a system failure.

Authentication—Validating a person's credentials, 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 credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of usernames and passwords. See Biometrics.

Biometrics—A general term used alternatively to describe a characteristic or a process. (1) As a characteristic: a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition. (2) As a process: automated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. See Glossary, Facial Identification Scientific Working Group (FISWG), Version 1.1, February 2, 2012, https://www.fiswg.org/FISWG_Glossary_v1.1_2012_02_02.pdf.

Center—Refers to the Louisiana State Analytical & Fusion Exchange and all participating agencies of the Louisiana State Analytical & Fusion Exchange.

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 protect 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 based on 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.

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.

Credentials—Information including identification and proof of identification used to access 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 by an individual or organization reasonably suspected of involvement in illegal activity. Criminal intelligence records are maintained in a criminal intelligence system per 28 CFR Part 23.

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.

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. State law or agency policy may address the center's response to a data breach. 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.

[1] Civil Rights and Civil Liberties Protections Guidance, at 4 (August 2008), available at https://www.dni.gov/index.php/nctc-who-we-are/organization/305-about/organization/information-sharing-environment/resources/1767-privacy-civil-rights-and-civil-liberties.

[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.dni.gov/index.php/nctc-who-we-are/organization/305-about/organization/information-sharing-environment/resources/1767-privacy-civil-rights-and-civil-liberties.

- Moving such information to a computer otherwise accessible from the Internet without proper information security precautions.
- Intentional or unintentional transfer of such information to a system that is not entirely 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 Quality—Refers to various aspects of the information: the accuracy and validity of the actual data values, information structure, and database/information repository design. Traditionally, the essential 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.

Deputy Director of LA-SAFE— The Louisiana State Police (LSP) Lieutenant assigned to the Investigative Support Section whose primary responsibility is the operation of LA-SAFE, coordination of personnel, the receiving, seeking, retention, evaluation, sharing, or disclosure of information, and the enforcement of these responsibilities. The Deputy Director can be contacted at lafusion.center@la.gov. He shall be the liaison for the Information Sharing Environment (ISE).

Director of LA-SAFE—The Louisiana State Police Captain assigned to the Investigative Support Section whose primary responsibility is the operation of LA-SAFE, coordination of personnel, the receiving, seeking, retention, evaluation, sharing, or disclosure of information, and the enforcement of these responsibilities. The Director of LA-SAFE and/or his designee will serve as the trained LA-SAFE privacy officer. He can be contacted at lafusion.center@la.gov.

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

Evaluation—An assessment of the source's reliability and accuracy of the raw data.

Fair Information Practice Principles (FIPPs)—FIPPs are internationally recognized principles that inform information privacy policies within the 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 worldwide. They provide a detailed description of underlying privacy and information exchange principles and a simple framework for the legal use that needs to be done concerning privacy in integrated justice systems. Because of operational necessity, applying all principles equally may not always be possible. 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

See Appendix C for further background on the FIPPs.

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, Version 1.5.5 as "[a] collaborative effort of two or more Federal, State, local, tribal, or territorial (SLTT) government agencies that combine resources, expertise, or information to maximize 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.

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 similar entities. The information set 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 acquiring relevant identifying information.

Information—Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into three general areas: general data, including investigative information; tips and leads data (including suspicious activity reports); and criminal intelligence information.

Information 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, targeted strategic, operational, and tactical decisions.

LA-SAFE Governance Board—Comprises the heads of internal agency partners or their designated representative(s) who provide input and guidance on the center's strategic goals.

LA-SAFE's Privacy Oversight Committee—A designated group comprised of the Director, Deputy Director, Investigative Specialist Manager, Compliance Investigator, and Department of Homeland Security Intelligence Officer that protects privacy, civil rights, and civil liberties, charged with guiding the operations of LA-SAFE to the Deputy Secretary of Public Safety and responsible for approving all Standards of Operating Procedures, including LA-SAFE's privacy policy.

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.

Law Enforcement Sensitive (LES)—Information that could adversely affect ongoing investigations, create safety hazards for officers/agents, informants, or others, and/or compromise their identities. Law Enforcement Sensitive information may only be released to authorized individuals with the need and right to know with the approval of the Watch Center Supervisors, Watch Center Assistant Directors, Deputy Directors, or LA-SAFE Director.

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

Metadata—In its simplest form, metadata is information (data) about information, more specifically, about a particular aspect of the collected information. A metadata item may describe an individual 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 data stewardship, incorporating federal, state, and local retention policies. Within the SDR, hosted data enclaves extend this approach to information management and safeguarding practices by separating 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.

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

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

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, 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, alone or when combined with other information linked or linkable to a specific individual.[3]

Preoperational Planning—As defined in ISE-SAR Functional Standard, Version 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, Civil Rights, and Civil Liberties (P/CRCL) Policy—A printed, published statement articulating an organization's policy position on how it handles the PII that it maintains and uses in the normal course of business. The policy should include information relating to 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 the 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.

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

Protected Information—For the non-intelligence community, protected information is information about United States citizens and lawful permanent residents 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 have other information the U.S. government expressly determines by Executive Order, international agreement, policy, or other similar instruments should be covered.

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.

[3] For further information about the breadth of PII and how to assess 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.

- 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 commonly used to describe methods that render data unrecoverable in a storage space or to destroy data in a manner that cannot be reconstituted. There are many different strategies and techniques for data purging, 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 considers 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 is collected, received, accessed, used, disseminated, retained, and purged by or for the collecting agency or organization.

Records Management System—The case management system used by the fusion center. It is the Department's records management system for its intelligence and criminal files.

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

Requestor—The individual law enforcement officer, Fusion Liaison Officer, or agency requesting information from, or reporting an incident to, LA-SAFE; synonymous with "user."

Retention—Refer to Storage.

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 operations of law enforcement, homeland security, counterterrorism, or other lawful and authorized government activity or the roles and responsibilities of particular personnel in 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 with 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 strive to ensure the accuracy and timely availability of information for the legitimate user set and promote failure resistance in the electronic systems overall.

Source Agency—Defined in the ISE-SAR Functional Standard, Version 1.5.5, source agency refers to the agency or entity that originates the SAR (examples include a local police department, a private security firm handling security for a power plant, and a security force at a military installation). The source organization will not change throughout the life of the SAR.

Stakeholder Agencies—Those agencies participating in LA-SAFE operations, in addition to sharing and collecting information.

Storage—In a computer, storage is 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 additional in-computer storage. This is probably the most common meaning in the IT industry.
- In 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.

Concerning 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.

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

Suspicious Activity Report (SAR)—Defined in the ISE-SAR Functional Standard, Version 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 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-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 alleges or indicates 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, at most, SAR information should be viewed 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 various 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 a level of suspicion that is less than "reasonable suspicion," without further information or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of little or no use to law enforcement and being extremely valuable depending on the availability of time and resources to determine its meaning.

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

Appendix B
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, 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 constitutions.

Civil liberties protections are primarily founded in the Bill of Rights. They include the fundamental 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 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. Information sharing is enhanced when staff members know the rules through sound policies and procedures communicated through ongoing training.

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 form). Other laws may have additional 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 description to ensure that the scope of the terminology used is properly understood and implemented.

[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 website at https://www.dni.gov/index.php/nctc-who-we-are/organization/305-about/organization/information-sharing-environment/resources/1767-privacy-civil-rights-and-civil-liberties.

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 the 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 valuable 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. It requires the patient's consent except in specific emergencies,, 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 applies 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 guide law enforcement on 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. Law enforcement may make this connection (using other systems) only with a permissible purpose, 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 an identifiable form. A PIA evaluates 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 specialized agencies, such as agencies that sell information about employment history, insurance claims, check-writing histories, medical records, rental history records, and 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 §§ 164.502(a) and 164.103 [defining protected health information and use]). The Privacy Rule applies to the following covered entities: (1) a health plan, (2) a health care clearinghouse, and (3) a health care provider who transmits any health information in electronic form in connection with certain transactions (42 U.S.C. §1320d-1(a) (2003); 45 CFR § 160.102 (2003). Since the Privacy Rule applies only to a covered entity, a governmental body begins its inquiry by first determining whether it is a covered entity under the Privacy Rule (45 CFR § 160.103 (2003) [defining health plan, health care clearinghouse, health care provider]). If it is a covered entity, it then looks to the Privacy Rule for a permitted or required disclosure.

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

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

22. **National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490—**In each state, an authorized criminal justice agency of the state shall report child abuse crime information to or index child abuse crime information in the national criminal history background check system. A criminal justice agency can satisfy the requirement by reporting or indexing all

felony and serious misdemeanor arrests and dispositions. The U.S. Attorney General (AG) is required to publish an annual statistical summary of child abuse crimes. The act requires that 80 percent of final dispositions be entered in the state databases by December 1998, with steps being taken toward 100 percent entry.

A 1994 amendment required that the AG—in consultation with federal, state, and local officials, including officials responsible for criminal history record systems, and representatives of public and private care organizations and health, legal, and social welfare organizations—shall develop guidelines for the adoption of appropriate safeguards by care providers and by the state for protecting children, the elderly, and individuals with disabilities from abuse.

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 non-criminal 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 record-keeping 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,[5] 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.

1. **Louisiana Constitution Article 1, Section 5 – Right to Privacy—**Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy. No warrant shall issue without probable cause supported by oath or affirmation, and particularly describing the place to be searched, the persons or things to be seized, and the lawful purpose or reason for the search. Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court.

2. **Louisiana Constitution Article 12, Section 3 – Right to Direct Participation—**No person shall be denied the right to observe the deliberations of public bodies and examine public documents, except in cases established by law.

3. **Louisiana Revised Statute 44:1 et seq. – Public Records and Recorders—**A.(1) As used in this Chapter, the phrase "public body" means any branch, department, office, agency, board, commission, district, governing authority, political subdivision, or any committee, subcommittee, advisory board, or task force thereof, any other instrumentality of state, parish, or municipal government, including a public or quasi-public nonprofit corporation designated as an entity to perform a governmental or proprietary function, or an affiliate of a housing authority. (2)(a) All books, records, writings, accounts, letters and letter books, maps, drawings, photographs, cards, tapes, recordings, memoranda, and papers, and all copies, duplicates, photographs, including

[5] The confidentiality requirements established by VAWA are unaffected by a lapse in programmatic funding for VAWA.

microfilm, or other reproductions thereof, or any other documentary materials, regardless of physical form or characteristics, including information contained in electronic data processing equipment, having been used, being in use, or prepared, possessed, or retained for use in the conduct, transaction, or performance of any business, transaction, work, duty, or function which was conducted, transacted, or performed by or under the authority of the constitution or laws of this state, or by or under the authority of any ordinance, regulation, mandate, or order of any public body or concerning the receipt or payment of any money received or paid by or under the authority of the constitution or the laws of this state, are "public records", except as otherwise provided in this Chapter or the Constitution of Louisiana. (b) Notwithstanding Subparagraph (a) of this Paragraph, any documentary material of a security feature of a public body's electronic data processing system, information technology system, telecommunications network, or electronic security system, including hardware or software security, password, or security procedure, process, configuration, software, and code is not a "public record". (c) Notwithstanding Subparagraph (a) of this Paragraph, any blueprint or floor plan of the interior of a public school building or facility is not a "public record". (3) As used in this Chapter, the word "custodian" means the public official or head of any public body having custody or control of a public record, or a representative specifically authorized by him to respond to requests to inspect any such public records. B.(1) Electrical well surveys produced from wells drilled in search of oil and gas located in established units and which are filed with the assistant secretary of the office of conservation shall be placed in the open files of the office of conservation. Any party or firm shall have the right to examine or reproduce, or both, at their own expense, copies of said survey, by photography or other means not injurious to said records. All other electric logs and other electronic surveys, other than seismic data, produced from wells drilled in search of oil and gas which are filed with the assistant secretary of the office of conservation shall remain confidential upon the request of the owner so filing for periods as follows: (2) For wells shallower than fifteen thousand feet a period of one year, plus one additional year when evidence is submitted to the assistant secretary of the office of conservation that the owner of the log has a leasehold interest in the general area in which the well was drilled and the log produced; for wells fifteen thousand feet deep or deeper, a period of two years, plus two additional years when evidence is submitted to the assistant secretary of the office of conservation that the owner of the log has such an interest in the general area in which the well was drilled and the log produced; and for wells drilled in the offshore area, subsequent to July 1, 1977, regardless of depth, a period of two years from the filing of the log with the office of conservation, plus two additional years where evidence is submitted to the assistant secretary of the office of conservation that the owner of the log has such an interest in the general area in which the well was drilled and the log produced and has immediate plans to develop the said general area, unless a shorter period of confidentiality is specifically provided in the existing lease. (3) At the expiration of time in which any log or electronic surveys, other than seismic data, shall be held as confidential by the assistant secretary of the office of conservation as provided for above, said log or logs shall be placed in the open files of the office of conservation and any party or firm shall have the right to examine or reproduce, or both, at their own expense, copies of said log or electronic survey, other than seismic data, by photography or other means not injurious to said records. *Amended by Acts 1973, No. 135, §1; Acts 1973, Ex.Sess., No. 4, §1; Acts 1978, No. 686, §1; Acts 1979, No. 691, §1; Acts 1980, No. 248, §1; Acts 2001, No. 707, §1, eff. June 25, 2001; Acts 2001, No. 882, §1; Acts 2011, No. 79, §2; Acts 2020, No. 211, §2, eff. June 11, 2020. NOTE: See Acts 2011, No. 79, §3, re applicability of provisions concerning affiliates of housing authorities.*

4. **Louisiana Revised Statute 44.3 – Public Records and Recorders – Records of prosecutive, investigative, and law enforcement agencies, and communications districts—**Records of prosecutive, investigative, and law enforcement agencies, and communications districts. A. Nothing in this Chapter shall be construed to require disclosures of records, or the information contained therein, held by the offices of the attorney general, district attorneys, sheriffs, police departments, Department of Public Safety and Corrections, marshals, investigators, public health investigators, correctional agencies, communications districts, intelligence agencies, or publicly owned water districts of the state, which records are: (1) Records pertaining to pending criminal litigation or any criminal litigation which can be reasonably anticipated, until such litigation has been finally adjudicated or otherwise settled, except as otherwise provided in Subsection F of this Section; or (2) Records containing the identity of a confidential source of information or records which would tend to reveal the identity of a confidential source of information; or (3) Records containing security procedures, investigative training information or aids, investigative techniques, investigative technical equipment or instructions on the use thereof, criminal intelligence information pertaining to terrorist-related activity, or threat or vulnerability assessments collected or obtained in the prevention of terrorist-related activity, including but not limited to physical security information, proprietary information, operational plans, and the analysis of such information, or internal security information; or (4)(a) The records of the arrest of a person, other than the report of the officer or officers investigating a complaint, until a final judgment of conviction or the acceptance of a plea of guilty by a court of competent jurisdiction. However, the initial report of the officer or officers investigating a complaint, but not to apply to any followup or subsequent report or investigation, records of the booking of a person as provided in Louisiana Code of Criminal Procedure Article 228, records of the issuance of a summons or citation, and records of the filing of a bill of information shall be a public record. (b) The initial report shall set forth: (i) A narrative description of the alleged offense, including appropriate details thereof as determined by the law enforcement agency. (ii) The name and identification of each person charged with or arrested for the alleged offense. (iii) The time and date of the alleged offense. (iv) The location of the alleged offense. (v) The property involved. (vi) The vehicles involved. (vii) The names of investigating officers. (c) Nothing herein shall be construed to require the disclosure of information which would reveal undercover or intelligence operations. (d) Nothing herein shall be construed to require the disclosure of information which would reveal the identity of the victim of a sexual offense. (5) Records containing the identity of an undercover police officer or records which would tend to reveal the identity of an undercover police officer; or (6) Records concerning status offenders as defined in the Code of Juvenile Procedure. (7) Collected and maintained by the Louisiana Bureau of Criminal Identification and Information, provided that this exception shall not apply to the central registry of sex offenders maintained by the bureau. B. All records, files, documents, and communications, and information contained therein, pertaining to or tending to impart the identity of any confidential source of information of any of the state officers, agencies, or departments mentioned in Paragraph A above, shall be privileged, and no court shall order the disclosure of same except on grounds of due process or constitutional law. No officer or employee of any of the officers, agencies, or departments mentioned in Paragraph A above shall disclose said privileged information or produce said privileged records, files, documents, or communications, except on a court order as provided above or with the written consent of the chief officer of the agency or department where he is employed or in which he holds office, and to this end said officer or employee shall be immune from contempt of court and from any and all other criminal penalties for compliance with this paragraph. C. Whenever the same is necessary, judicial determination pertaining to compliance with this section or with constitutional law shall be made after a contradictory hearing as provided by law. An appeal by the state or an officer, agency, or department thereof shall be suspensive. D. Nothing in this Section shall be construed to prevent any and all prosecutive, investigative, and law enforcement agencies and communications districts from having among themselves a free flow of information for the purpose of achieving coordinated

and effective criminal justice. E. Nothing in this Section shall be construed as forbidding the release of all or part of investigative files of fires classified as arson, incendiary, or suspicious unless, after consultation with the appropriate law enforcement agency, any sheriff, district attorney, or other law enforcement agency directs that the records not be disclosed because of pending or anticipated criminal adjudication. F. Notwithstanding any other provision of law to the contrary, after a period of ten years has lapsed from the date of death of a person by other than natural causes, and upon approval by the district court having jurisdiction over any criminal prosecution which may result due to the death of such person, any prosecutive, investigative, and other law enforcement agency, or any other governmental agency in possession of investigative files or evidence or potential evidence, or any other record, document, or item relating to said death shall, upon request, provide copies of all such files, records, and documents to immediate family members of the victim and shall provide unlimited access for any and all purposes to all such evidence, potential evidence, and other items to any member of the immediate family and to any person or persons whom any member of the immediate family has designated for such purposes. The access granted shall include but not be limited to the examination, inspection, photographing, copying, testing, making impressions, and the use in any court proceeding of and conducting forensic studies on such evidence, potential evidence, and other items. For the purposes of this Subsection, the term "immediate family" shall mean the surviving spouse, children, grandchildren, and siblings of the victim. G. Nothing in this Chapter shall be construed to require disclosures of certificates of official driving records in the custody and control of the Department of Public Safety and Corrections, office of motor vehicles, except as specifically provided for in R.S. 15:521. H. Nothing in this Section shall be construed as prohibiting the release of any report resulting from a request for an investigation of an alleged violation of the crime of identity theft as defined under the provisions of R.S. 14:67.16 to the victim of such alleged crime. However, the information which shall be released to such victim shall be limited to that information required to be released under the provisions of R.S. 14:67.16(G)(2). *Amended by Acts 1972, No. 448, §1; Acts 1978, No. 313, §1; Acts 1978, No. 686, §1; Acts 1979, No. 336, §1; Acts 1983, No. 247, §1; Acts 1984, No. 945, §1; S.C.R. No. 139, 1985 R.S.; Acts 1986, No. 785, §1; Acts 1988, No. 438, §1; Acts 1990, No. 59, §§2 and 3, eff. June 26, 1990; Acts 1990, No. 218, §1, eff. July 2, 1990; Acts 1991, No. 86, §1; Acts 1995, No. 519, §1, eff. June 18, 1995; Acts 1999, No. 484, §1, eff. June 18, 1999; Acts 1999, No. 1189, §1; Acts 2002, 1st Ex. Sess., No. 128, §4; Acts 2003, No. 631, §2; Acts 2003, No. 844, §3; Acts 2003, No. 1197, §1.*

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.[6]
- 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).[7] 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 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.

[6] 5 U.S.C. § 552a.
[7] 6 U.S.C. § 142.

- 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.

Addendum A
Acronyms

CFR	Code of Federal Regulations
DOJ	U.S. Department of Justice
FIPPs	Fair Information Practice Principles
ILP	Intelligence-led policing
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISE	Information Sharing Environment
ISE-SAR EE	ISE-SAR Evaluation Environment
JTTFs	Joint Terrorism Task Forces
NCISP	*National Criminal Intelligence Sharing Plan*
NSI	Nationwide Suspicious Activity Reporting (SAR) Initiative
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
P/CRCL	Privacy, civil rights, and civil liberties
PIA	Privacy Impact Assessment
PII	Personally identifiable information
PM-ISE	Program Manager for the ISE
ROSA	Real-Time Open Source Analysis
SAR	Suspicious activity reporting
SDR	SAR Data Repository
SLTT	State, local, tribal, and territorial