Privacy Policy
Version 3.3

Covers the operations of the Florida Fusion Center, participants and source agencies submitting, receiving or disseminating criminal intelligence or criminal investigative information or suspicious activity reports to the FFC.

Table of Contents

A. Intent 3
B. Background 3
C. Purpose 3
D. Policy Applicability and Legal Compliance 4
E. Membership of the FFC 4
F. Governance and Oversight 5
G. Information 5
H. Acquiring and Receiving Information 9
I. Information Quality Assurance 10
J. Collation and Analysis 11
K. Merging Records 12
L. Sharing and Disclosure 12
M. Redress 14
N. Security Safeguards 15
O. Information Retention and Destruction 16
P. Information System Transparency 16
Q. Accountability 16
R. Enforcement 17
S. Training 17
Appendix I: Terms and Definitions 19

A. Intent

The Florida Fusion Center (FFC) is committed to the responsible and legal compilation and utilization of criminal investigative, criminal intelligence information, and other information important to protecting the safety and security of the people, facilities, and resources of the State of Florida and the United States. All compilation, utilization, and dissemination of information by FFC participants and source agencies will conform to requirements of applicable state and federal laws, regulations and rules, and to the greatest extent possible be consistent with the Fair Information Practice Principles.

The intent of this policy is to ensure that the FFC protects both the security of the people of the State of Florida as well as their liberty interest. The FFC will abide by all privacy, civil rights and civil liberties guidance issued as part of the Intelligence Reform and Terrorism Prevention Act of 2004, National Fusion Center Guidelines, State and Major Urban Area Fusion Center Baseline Capabilities and the National Suspicious Activity Reporting (SAR) Initiative. All local, state, tribal and federal agencies participating with the FFC by virtue of submitting, receiving or disseminating criminal intelligence or criminal investigative information, SAR information, tips or leads via the FFC are required to adhere to the requirements of the FFC Privacy Policy.

B. Background

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) directed the establishment of an Information Sharing Environment (ISE) to improve and facilitate the sharing of terrorism information across all levels of government. Fusion centers are an outgrowth of the need to coordinate information sharing efforts across the spectrum of government and private sector entities that collect and analyze information, which could be vital to supporting law enforcement, domestic security, and public safety missions. A fusion center is a collaborative effort of two or more agencies that provide resources, expertise, and/or information with the goal of maximizing the ability to detect, prevent, apprehend and respond to criminal and terrorist activity utilizing an all crimes/all hazards approach. The FFC is located within the Florida Department of Law Enforcement's (FDLE) Office of Statewide Intelligence, located in Tallahassee, Florida, and consists of federal agencies, state multi-disciplinary partners, local law enforcement and criminal justice agencies. Information used by the FFC includes criminal intelligence information, criminal investigative information, tips and leads, and suspicious activity reports documented by local, state, tribal and federal agencies in a variety of systems to include the designated Florida statewide intelligence system.

C. Purpose

The purpose of this privacy policy is to ensure the FFC and its members comply with applicable federal, state, local and tribal laws, regulations, and policies and assist all parties in:

- Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
- Increasing public safety and domestic security while maintaining appropriate levels of transparency.
- Protecting the integrity of systems used for the observation and reporting of criminal activity and information.
- Encouraging individuals or community groups to trust and cooperate with the justice system.
- Promoting governmental legitimacy and accountability.
- Making the most effective use of publicly allocated resources to public safety agencies.

D. Policy Applicability and Legal Compliance

All FFC members, participating agency members, personnel providing information technology services to the agency, private contractors, and other authorized users will comply with this Privacy Policy, as well as any applicable laws and policies protecting privacy, civil rights, and civil liberties.

All FFC members are operating under a Memorandum of Understanding and each member is required to sign an information security agreement to participate. Information Security Agreements are written with the intent to protect sensitive information while comporting with transparency and accountability expectations codified in Florida's sunshine laws. These agreements are physically maintained in the FFC and the FDLE Office of General Counsel. All agencies providing criminal intelligence, tips and leads, or SAR information to the designated Florida statewide intelligence system are operating under Agency User Agreements and Individual User Agreements, which are physically maintained by the FDLE.

Any FFC activity pertaining to the identification and submission of information, access to, or disclosure of information will comport with this Privacy Policy. All participants and members of the FFC are required to review, acknowledge and adhere to the FFC Privacy Policy. All participants and source agencies, to include all individual users of the designated Florida statewide intelligence system are required to review and adhere to the FFC Privacy Policy. The FFC will provide a printed copy of this policy upon request to all entities participating in the FFC and will require a written acknowledgement to comply with this policy and the provisions it contains. The FFC Privacy Policy will also be posted on FFC-controlled intelligence systems. The FFC Privacy Policy is posted on the FFC public website.

The FFC has adopted internal operating policies and/or procedures, all of which will be compliant with this Policy, as well as applicable laws and regulations protecting privacy, civil rights, and civil liberties including but not limited to, the U.S. Constitution and the Florida Constitution as well as applicable state, local, and federal laws and regulations regarding privacy, civil rights, and civil liberties. The FFC will comply with all applicable public record laws pertaining to criminal intelligence and criminal investigative information.

E. Membership of the FFC

All local and state agencies participating in operations of the FFC must enter into a memorandum of understanding (MOU) with the FDLE outlining and agreeing to the terms and agreements for such participation. Each participating governmental agency will assign an Executive Board member and an Intelligence Liaison to the FFC. Members assigned to the FFC will be expected to participate in a capacity as deemed appropriate by the member's agency and will have the ability to be virtually connected to the FFC. FFC membership is restricted to designated Intelligence Liaison Officers (ILOs) and Interagency Fusion Liaisons (IFLs) from local, state, tribal, federal agencies, trusted private partners and FDLE personnel. Regional fusion centers and their employees that have been adopted as certified nodes of the FFC shall also be considered FFC members.

All FFC members must adhere to training requirements set forth by the FDLE for the FFC. These training requirements include training on 28 CFR Part 23, which will be on an annual basis as well as annual refresher training on the FFC Privacy Policy and Standard Operating Procedures.

F. Governance and Oversight

Primary responsibility for the operation of the FFC is assigned to the FDLE Special Agent in Charge of OSI and Chief of Intelligence. The FDLE Chief of Intelligence serves as the FFC Director, who is appointed internally by the FDLE. The Director of the FFC will have the responsibility for ensuring compliance by members from the FFC, as well as embedded assets from partner agencies. All FFC members are personally responsible and will be personally accountable for adhering to this policy, maintaining information standards, processes, procedures and practices. Individuals assigned to the FFC from agencies outside FDLE are also bound by an Information Security Agreement, to the extent allowable by law.

The FFC is also guided by the FDLE Office of the General Counsel and its designated Privacy Officer to assist in the enforcement of the provisions of this policy. The Privacy Officer will receive and review reports regarding alleged errors and violations of this policy and provide recommendations to the FFC Director to ensure compliance.

The FFC requires that all FFC analytical products be reviewed and approved by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties (P/CRCL) protections prior to dissemination or sharing by the center. The FFC maintains the same P/CRCL protections for pass-through information provided by other entities, and the Privacy Officer will maintain visibility on all information provided through the FFC.

G. Information

1. The FFC will seek or retain information that:
    - Constitutes a credible criminal predicate or a potential threat to public safety based on at least a reasonable suspicion standard; or
    - Demonstrates by at least a reasonable suspicion threshold that an identifiable individual or organization has committed, is committing, or is planning to commit criminal conduct or activity that presents a threat to any individual, community, or the nation; or
    - Is relevant to an active or ongoing investigation and prosecution of a suspected criminal incident; the resulting justice system response, the enforcement of sanctions, orders, or sentences by response of any such incident or response; or the prevention of crime reasonably believed likely to occur without such preventative effort; and
    - Is such that the source of the information is reasonably believed to be reliable and is verifiable and, when appropriate, the limitations on the reliability or veracity of the information is clearly stated; and
    - Is information that was collected in a fair and lawful manner.

2. The FFC will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, gender identity or sexual orientation. Information related to these factors may be retained if there is a relevance between such information and the effort to detect, anticipate, or prevent criminal activity, there is at least a reasonable suspicion that criminal activity may be upcoming or ongoing, and this information is not the sole basis for retention or indexing. When there is reasonable suspicion that a criminal nexus exists, the information concerning the criminal conduct or activity may be retained or indexed; however, it is the responsibility of the source agency or FFC members to ascertain and clearly affirm

the relationship to the key element of criminal activity prior to the retention or indexing of the information.

3. The FFC is a participant in the Information Sharing Environment (ISE) National Suspicious Activity Reporting (SAR) Initiative (NSI). SARs with a nexus to terrorism will be provided to the designated national suspicious activity reporting system by the FFC after appropriate review. The FFC will retain tips, leads, or suspicious activity reports (SARs) within the designated Florida statewide intelligence system only for the length of time necessary to determine if it has criminal intelligence value. As a general rule, SARs, tips, and leads should be reviewed and evaluated for contemporaneous value within 90 days and purged within a two year window of inactive status. In addition, FDLE may require a contributing agency to justify why any particular tip, lead, or SAR should remain in the system if it appears to FDLE that the information is no longer active or otherwise of intelligence or investigative value. Failure to satisfy FDLE's request may result in the information being unilaterally removed from the system by FDLE. Notice of any such removal will be made to the contributor.

   Suspicious activity is defined as reported or observed activity and/or behavior that, based on an officer or analyst's training and experience, is reasonably believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit (illegal) intention. Suspicious Activity Reports (SARs) are reports that record the observation and documentation of suspicious activity. SARs are meant to offer a standardized means for feeding information repositories. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the state-designated fusion center, the appropriate FDLE Regional Operations Center and Joint Terrorism Task Forces. SARs are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service. Other forms of terrorism information shared in the ISE by the FFC will be in accordance with the ISE Privacy Guidelines. Tips and leads are defined as reported or observed activity and/or behavior that, based on an officer or analyst's training and experience, is reasonably believed to be indicative of intelligence gathering or preoperational planning related to non-terrorism criminal activity. Tips and leads are distinguished from SARs due to their lack of nexus to terrorism, but are treated similarly in all other regards in this policy.

4. The FFC requires certain basic descriptive information to be entered and electronically associated with data (or content), SARs, tips and leads, and intelligence products that are to be accessed, used, and disclosed, including:
   - The name of the originating department, or source agency.
   - The date the information was collected and to the extent possible, the date its accuracy was last verified.
   - To the extent possible, data fields will indicate whether the record includes protected information, to include information about U.S. persons, lawful permanent residents or personally identifiable information (PII).
   - The title and contact information for the person to whom questions regarding the information should be directed, as well as the individual accountable for the decision to submit the information and the assurance of its conformity to FFC submission standards.
   - Any particular limitations to the use or disclosure of the information based on the classification or sensitivity of the information or other similar restrictions on access, use or disclosure, and if so the nature of those restrictions.

- To the extent possible, the source reliability and the information validity will be assessed and documented.

5. The FFC participating agency members will, upon receipt of information, to include SAR information, tips and leads, assess the information to determine its nature and purpose. Members of the FFC will assign information to categories to indicate the result of the assessment, such as:
   - Whether the information is tips and leads data, suspicious activity reports, or criminal intelligence information;
   - The nature of the source (for example, fellow criminal justice or public safety agency, anonymous tip, interview, public records, private sector);
   - The reliability of the source
     - Reliable – the source has been determined to be reliable
     - Unreliable – the reliability of the source is doubtful or has been determined to be unreliable
     - Unknown – the reliability of the source cannot be judged or has not as yet been assessed
   - The validity of the content
     - Confirmed – the information has been corroborated by a trained law enforcement analyst or officer or other reliable source
     - Doubtful – the information is of questionable credibility but cannot be discounted based on the knowledge and skills of the reviewer
     - Cannot be judged – the information cannot be confirmed at the time of review
   - Unless otherwise indicated by the source or submitting agency, source reliability is deemed to be "unknown" and content validity "cannot be judged." In such case, users must independently confirm source reliability and content validity with the source or submitting agency or through their own investigation.
   - Due diligence will be exercised by all participating agencies in determining source reliability and content validity. FFC members may reject information as failing to meet any criteria for inclusion.
   - Information determined to be unfounded will be purged from the Florida statewide intelligence system and from the designated national suspicious activity reporting system.

6. The FFC participating agency members upon receipt of designated SAR information will:
   - Review and vet the SAR information and provide the two-step assessment set forth in the NSI functional standard to determine whether the information qualifies as an ISE-SAR for contribution to the designated national suspicious activity reporting system.
   - Provide appropriate reliability and validity labels.

7. At the time a decision is made to contribute SAR information to the designated national suspicious activity reporting system, FFC members or source agency personnel will label it (by record, data set, or system of records and to the extent feasible, consistent with NSI functional standards) pursuant to applicable limitations on access and sensitivity of disclosure in order to:
   - Protect an individual's right to privacy and their respective civil rights and civil liberties;
   - Protect confidential sources and police undercover techniques and methods;
   - Not interfere with or compromise pending criminal investigations; and

- Provide any 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.

8. At the time information is retained, the date of review of such information to determine whether it should be purged or continued to be retained will be noted.
   - Records that are five years old and determined to be no longer active criminal intelligence information or active criminal investigative information will be purged in accordance with approved records retention schedules, with only statistical information being kept.
   - Tips and leads or SAR information will be reviewed within 90 days after entry to make a determination of its status. Tips and leads that are determined not to be substantiated or valid will be purged within a two-year period. FFC members will strive to purge tips and leads prior to the maximum two-year period.

9. The retention or classification of existing information will be re-evaluated whenever:
   - New information is added that has an impact on access limitations, the sensitivity of disclosure, or confidence in the information;
   - There is a change in the use of the information affecting access or disclosure limitations; or
   - Information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention.

10. FFC members are required to adhere to the following practices and procedures for the storage, access, dissemination, retention, and security of tips and leads and suspicious activity reports (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. The storage of SARs, tips and leads will be through the designated Florida statewide intelligence system.
    - Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination method 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).
    - 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 criminal intelligence information when credible information indicates potential imminent danger to life or property.
    - Retain information long enough to work a tip or lead to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, meets reasonable suspicion/risen to criminal intelligence) so that an authorized user knows that status and purpose for the retention and will retain the information based upon the retention period associated with the disposition label.
    - Adhere to and follow the FFC's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SARs 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.
    - Routinely and regularly review information to determine if it should be purged.

11. The FFC will maintain a record of all formal requests for information (RFIs) to which it responds from other criminal justice or public safety agencies that are participating FFC members, other fusion centers, and criminal justice agencies. The initial request along with the completed responses to these RFIs will be documented in the FDLE case management system. Requests by the FFC to other entities will also be documented in the FDLE case management system.

H. Acquiring and Receiving Information

1. Information gathering and investigative techniques used by the FFC, affiliated agencies and all personnel assigned to the FFC will comply and adhere to the following regulations and guidelines:
   - The FFC will follow 28 CFR Part 23 with regard to the collection and retention of criminal intelligence information.
   - The FFC will adhere to criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
   - The FFC will adhere to all obligations of law, including Florida's public records laws, as well as any regulations that apply to multi-jurisdictional intelligence databases.

2. Regardless of the criminal activity involved, no information which a user has reason to believe may have been obtained in violation of law shall be used or retained by the FFC unless and until its legality can be verified. If the FFC is notified or otherwise learns that information has been obtained illegally, it will be immediately purged, absent a need to retain the information for an accountability review.

3. Agencies that participate in the FFC and which provide information to the FFC are governed by state and local laws and rules governing them, as well as by applicable federal laws. The FFC will not knowingly contract with commercial database entities that demonstrate that they gather personally identifiable information out of compliance with local, state, tribal, territorial, and federal laws, or which is based on misleading information collection practices.

4. The FFC will not directly or indirectly receive, seek, accept, or retain information from any individual or provider if the FFC knows or has reason to believe that the individual or information provider is legally prohibited from obtaining or disclosing the information, or if the FFC has reason to believe that the source used prohibited means to gather the information.

5. FFC members who acquire SAR information that may be shared with the FFC should be trained to recognize behavior that is indicative of criminal activity related to terrorism. The FFC will ensure all members receive annual SAR refresher training.

6. When a choice of investigative techniques is available, information documented as a SAR, tip, or lead should be acquired or investigated using the least intrusive feasible means, taking into account such factors as the effect on individuals' privacy and potential damage to reputation. The Florida Department of Law Enforcement adheres to investigative and operational practices that meet all Commission on Accreditation for Law Enforcement Agencies (CALEA) standards and which are memorialized in an FDLE Procedures Manual. These practices reflect the need to balance privacy, civil rights, and civil liberties with law enforcement investigative operations.

7. Access to and use of ISE-SAR information will comply with all relevant laws and regulations including those derived from the U.S. Constitution, the Florida Constitution, applicable federal and state laws and local ordinances, and the Office of the Program Manager for the Information Sharing Environment (PM-ISE) policy guidance applicable to the ISE-SAR initiative.

I. Information Quality Assurance

1. To the extent possible, the FFC will implement the "Fair Information Practice Principles" as detailed by the Department of Justice's Global Initiative, recognizing that some of the practices (such as allowing individuals about whom information is retained to review the information for accuracy) may apply, at best, in a restricted fashion to an intelligence-gathering enterprise. All contributors of information to the FFC should be familiar with the Global "Fair Information Practice Principles" and will apply those practices to the best extent practicable to the information gathered, retained, reported to, and disseminated from the FFC.

2. The FFC will make every reasonable effort to ensure that information sought, retained, or disseminated to include ISE-SAR information, tips and leads, and intelligence products is derived from dependable and trustworthy sources of information; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met.

3. State, Local, Tribal, and Territorial (SLTT) agencies, including agencies participating in the FFC, are primarily responsible for the quality and accuracy of the data accessed by, or shared with the FFC, to include SAR data. At the time of sharing, intelligence information will be labeled according to the level of confidence in the information to the maximum extent feasible. The labeling of intelligence information will be periodically evaluated and updated when new information is acquired that has an impact on confidence in the information.

4. Information provided through the designated Florida Statewide Intelligence system by the FFC is not designed to provide users with information upon which official actions may be taken. The mere existence of records in the Florida statewide intelligence system or provided by the FFC should not be used to provide or establish probable cause for an arrest, be documented in an affidavit for a search warrant or serve as documentation in court proceedings. The source agency should be contacted to obtain and verify the facts needed for any official action.

5. When the FFC receives or acquires new information relevant to an existing FDLE or FFC intelligence product, SAR record, tip or lead, FFC members will evaluate whether said information has a bearing on the records current labeling. This review will include an evaluation of the following data/record factors:
    - Accuracy
    - Currency
    - Reliability
    - Validity

If this review indicates that there is a reasonable belief that the rights of an individual may have been violated, the FFC will notify the original agency and may, as appropriate, notify the affected individual.

6. The FFC will notify participating agencies when a review of FFC products indicates that information provided by the FFC may be inaccurate, incomplete, incorrectly merged, or cannot be verified. Any needed corrections to or deletions made to SAR information will be made to such information in the designated national suspicious activity reporting system.

7. Intelligence information, ISE-SAR information, tips and leads will be removed or requested to be removed from the applicable reporting system or database if it is determined the source agency did not have the authority to acquire the original information, used prohibited means to acquire it, or did not have the authority to provide it to the FFC or the relevant system. Information subject to an expungement order in state or federal court that is enforceable under state law or policy will also be removed from the designated Florida statewide intelligence system and the designated national suspicious activity reporting system.

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

9. The FFC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared. These safeguards are intended to ensure that information that could violate civil rights and civil liberties will not be intentionally or inadvertently gathered, documented, processed, and shared.

10. If FFC personnel believe that a SAR may meet the basic threshold for sufficiency, the FFC will seek additional fact development during the vetting process where a SAR includes PII and is based on behaviors that are not inherently criminal. The FFC 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.

J. Collation and Analysis

1. Information acquired by the FFC, to include ISE-SAR information, or accessed from other sources will only be analyzed by qualified individuals who have successfully completed a background check, and if applicable obtained an appropriate security clearance, and have been selected, approved, and trained accordingly. Individuals from participating FFC agencies must sign and adhere to this Privacy Policy and a non-disclosure agreement.

2. Information acquired by the FFC or accessed from other sources is analyzed according to priorities and needs and will only be analyzed to:
   - Further crime/terrorism prevention, enforcement, force deployment, or prosecution objectives and priorities established by the FFC, and

- 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 activities, including criminal solicitations, criminal conspiracies, and/or attempts to obstruct justice.

K. Merging Records

1. Records about an individual or organization from two or more sources will not be merged unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to higher accuracy of match.

2. Sufficient identifying information 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.

   The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same subject organization may include the name, federal or state tax ID number, office address, and telephone number. The reality that identities can be stolen by those who perpetrate crimes makes the verification of factors in support of merging of records particularly important. Innocent individuals' identities may be utilized by criminals and merging of an innocent individual's information into records related to the criminal without explanation or other appropriate safeguards against misinterpretation of the information should not occur.

3. 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 and a reminder that identity theft may be the reason there has been the partial match.

L. Sharing and Disclosure

1. Credentialed security access will be utilized to control:
   - To what information a class of users can have access;
   - To what information a class of users can add, change, delete, or print; and
   - To whom the information can be disclosed and under what circumstances.

2. Personally identifiable information (PII) (such as social security numbers) will be removed from disseminated products as appropriate.

3. Agencies contributing information to the FFC will indicate at the time of submission the intent to have said information disseminated by FFC to other appropriate fusion or criminal justice, or public safety partners. In the absence of a request for additional dissemination, the FFC will operate according to the Third Agency Rule unless otherwise instructed by law,

rule or Memorandum of Understanding; therefore, FFC participating agencies may not unilaterally disseminate information received from FFC without approval from the originator of the information. There is a presumption that all records contributed to the designated Florida statewide intelligence system and the designated national suspicious activity reporting system are intended to be shared with other agencies participating in said systems.

4. Florida has broad public record laws that may require disclosure in contravention to an originating agency's wishes. However, the FFC considers it a best practice to reach out to the originating agency prior to releasing information as part of a public records request.

5. Records retained by the FFC may be accessed or disseminated *to those responsible for law enforcement, public health and safety protection, prosecutions, or criminal justice purposes derived from criminal investigations or prosecutions* only for such purposes and then only in the performance of official duties in accordance with applicable laws, regulations, and procedures. Records will be kept of access by or dissemination of information to such persons in the event an audit is required. Information gathered and records retained by the FFC may be accessed or disseminated *for specific purposes* upon request by persons authorized by law to have such access and only for those users or purposes specified by law.

6. As long as information constitutes active criminal investigative or active criminal intelligence information, or is otherwise within the scope of an applicable exemption or confidentiality provision of Florida law, information gathered and records retained by the FFC, to include intelligence or investigative information, ISE-SAR information, tips and leads, and those records within the designated Florida Statewide intelligence system, will not be released to the public. Such information shared by the FFC may be disclosed to a member of the public only if the information is defined by law to be public record, or otherwise appropriate for release to further the FFC mission, and is not exempt or prohibited from disclosure by law.

7. The FFC shall not confirm the existence or nonexistence of information, to include the designated Florida statewide intelligence system records or ISE-SAR information to any person or agency that would not be eligible to receive the information itself. ISE-SAR information will not be provided to the public if, pursuant to applicable law, it is:
   - Required to be kept confidential or exempt from disclosure.
   - Classified as active criminal investigative or intelligence information and exempt from disclosure.
   - Protected federal, state, or tribal records originated and controlled by the source agency that cannot be shared without permission.

8. Information that is no longer active criminal investigative or active criminal intelligence information will be promptly purged in a manner consistent with Florida law.

9. Information gathered and records retained by the FFC will not be sold, published, exchanged, or disclosed for commercial purposes. It will not be disclosed or published without prior notice to the contributing agency. Information will not be disseminated to unauthorized persons.

M. Redress

1. Information that is retained by the FFC is considered active intelligence or criminal investigative information and, therefore, is exempt from public disclosure. If an individual wants to review information that has been documented in an intelligence file or system or as part of an investigative case management system, a formal public records request must be made via the Florida Department of Law Enforcement. Records of public records requests made to FDLE are maintained by the Office of the General Counsel.

2. The existence, content, and source of the information will not be made available to an individual when there is legal basis for denial. To the extent allowed by law, information will not be verified or released if:
   - the disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution;
   - the disclosure would endanger the health or safety of an individual, organization, or community; or
   - the information is in a criminal intelligence system.

3. If FDLE is not the original source of the information about which the public records request has been made, the original source agency will be contacted by FDLE for appropriate response to said request. If a public records request was made through the Florida Department of Law Enforcement (FDLE) and the decision was made to release information, any complaints or objections to the accuracy or completeness of information retained about him or her should be made in writing and handled through the FFC Privacy Officer. The individual would be required to provide a written request to modify the documentation, remove the record and provide adequate reasoning for the request. The information would then be submitted to the Florida Department of Law Enforcement for consideration.

4. The individual to whom information has been disclosed will be provided with a justification and the opportunity for an appeal if the request for correction is denied by the FFC. Upon denial, the individual will be informed of the methods for correcting or modifying the information, if available. All appeals with be handled by the Florida Department of Law Enforcement, Office of General Counsel in consultation with the Office of Inspector General. A record will be kept of all requests and of what information is disclosed to an individual.

5. If an individual has complaints or objections to the accuracy or completeness of ISE-SAR information resulting in specific, demonstrable harm to said individual, and that such information about him or her is alleged to be held by the FFC, the FFC**,** must inform the individual how to submit complaints or request corrections. A record will be kept of all complaints and requests for corrections and the resulting action, if any. Should it be deemed appropriate, FDLE and the FFC will assist the originating agency upon request in correcting, purging or clarifying any identified data/record deficiencies identified in the public records request.

6. The FFC will acknowledge the complaint and state that it will be reviewed, but will not confirm the existence of any ISE-SAR or information provided to the ISE that contains information in privacy fields that identifies the individual. However, any personal information will be reviewed and corrected or deleted if the information is determined to be erroneous, includes incorrectly merged information, or is out of date.

7. The designated Assistant General Counsel from the FDLE Office of General Counsel serves as the FFC Privacy Officer. The Director of OSI and the Chief of Intelligence will assist the Privacy Officer in determining whether complaints involve information that has been submitted to the ISE or is otherwise in the possession of the FFC. A written record of complaints including information which has been provided to the ISE will be maintained by the Director of OSI and the Chief of Intelligence and shall be made available for additional action as appropriate. The FFC will provide written notice to receiving ISE entities of information it has received from the FFC that is in need of redress.

N. Security Safeguards

1. The FFC Director has designated an FDLE member to serve as the security officer who shall receive appropriate training and shall support the security needs of the FFC.

2. The FFC will operate in a secure facility, protecting it from external intrusion. The FFC will utilize secure internal and external safeguards against network intrusions, to include intelligence system records. Access to FFC databases and reporting systems from outside the facility will only be allowed over secure networks.

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

4. Access to FFC information will only be granted to FFC members whose position and job duties require such access and who have successfully completed a background check and appropriate security clearance, if applicable, and those who have been selected, approved, and trained accordingly.

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

6. The FDLE has stringent physical, procedural and technical security safeguards that govern the security of data systems administered by the FDLE and accessed by FFC and FDLE members. The following operational security issues are addressed by FDLE procedures 2.5, 2.6, 2.7, 2.8 and 2.11:
    - Confidentiality of data and information
    - Control of computers and information resources
    - Physical security and access to data processing facilities
    - Logistical and data access controls/data and system integrity
    - Network security
    - Backup and recovery
    - Personnel security and security awareness
    - Systems acquisition, auditing and reporting
    - Information technology resource standards
    - Software management and accountability
    - Password management
    - Security of mobile devices

As the FFC falls under the administration and authority of the FDLE, these procedures are applicable to and govern FFC operations. The FFC will, in the event of a data security breach,

comply with all applicable state and federal laws regarding notification to compromised individuals.

O. Information Retention and Destruction

1. All criminal intelligence information will be reviewed for record retention (validation or purge) at least every five (5) years, as required by 28 CFR Part 23. When information has no further value or meets the criteria for removal according to FDLE Policy 1.15 and the FFC retention and destruction policy, and according to applicable law, it will be purged and/or returned to the contributing agency. Each contributor is responsible for its compliance with applicable public records laws, as well as the records retention and destruction rules and guidelines of the Department of State.

2. The FFC will retain ISE-SAR information in the designated national suspicious activity reporting system for a sufficient period of time to permit the information to be validated or refuted, its credibility and value to be reassessed, and to the degree possible a "disposition" label will be assigned so that subsequent authorized users know the status and purpose for the retention.

3. All SAR information, tips, and leads contained in the designated Florida statewide intelligence system and contributed to the designated national space by the FFC will be reviewed no later than 90 days after entry to make a determination of its status. SARs, tips, and leads that are determined not to be valid will be purged from the system. SARs, tips, and leads that are unsubstantiated within a two year period will be purged from the system.

P. Information System Transparency

1. The FFC will be transparent with the public in regard to information and intelligence collection practices. The FFC's Privacy Policy will be provided to the public for review via the FDLE public website.

2. The FFC Privacy Officer will be responsible for receiving and coordinating a response to inquiries and complaints about privacy, civil rights, and civil liberties protections related to ISE-SAR information and the operations of the FFC.

Q. Accountability

1. The FFC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with their systems, in accordance with this policy and applicable law. These procedures will be incorporated into the FFC Standard Operational Procedures.

2. The FFC will have access to records of inquiries to and information disseminated from the ISE platforms.

   An audit log of queries will identify the user initiating the query. This will include periodic and random audits of logged access to the designated national suspicious activity reporting system in accordance with audit obligations within the ISE-SAR policy or as otherwise utilized by the FFC Privacy Officer.

3. Records of audits will be maintained by the FFC Privacy Officer or their designee. Any audits conducted will be in such a manner as to protect the confidentiality, sensitivity, and privacy of records and/or reports of audits, as well as any related documentation. The Director of OSI and the Chief of Intelligence will request annual audits of the criminal intelligence systems maintained and controlled by the FFC.

4. The members of the FFC may report violations or suspected violations of the Privacy Policy to the FFC Privacy Officer.

5. If an authorized user is found to have violated the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the FFC may**,** in consultation with the FDLE Office of General Counsel, the FDLE Inspector General, or the Office of Executive Investigations, as appropriate:
   - Suspend or discontinue access to information by the user;
   - Suspend, demote, transfer, or terminate the person, as permitted by applicable personnel policies;
   - Apply administrative actions or sanctions as provided by rules and regulations or as provided in agency personnel policies;
   - If the user is from an agency external to the FDLE, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions; or
   - Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

6. The FFC's Executive Advisory Board in consultation with the FFC Privacy Officer will annually review and provide guidance, as appropriate, on the provisions protecting privacy, civil rights, and civil liberties contained within this policy and provide guidance on appropriate changes in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems, and changes in public expectations.

R. Enforcement

The FFC reserves the right of access to FFC information and to suspend or withhold service to any personnel violating the Privacy Policy. The FFC reserves the right to deny access to systems, FFC products or ISE-SAR information to any participating agency or individual user who fails to comply with the applicable restrictions and limitations of the FFC Privacy Policy.

S. Training

1. All participants and source agencies submitting, receiving or disseminating criminal intelligence or criminal investigative information or suspicious activity reports to the designated Florida statewide intelligence system, will participate in training programs regarding implementation of and adherence to privacy, civil rights and civil liberties policies and protections pertinent to the scope of their employment and access to said information.

2. FFC members must attend privacy training as determined by the Director of OSI and the Chief of Intelligence.

3. The Privacy Policy will be posted on the FDLE public website for review. All FFC members, are required to attend training regarding privacy, civil rights and liberties as determined by the FFC Executive Advisory Board and the Director of OSI and the Chief of Intelligence. These trainings will include the following:
    - Purpose of the Privacy Policy
    - Substance and intent of the provisions of the policy relating to the collection, use, analysis, retention, destruction, sharing and disclosure of SAR and ISE-SAR information
    - How to implement the policy in the day-to-day work of a participating agency
    - The impact of improper activities associated with violations of the policy
    - Mechanisms for reporting violations of the policy
    - The possible penalties for policy violations, to include criminal liability.

Appendix I

Terms and Definitions

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. For data access, access is usually specified as read-only access and read/write access.

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

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

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

Agency/Center—Agency/Center refers to the FFC and all participating local, state or federal agencies of the FFC.

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

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

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

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

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

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

Civil Rights—The term "civil rights" is used to imply that the state (or government) has a role in ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments to the Constitution and by acts of Congress.

Computer Security—Protection of information assets through the use of technology, processes, and training.

Confidentiality—Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials—Information that includes identification and proof of identification that is utilized by FFC members to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates. Credentialed security access will be utilized to control:

- What information a class of users can have access to;
- What information a class of users can add, change, delete, or print; and
- To whom the information can be disclosed and under what circumstances.

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

Data—Elements of information, inert symbols, signs or measures.

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

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

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

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

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

Executive Advisory Board—Comprised of one or more representatives from each of the participating agencies and chaired the Director of the Florida Department of Law Enforcement's Office of Statewide Intelligence or their designee. The FFC Executive Advisory Board will serve in an advisory capacity only.

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

1. Define agency purposes for information to help ensure agency uses of information are appropriate. ("Purpose Specification Principle")

2. Limit the collection of personal information to that required for the purposes intended. ("Collection Limitation Principle")

3. Ensure data accuracy. ("Data Quality Principle")

4. Ensure appropriate limits on agency use of personal information. ("Use Limitation Principle")

5. Maintain effective security over personal information. ("Security Safeguards Principle")

6. Promote a general policy of openness about agency practices and policies regarding personal information. ("Openness Principle")

7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. ("Individual Participation Principle")

8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. ("Accountability Principle")

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

Fusion Center—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

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

Homeland Security Advisor—Coordinates the efforts of the department in the ongoing assessment of this state's vulnerability to, and ability to detect, prevent, prepare for, respond to, and recover from acts of terrorism within or affecting this state. Appointed by the Commissioner of Law Enforcement to represent the State of Florida on issues involving the security of the State of Florida.

Homeland Security Information—As defined in Section 482(f)(1) of the Homeland Security Act, homeland security information means any information possessed by a federal, state, local, or tribal agency that relates to (A) a threat of terrorist activity; (B) the ability to prevent, interdict, or disrupt terrorist activity; (C) the identification or investigation of a suspected terrorist or terrorist organization or any person, group, or entity associated with or assisting a suspected terrorist or terrorist organization; or (D) a planned or actual response to a terrorist act.

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

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, tips and leads data, and criminal intelligence data.

Information Quality—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy, completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Intelligence Products—Reports or documents that contain assessments, forecasts, associations, links, and other outcomes of the analytic process that may be disseminated for use by law enforcement agencies for the prevention of crimes, target hardening, apprehension of offenders, and prosecution.

Invasion of Privacy—Invasion of privacy can be defined as intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts

one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Information Sharing Environment (ISE)—An approach that facilitates the sharing of terrorism information, which approach may include any methods determined necessary and appropriate for carrying out this section [1016]. [IRTPA 1016(a)(2)]. The ISE is to provide and facilitate the means for sharing terrorism information among all appropriate Federal, State, local, and tribal entities, and the private sector through the use of policy guidelines and technologies. [Extracted from IRTPA 1016(b)(2)]

ISE-SAR—A suspicious activity report that has been determined, pursuant to a two-part process, to have a potential terrorism nexus. ISE-SAR business rules will serve as a unifying process to support the reporting, tracking, processing, storage, and retrieval of terrorism-related suspicious activity reports across the ISE.

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

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

Law Enforcement Intelligence—The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution, project crime trends, or support informed decision making by management.

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

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

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

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

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

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).
- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

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

Privacy Policy—A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, and access. The purpose of the privacy policy is to articulate that the agency will adhere to those legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

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

Protected Information—Protected information is information about United States citizens and lawful permanent residents that is subject to information privacy or other legal protections under

the Constitution and laws of the United States. For state, local, and tribal governments, it would include applicable state and tribal constitutions and State, Local and Tribal laws, ordinances, and codes. For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument.

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

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

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

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

Retention—Refer to "Storage."

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in a person's activities.

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

Security—Security refers to the range of administrative, technical, and physical mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Designated national suspicious activity reporting system—A networked data and information repository which is under the control of submitting agencies and which provides terrorism-related information, applications, and services to other ISE participants.

SLTT—State, Local, Tribal, and Territorial.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the IT industry than meaning 2.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in"

devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism related information, to include 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.

Source Agency—The agency or entity that originates SAR information, criminal intelligence information, or criminal investigative information.

Submitting Agency—The agency or entity providing ISE-SAR information to the designated national suspicious activity reporting system.

Suspicious Activity—Reported or observed activity and/or behavior that, based on an officer's training and experience, is believed to be indicative of intelligence gathering or preoperational planning related to terrorism, criminal or other illicit/illegal intention. Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SARs)—Reports that record the observation and documentation of a suspicious activity. Suspicious activity reports (SARs) are meant to offer a standardized means for feeding information repositories. Any patterns identified during SAR analysis may be investigated in coordination with the reporting agency and the state designated fusion center. Suspicious activity reports are not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of IRTPA, all information relating to the (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism, (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations, (C) communications of or by such groups or individuals, of (D) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals. In accordance with IRTPA, as recently as amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)1) (6 U.S.C. § 482(f)1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in 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 includes intelligence information.

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

Third Agency Rule—A traditionally implied understanding among criminal justice agencies that active criminal intelligence information, which is exempt from public review, will not be disseminated without the permission of the originator.

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

A tip or lead can result from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information has some suspicion or mere suspicion attached to it, but without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information hangs between being of no use to law enforcement and being extremely valuable if time and resources are available to determine its meaning.

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

U.S. Persons—Executive Order 12333 defines "United States persons" as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

User Agency—The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE platforms, which may include analytical or operational component(s) of the submitting or authorizing agency or entity.

Vet/Vetting—A two-part process by which a trained law enforcement officer or analyst, to include Fusion Center personnel, determine the usefulness of a SAR. This process entails checking the facts reported in the SAR as well as ensuring that the SAR meets the set of requirements defined in the *ISE-SAR Functional Standards*. The first step in the vetting process is for a trained officer or analyst at a Fusion Center to determine whether suspicious activity falls within the criteria set forth in Part B – ISE SAR Criteria Guidance of the *ISE-SAR Functional Standard*. These criteria describe behaviors and incidents identified by law enforcement officials and counterterrorism experts from across the country as being indicative of criminal activity associated with terrorism. The second step in the vetting process is for a trained expert to determine, based on a combination of knowledge, experience, available information, and personal judgment whether the information has a potential nexus to terrorism.