Central Florida Intelligence Exchange (CFIX) Privacy Policy

A. Purpose Statement

The Privacy Policy of the Central Florida Intelligence Exchange (CFIX) was developed in accordance with Federal and State Guidelines to:

- Ensure individual privacy, civil rights and civil liberties
- Increase public safety and national security while maintaining appropriate levels for operational transparency
- Protect the integrity of systems for the observation and reporting of terrorism related criminal activity and information
- Promote governmental legitimacy and accountability
- Make the most effective use of public resources allocated to public safety agencies
- Minimize the threat and risk of injury to specific individuals
- Minimize the threat and risk of injury to law enforcement and others responsible for public protection, safety or health
- Protect the integrity of criminal investigations
- Protect criminal intelligence and justice system processes and information

B. Policy Applicability and Legal Compliance

All CFIX personnel, IT personnel, private contractors and consultants, analysts and virtual partners will comply with the center's privacy policy concerning the information the center collects, receives, maintains, archives, accesses or discloses to center personnel, governmental agencies, private partners and participating criminal justice and public safety agencies. CFIX personnel are required to sign a non-disclosure agreement when their employment with or assignment to CFIX commences.

Violations of the Non-Disclosure Agreement (NDA), Memorandum of Understanding (MOU) or other dissemination infractions could result in the revocation of the individual's security clearance and/or the termination of the information sharing participation with the violating individual and/or agency.

CFIX personnel are required to review and abide by the Privacy Policy that is contained in the Standard Operating Procedures (SOPs). Additionally, participating agencies and partners shall review and comply with the Privacy Policy. The policy is posted on the Region 5 page of the Florida Fusion Center Network's SharePoint Website for employees and partners to review periodically. This privacy policy applies to all entities that participate in the Fusion Process. Signatures acknowledging receipt and agreeing to stipulations of the privacy policy will be obtained from all participating parties to include representatives of the Governance Board, Executive Steering Committee, CFIX employees and representatives from agencies participating virtually with CFIX.

CFIX internal operating policies comply with the law of the State of Florida with respect to protecting the privacy of individuals and the collection, retention and dissemination of criminal intelligence information. Article I, Section 23 of the Florida Constitution explicitly provides for the right to privacy. [1]Article I, Section 24 of the Florida Constitution, entitled "Access to public records and meetings", ensures the public's right to access records, but recognizes that certain records will be exempt from disclosure to the public. Chapter 119, Florida Statutes, entitled "Public Records", provides in § 119.071 (2)(c) that "active criminal intelligence information and active criminal investigative information" are exempt from the constitutional and statutory provisions requiring disclosure of public records. The CFIX Privacy Policy adheres to these laws[2] as well as the requirements of federal and state law applicable to the protection of privacy, civil rights, and other civil liberties.[3] Further, the CFIX Privacy Policy complies with the requirements of 28 Code of Federal Regulations (CFR) Part 23 in the primary areas of submission and entry of criminal intelligence information, security, inquiry, dissemination, and the review-and-purge process.

C. Governance and Oversight

Primary responsibility for the operation of the CFIX, its justice systems, operations, coordination of personnel, the receiving, seeking, retention, evaluation, information quality, analysis destruction, sharing or disclosure of information and the enforcement of the privacy policy is assigned to the Director of the CFIX.

The CFIX is guided by a committee of the Governance Board that liaises with the community to ensure that privacy and civil rights 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 policy in response to changes in law and implementation experience, including the results of audits and inspections.

Victor L. Chapman, a local private attorney, is appointed as the Privacy Officer overseeing the implementation of the Privacy Policy. The Privacy Officer can be contacted at: Victor Lee Chapman, Barrett, Chapman & Ruta P.A, 18 Wall Street, Orlando, Florida, 32801. Telephone number (407) 839-6227, fax number (407) 648-1190, email victor@bcrlaw.net or c/o his assistant Vick@bcrlaw.net. In the event Mr. Chapman resigns or is replaced by decision of the Governance Board, the Governance Board and the Director of CFIX shall select a person to serve as Privacy Officer. The Privacy Officer will be the point of contact for ISE complaints and conduct audits to ensure compliance with ISE Privacy Guidelines. The Privacy Officer will conduct periodic audits to ensure compliance with Federal, State and Information Sharing Environment (ISE) Privacy Guidelines. The Privacy Officer shall

[1] Right of privacy.-Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law.‖

[2] The state constitutional right to privacy is much broader in scope, embraces more privacy interests, and extends more protection to those interests than its federal counterpart.‖ *Von Eiff v. Azicri*, 720 So. 2d 510, 514 (Fla. 1998). While the U.S. Constitution is the primary authority that applies to all federal, state and local agencies, compliance with Florida's stringent constitutional privacy provisions will exceed the requirements of federal law in that regard.

3 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 Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.ise.gov.

immediately bring any issues to the CFIX Director and to the Governance Board at the next scheduled meeting for resolution.

The Privacy Officer shall be trained in and familiar with local, state and federal laws and regulations that govern privacy rights, civil rights and civil liberties, including but not limited to the provisions of the Florida Constitution, Chapter 119, Florida Statutes and 28 C.F.R. Part 23 discussed above.

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

D. Terms and Definitions – See Appendix 1.

E. Information

It is the policy of the CFIX to continually provide information collection, analysis and dissemination of intelligence products to support regional law enforcement and homeland security efforts. This information shall be utilized in conformance with privacy issues, constitutional rights, civil rights and civil liberties.

CFIX Internal Database

CFIX maintains a Criminal Intelligence Database to document cases and assessments. CFIX Privacy Policy adheres to all regulations set forth by Florida State Statute 119 and 28 CFR part 23. CFIX will afford privacy, civil rights and civil liberties protection.

CFIX will seek or retain information that:

- Is based upon reasonable suspicion that the information constitutes a credible criminal predicate or a potential threat to public safety; or
- Is based upon reasonable suspicion 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, the community or the nation; or
- Is relevant to an active or ongoing investigation and prosecution of suspected criminal incidents; 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; or
- Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), 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 not otherwise prohibited by the law, with the consent of the affected individual to share the information being clearly noted when such consent has been provided.

CFIX will retain information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity reports (SARS) only for the length of time allowed under the retention limitations established by the guidelines of 28 CFR Part 23. In

accordance with the guidelines established by the Florida Fusion Center, SARS will be reviewed and evaluated for value within 90 days and purged with a two year window of inactive status.

CFIX will not seek or retain information:

- About individuals or organizations solely on the basis of their religious, political or social views or activities, or
- 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. Information related to these factors may be retained if there is a reasonable relationship or relevance to such information and the effort to detect, anticipate or prevent criminal activity and this information is not the sole basis for retention or indexing. When there is reasonable suspicion that a criminal relationship exists, the information concerning the criminal conduct or activity may be retained or indexed; however, it is the responsibility of the source agency or CFIX personnel to ascertain and clearly affirm the relationship to the key element of criminal activity prior to the retention or indexing of the information.

CFIX requires certain basic description information to be entered and electronically associated with tips or SARS that are to be accessed, used and subject to disclosure 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
- The title and contact information for the person to who questions regarding the information should be directed and who is accountable for the decision to submit the information and assuring it is believed to otherwise conform to CFIX standards.
- Any particular limitations to the use or disclosure of the information
- The type of activity associated with the SAR (criminal, gang, terrorism)
- Location of suspicious activity
- Description of location (bank, hospital, street, etc.)
- County of suspicious activity
- Date of suspicious activity
- Summary or description of the specific suspicious activity

The CFIX applies labels to agency-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

- The information is protected information as defined by the center to include personal data on any individual [per the definitions of “protected information” and “personal data” in Appendix 1 of policy], and, to the extent expressly provided in this policy, includes organizational entities.
- The information is subject to local, state or federal law restricting access, use, or disclosure.

CFIX participating agency personnel will, upon receipt of information, assess the information to determine its nature and purpose. Members of the CFIX will assign information to categories to indicate the result of the assessment, such as:

- Whether the information is general data, tips and leads data, suspicious activity reports or criminal intelligence information
- The nature of the source (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 had not as yet been assessed
- The validity of the content
    - Confirmed – the information has been determined to be reliable
    - 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 cases, 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 source or submitting agency as well as CFIX personnel in determining source reliability and content validity. CFIX personnel may reject information as failing to meet any criteria for inclusion and return such information to the submitting party with an indication of why it was rejected.
- Information determined to be unfounded will be purged from the SharePoint Website, the CFIX Internal Intelligence Database and InSITE (if applicable).

The labeling, retention, and classification of existing information will be reevaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information or
- There is a change in the use of the information affecting access or disclosure limitations
- Information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention

CFIX maintains a record of information sought, collected and disseminated on the CFIX SharePoint website. All requests or tasks are documented and when the task is completed, the disseminated product is attached to the electronic request for storage and accessible by CFIX personnel.

Information that is retained by CFIX will be labeled to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to protect confidential sources and police undercover techniques and methods, not interfere with or compromise pending criminal investigations, protect an individual's right of privacy or his or her civil rights and civil liberties, and provide legally required protection on an 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.

Information will be appropriately disseminated according to the recipient's need to know and right to know. When required, information that is disseminated will be appropriately labeled (Law Enforcement Sensitive, For Official Use Only, Sensitive but Unclassified). Information may be re-evaluated for dissemination to a broader or limited audience. Pertinent data that needs to be disseminated outside of the law enforcement community will be sanitized and all law enforcement specific information would be removed. Labeling of documentation will be modified accordingly. All intelligence products will include the third agency rule for dissemination clearly visible on the document. Standard dissemination for CFIX documents will

be to the originator of the request and the Florida Fusion Center (per MOU). Any other dissemination will be at the discretion of the originator. Dissemination information will be logged on all products. Dissemination information shall be recorded for all intelligence products and documents that are distributed by CFIX.

InSITE – FDLE Intelligence Database

CFIX will have access to InSITE tips, SARS and cases. CFIX usually receives SARS, particularly from ILO's[4], via the CFIX SharePoint Website. Tips and SARS received via the website shall be documented in InSITE for review and possible inclusion to the shared space. Upon receipt of designated SAR information, CFIX personnel will:

- Review and vet the SAR information and provide the two-step assessment set forth in the ISE-SAR functional standard to determine whether the information qualifies as an ISE-SAR for contribution to the shared space
- Provide appropriate reliability and validity labels
- All vetted ISE-SARS provided via the InSITE system will be contributed to the shared space unless the source agency requests otherwise

Use of InSITE is regulated by the FDLE and is restricted to law enforcement officials. Background checks, credit checks and mandatory training are required prior to any individual being given access to the database. All users are given individual accounts which are password protected. Users are given access to the InSITE Modules that are pertinent to their specific job assignment. CFIX personnel are granted access to all modules and can query and enter tips, cases and gang information. Storage of the information will be handled by FDLE. Information accessed by CFIX personnel will be disseminated according to InSITE Guidelines. Entries into InSITE allow the user to determine the proper procedure for dissemination. Choices for dissemination include: Disseminate, Do Not Disseminate and Check Before Disseminating.

Information that is documented and accessible through InSITE identifies protected information via relationship codes and associations to reports or tips. All subjects must be linked to a report, tip or gang, with their association clearly stated. Any information entered into InSITE must be categorized or labeled according to its purpose to include tip class (Critical Incident, Critical Infrastructure, Cyber Crime, Financial Incident, Intelligence, Security Issue, Suspicious Incident, or Threats/Crimes against Persons). This information is provided by the entering law enforcement agency, not necessarily CFIX.

CFIX members are required to adhere to the following practices and procedures for the storage, access, dissemination, retention, and security of tips, leads and suspicious activity reports (SARs) information:

- Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been 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.

[4] Intelligence Liaison Officers

- 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 CFIX SARs will be through the InSITE 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 when credible information indicates potential imminent danger to life or property
- Retain information for up to two years 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 center'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

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

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

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

Tip or SAR information will be reviewed 90 days after entry to make a determination of its status. Tips that are determined invalid will be purged from the system. Tips that are unsubstantiated within a two year period will be reviewed to determine if the records should be purged from the system. Retention and maintenance of tips and suspicious activity documented in InSITE will be the responsibility of the FDLE. Automated messages will be sent to CFIX personnel of entries they have made into InSITE when it is time to purge or update intelligence. CFIX will notify InSITE Administrator of information that can be purged prior to the designated purge date.

At the time information is retained, the date of review of such information to determine whether it should be purged or continue to be retained will be done electronically. The retention of classification of existing information will be reevaluated whenever:

- New information is added that has an impact on access limitations or the sensitivity of disclosure of the information; or
- There is a change in the use of the information affecting access or disclosure limitations
- Information has been developed that suggests the existing information is no longer of intelligence or investigative value or otherwise no longer warrants retention

Records (cases) that are five years old and determined to be no longer active intelligence or criminal investigative information will be purged in accordance with approved records retention schedules. The time a criminal subject is incarcerated may be used to extend the purge time for the amount of time the defendant was in custody.

The System Administrator at the FDLE can conduct audits on the users and their usage of InSITE. Retention and maintenance of tips and suspicious activity documented in InSITE will be the responsibility of the FDLE. CFIX personnel that are granted access to InSITE will take the necessary precautions to ensure the database cannot be accessed by unauthorized personnel. Personnel will maintain the confidentiality of their usernames and passwords and ensure that their computers are logged off, locked or shut down when they are away from their workstations.

F. Acquiring and Receiving Information

Information gathering and investigative techniques used by CFIX and affiliated agencies shall comply and adhere to guidelines established by 28 CFR Part 23, the Department of Justice (DOJ) National Criminal Intelligence Sharing Plan (NCISP), the U.S. and Florida constitutions, and statutes and regulations that apply to multi-jurisdictional intelligence and information databases, including Chapter 119, Florida Statutes (Florida's Public Records Law). Techniques used by CFIX will be the least intrusive means necessary in the particular circumstance to gather information it is authorized to seek or retain.

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

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

CFIX personnel will review incoming information from law enforcement partners to assure compliance with guidelines that govern the information collection by CFIX. CFIX will contract only with commercial database entities that provide an assurance that they gather personally identifiable information in compliance with local, state, tribal, territorial and federal laws and which is not based on misleading information collection practices.

Regardless of the criminal activity involved, no information that a user has reason to believe may have been obtained in violation of law shall be entered into any CFIX Database. If CFIX is notified or otherwise learns that information has been obtained illegally, it will be removed.

CFIX will not directly or indirectly receive, seek, accept or retain information from:

- An individual or non-governmental information provider who may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
- An individual or information provider is legally prohibited from obtaining or disclosing information or the source used prohibited means to gather the information.

Law enforcement officers and personnel at source agencies and CFIX who acquire SAR information that may be shared with CFIX shall be trained to recognize behavior that is indicative of criminal activity related to terrorism. Training shall be provided by CFIX through the Intelligence Liaison Officer Training Program.

When a choice of investigative techniques is available, information documented as a SAR or ISE-SAR 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.

External agencies that access the CFIX'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.

Access to and use of ISE-SAR information is governed by 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 Nationwide SAR Initiative (NSI).

G. Information Quality Assurance

CFIX 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 [refer to Section I, Merging Records, or appropriate policy section] has been met.

At the time of retention in the system, information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]. Contributors will indicate the reliability of the information in their submission to CFIX. CFIX will notify the appropriate data owner in writing (to include electronic notification) if the data contributed to the fusion center, the website or the shared space is found to be inaccurate, incomplete, out of date or unverifiable. Any needed corrections to or deletions made to SAR information will be made to such information in the shared space. CFIX will accurately document sources of information on all products prior to posting or dissemination.

The CFIX 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 gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

ISE – SAR information will be removed from the shared space if it is determined the source agency did not have the authority to acquire the original SAR information, used prohibited means to acquire it, or did not have the authority to provide it to CFIX.

CFIX will investigate, in a timely manner, alleged errors and deficiencies and will correct, delete or refrain from using protected information found to be erroneous or deficient. Any discrepancies that are corrected or omitted will result in the dissemination of an updated product which will include an explanation of and reason for changes. The new product will reflect accurate, updating labeling vouching for the accuracy and reliability of the information.

State, Local and Tribal agencies, including agencies participating in the Information Sharing Environment, are responsible for the quality and accuracy of the data accessed by or shared with the center. Originating agencies providing data remain the owners of the data contributed. CFIX will advise in writing or electronically the appropriate data owner, if its data is found to be inaccurate, incomplete, out of date or unverifiable.

Information provided through the CFIX database, the SharePoint website or the shared space is not designed to provide users with information upon which official actions may be taken. The mere existence of records in InSITE or the shared space or provided by CFIX 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. Only the facts, which led to the entry of the record into the database or shared space, can be used to establish probable cause in an affidavit. The source agency should be contacted to obtain and verify the facts needed for any official action.

The CFIX will use written or 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.

H. Collation and Analysis

Information acquired by CFIX or accessed from other sources will only be analyzed by qualified individuals who have successfully completed a background check, have secured the appropriate security clearance and been selected, approved and trained accordingly.

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

CFIX will analyze incoming information according to priorities and needs. Information will be analyzed to further crime prevention (including terrorism), enforcement, force deployment, or prosecution objectives. It will also be analyzed to provide tactical and/or strategic intelligence on the existence, identification and capability of individuals and organizations suspected of having engaged in criminal (including terrorist) activities.

I. Merging Records

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. 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 identifies, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, 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 organization may include the name, federal or state tax ID number, office address and phone number.

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

J. Sharing and Disclosure

The CFIX website, CFIX database and InSITE are all controlled by granted access. Users have personal passwords to access each system and permissions for specific capabilities in each system.

The CFIX 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 (Version 1.5) for suspicious activity potentially related to terrorism.

Personal identifiable information will be removed from disseminated products as appropriate, specifically when dissemination includes non-law enforcement entities.

Access to or disclosure of records retained by CFIX will only be provided to persons within CFIX or in 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 whom the person is working. An audit trail will be kept of access by or dissemination of information to such persons. Appropriate dissemination logs will be kept in accordance with criteria specified by the program agreements. Dissemination logs will be kept electronically.

CFIX will operate according to the Third Agency Rule (definition in Section E). Participating agencies may not disseminate information received from CFIX without approval from the originator of the information.

Records retained by the CFIX may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who

accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

Information gathered or collected and records retained by the CFIX may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center, the nature of the information requested, accessed, or received, and the specific purpose will be kept for a minimum of [specify the retention period for your jurisdiction for this type of request] by the center.

Information gathered or collected and records retained by the CFIX may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

Information gathered and records retained by CFIX 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.

There are several categories of records that will ordinarily ***not be provided*** to the public under Florida State Statute 119 (Public Records) (at §119.071 (2) providing exemptions for agency investigations), exempt from disclosure under a general or special law of the State of Florida, or the Criminal Intelligence Systems Operating Policies (28 CFR Part 23):

- Records required to be kept confidential by law are exempted from disclosure requirements under Florida sunshine laws (s.286.011, F.S), Florida State Statute 119 (Public Records), and the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations, Part 23).
- Information that meets the definition of "classified information" as that term is defined in the National Security Act, Public Law 235, Section 606 and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Investigatory records of law enforcement agencies that are exempted from disclosure requirements under Florida sunshine laws (s.286.011, F.S), Florida State Statute 119 (Public Records), and the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations, Part 23).However, certain law enforcement records must be made available for inspection and copying under Florida sunshine laws (s.286.011, F.S), Florida State Statute 119 (Public Records), and the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations, Part 23).
- A record or part of a record the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack is exempted from disclosure requirements under Florida sunshine laws (s.286.011, F.S), Florida State Statute 119 (Public Records), and the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations, Part 23). This includes a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism under Florida sunshine laws (s.286.011, F.S), Florida State Statute 119 (Public Records),

and the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations, Part 23) or an act of agricultural terrorism under Florida sunshine laws (s.286.011, F.S), Florida State Statute 119 (Public Records), and the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations, Part 23), vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot, under Florida sunshine laws (s.286.011, F.S), Florida State Statute 119 (Public Records), and the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations, Part 23), be shared without permission.
- A violation of an authorized nondisclosure agreement under Florida sunshine laws (s.286.011, F.S), Florida State Statute 119 (Public Records), and the Criminal Intelligence Systems Operating Policies (28 Code of Federal Regulations, Part 23).

CFIX will not confirm whether or not information exists on its Intelligence Database, including any ISE-SAR information, unless the individual or agency requesting that information is authorized access to that information by existing Memorandum of Understanding with that individual or agency or unless otherwise required by law. 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 intelligence information" or "active criminal investigative information" and therefore exempt from disclosure pursuant to Fla. Stat. § 119.071(2)(c).
- Protected federal, state or tribal records originated and controlled by the source agency that cannot be shared without permission.
- A violation of an authorized nondisclosure agreement

K. Redress/ Disclosure

Information retained by CFIX is "active criminal intelligence information" or "active criminal investigative information" and therefore exempt from disclosure pursuant to Fla. Stat. § 119.071(2)(c). If a request is made under the Florida Public Records Act for information or intelligence that has been documented in CFIX files, the public records request shall be forwarded to the CFIX Director, who shall immediately contact the Privacy Officer to assist him in formulating a response to the request. Requests to CFIX under the Florida Public Records Act shall be directed to the CFIX Director at the following address: CFIX Director, P.O. Box 621133 Orlando, FL 32862. The CFIX Director, as the custodian of the public records maintained by CFIX[5], shall respond to the public records request if in his opinion there are sufficient facts to support a denial of the request. If the CFIX Director believes the matter should be reviewed for legal sufficiency before responding, the CFIX Director will document the request as a task and forward the public records request along with the recommendation of the Privacy Officer to legal counsel. When the review is complete, CFIX will label the task as completed in the tasking log.

[5] *See* Fla. Stat. § 119.07(1)(e), which requires the custodian of the record to assert any applicable exemptions. §119.07(1)(f) provides that the person requesting the public record is entitled to a written response asserting any exemption, if one is requested.

CFIX will keep accurate records of all requests, the result of the request and any information that was disclosed to the requestor. Record shall reflect name of requestor, date of request, specifications of request, outcome of request and the date the request was completed.

The existence, content and source of information will not be made available to an individual when it is within the provisions of Florida State Statute 119 (Public Records) (at §119.071 (2) providing exemptions for agency investigations), exempt from disclosure under a general or special law of the State of Florida, or the Criminal Intelligence Systems Operating Policies (28 CFR Part 23) including when:

- 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 ,
- the information is in a criminal intelligence system, subject to 28 CFR Part 23,
- The information source does not reside with CFIX , or
- CFIX did not originate or does not own or have a right to disclose the information

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

If a public records request under Florida Statute 119 was made via FDLE Office of General Counsel and the decision was made to release information, any complaints or objections to the accuracy or completeness of information retained about an individual would be handled via the FDLE legal staff. Initially the complaint will be reviewed by the CFIX Director and the Privacy Officer. The individual would be requested to provide a written request to modify the documentation, remove the record and provide adequate reasoning for the request. CFIX would assist in investigating and correcting any erroneous documentation that was discovered as the result of the public record request. CFIX would coordinate with the appropriate agency to assure the information is corrected timely. The information would then be submitted to the FDLE legal staff with explanations and recommendations whether or not the documentation should be retained or modified.

The individual to whom information has been disclosed will be given reasons if requests for correction(s) are denied by the center or the originating agency. The individual will also be informed of the procedure for appeal when the original request to correct or modify challenged information is declined. All challenges will also be handled by the FDLE Legal Staff.
Any issues or complaints that involve terrorism-related information shall be considered an ISE related issue. Complaints or challenges for this type of information will be handled in the same manner that complaints regarding other intelligence collection and retention issues are handled.

If an individual has a complaint with regard to the accuracy or completeness of protected information that:

(a) Is exempt from disclosure, and
(b) (1) Is held by the CFIX and
(2) Allegedly has resulted in demonstrable harm to the complainant,

- The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the center's Director and forwarded to the Privacy Officer. The Privacy Officer can be contacted at: Victor Lee Chapman, Barrett, Chapman & Ruta P.A, 18 Wall Street, Orlando, Florida,

32801. Telephone number (407) 839-6227, fax number (407) 648-1190, email victor@bcrlaw.net or c/o his assistant Vicki@bcrlaw.net . The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the center that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate, incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the center of all complaints and the resulting action taken in response to the complaint.

L. Security Safeguards

The CFIX Director or his designee will serve as the Security Officer. Training for this position is provided by the Department of Homeland Security (DHS) Representative for the State of Florida. The CFIX will operate in a secure facility protected from external intrusion. The CFIX will utilize secure internal and external safeguards against network intrusions. Access to CFIX databases from outside the facility will only be allowed over secure networks.

The CFIX 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.

The CFIX 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.

Access to the center information will only be granted to center personnel whose position and job duties require such access and the individual has successfully completed a background check and appropriate security clearance, if applicable, and has been selected, approved, and trained accordingly.

Queries made to the CFIX database are electronically logged. Databases and programs will be password protected and audit trails for database use are available.

The CFIX will utilize watch logs to maintain audit trails of requested and disseminated information.

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

In the event of a security breach, the CFIX Security Director would notify the agency that submitted the data and alert them to the breach. The Security Director and/or the contributor would notify the individual about whom personal information was or is reasonably believed to have been compromised or obtained by an unauthorized person and access to which threatens physical, reputation, or financial harm to the person. Any notice will be made promptly and without unreasonable delay following discovery or notification of the access of the information,

consistent with the legitimate needs of law enforcement to investigate the breach or any measure necessary to determine the scope of the breach and, if necessary, to restore the integrity of the system.

M. Information Retention and Destruction

All applicable information will be reviewed for record retention (validation or purge) at least every five (5) years, as provided by 28 CFR Part 23. Consistent with the Florida Fusion Center guidelines, information including tips and SARs should be reviewed and evaluated for contemporaneous value within 90 days and purged within a 2 year window if inactive status.

When information has no further value or meets the criteria for removal according to the CFIX's retention and destruction policy, it will be purged, destroyed, and deleted or returned to the submitting source.

The CFIX will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency in a participation or membership agreement.

Permission to destroy or return information or records will be presumed if the applicable information is not validated within the specified time period.

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

A record of information to be reviewed for retention will be maintained by the CFIX and for appropriate system(s), notice will be given to the submitter when it is time to be reviewed and/or purged.

N. Accountability and Enforcement

The CFIX will be open with the public in regard to information and intelligence collections practices. The CFIX's privacy policy will be provided to the public for review and will be made available upon request.

The Privacy Policy will be posted on the CFIX website in an area viewable by the general public. A link to the CFIX website will be available to be posted on each law enforcement agency's website within Region 5 of the Domestic Security Task Force.

The CFIX Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the agency. The Privacy Officer can be contacted at: Victor Lee Chapman, Barrett, Chapman & Ruta P.A, 18 Wall Street, Orlando, Florida, 32801. Telephone number (407) 839-6227, fax number (407) 648-1190, email victor@bcrlaw.net or c/o his assistant vicki@bcrlaw.net.

All CFIX personnel will sign a Non-disclosure agreement when assigned to CFIX. The non-disclosure agreement specifies that all personnel will comply with the established privacy policy

and the security policy. If there are any suspected violations of the release of information or privacy policy, they shall be reported to the Privacy Officer.

The audit log of queries made to the CFIX will identify the user initiating the query.

The CFIX will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of 2 years for this type of request for access to information for specific purposes and of what information is disseminated to each person in response to the request.

The CFIX will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least annually and a record of the audits will be maintained by the CFIX Director.

Annual audits will be conducted, by the Privacy Officer or a designated representative of the agency, in such a manner so as to protect the confidentiality, sensitivity, and privacy of the center's criminal intelligence system. The Privacy Officer has the option of conducting a random audit, without announcement, at any time and without prior notice to staff of the center. Audit records will be reviewed as needed.

The Privacy Officer will make recommendations to the CFIX Governing Board of appropriate changes to the Privacy Policy annually in response to changes in applicable law, changes in technology, changes in the purpose and use of the information systems. The decision as to the implementation of any changes will be within the discretion of the Governing Board. The Privacy Officer will also serve as the point of contact for all complaints to include ISE related issues.

If an authorized user is found to be not complying with the provisions of this policy regarding the collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of CFIX may:

- 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 center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

The CFIX reserves the right to restrict the qualifications and number of personnel having access to center information and to suspend or withhold service to any personnel violating the privacy policy. The center reserves the right to deny access to any participating agency user who fails to comply with the applicable restrictions and limitations of the CFIX Privacy Policy.

O. Training

All authorized individuals and source agencies submitting, receiving or disseminating criminal intelligence or criminal investigative information or suspicious activity reports to CFIX., or having access to the shared space and ISE-SAR information will participate in training programs regarding implementation of the adherence to privacy, civil rights and civil liberties policies and protections pertinent to the scope of their employment and access to said information.

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

The training program will include the purpose of the policy, the intent of the provisions, the impact of infractions and the enforcement ramifications for noncompliance, originating and participating agency responsibilities and obligations under applicable law and policy, how to implement the policy in the day-to-day work of the user, whether a paper or systems user, mechanisms for reporting violations of center privacy protection policies and procedures, and the nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any. All personnel will sign an acknowledgement form indicating they were trained on, have access to and understand the privacy policy.

APPENDIX 1
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 which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information and law enforcement information acquired and documented 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.

Active Intelligence – criminal intelligence information shall be considered ―active‖ as long as it is related to intelligence gathering conducted with a reasonable, good faith belief that it will lead to detection of ongoing or reasonably anticipated criminal activity.

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

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 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.

Authorization - The process of granting a person, computer access or 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.

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.

Center - Center refers to CFIX

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. Civil rights are, therefore, obligations imposed upon government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

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.

Credentials - Information that includes identification and proof of identification that is utilized by CFIX 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. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Criminal Intelligence System – the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information.

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 Steering Committee - Comprised of one representative from each county law enforcement agency in Region 5 of the Domestic Security Task Force (DSTF) of the participating agencies and chaired by a member elected by a majority of the board. The CFIX Executive Steering Committee will serve in an advisory capacity only.

Fair Information Practices -The Fair Information Practices (FIPs) 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 transporter 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 CFIX Privacy Policy 17 8/27/2010

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 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. The Homeland Security Advisor is 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.

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.

ISE-SAR Information Exchange Package Documentation (IEPD) - A schema that facilitates the posting and sharing of ISE-SAR information. The ISE-SAR IEPD is used to represent ISE information in two different data formats:
(1) The **Detailed format** includes information contained in all data elements set forth in Section IV of the ISE-SAR FS (―ISE-SAR Exchange Data Model‖), including fields denoted as privacy fields.
(2) The **Summary format** excludes certain privacy fields as identified in the ISE-SAR FS. The ISE-SAR FS identifies the minimum privacy fields that must be excluded. Each ISE participant may exclude additional privacy fields from its Summary ISE-SARs, in accordance with applicable legal requirements.

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.

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

Least Privilege Administration - A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks they are authorized to perform.

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

Maintenance of Information - The maintenance of information applies to all forms of information storage. This would include electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an

organization is not required to create new systems to maintain information or maintain information beyond a time when it no longer serves an organization's purpose.

Metadata - In its simplest form, metadata is information (data) about information, more specifically information about a particular content. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based upon the type of information and context of use.

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

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

Originator – an agency that has provided criminal intelligence information to this agency

Participating Agencies - Participating agencies, for purposes of the EE Initiative, include source [the agency or entity that originates SAR (and, when authorized, ISE-SAR) information], submitting (the agency or entity posting ISE-SAR information to the shared space), and user (an agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information, including information in the shared space(s), and which may include analytical or operational component(s) of the submitting or authorizing agency or entity) agencies, in support of their responsibility to collect, document, process, access, or use SAR and ISE-SAR information.

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.).

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.

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 Fields - Data fields in ISE-SAR IEPDs that contain personal information.

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

Privacy Protection - This is a process of finding appropriate balances between privacy and multiple competing interests, such as justice information sharing. 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 includes information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Florida 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, and tribal laws and ordinances. Protection may be extended to organizations by CFIX policy or state, local, or tribal law.

Public - Public includes:
- Any person and any for-profit or nonprofit entity, organization, or association;

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

Public does not include:

- Employees of the agency;
- People or entities, private or governmental, who assist the agency in the operation of the justice information system, and agency in the operation of the justice information system; and
- Public agencies whose authority to access information gathered and retained by the agency is specified in law.

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

Reasonable Suspicion – is established when there are sufficient facts to give a trained member of law enforcement a reasonable basis to suspect that an individual or organization has engaged, is engaging, or is about to engage in criminal activity.

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 Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

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

Role-Based Authorization/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.

Shared Space - 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.

Sharing - The act of one ISE participant disseminating or giving homeland security information, terrorism information, or law enforcement information to another ISE participant.

SLT - State, Local and Tribal

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 (and, when authorized, ISE-SAR) information.

Submitting Agency - The agency or entity providing ISE-SAR information to the shared space.

Suspicious Activity -. Defined in the ISE-SAR Functional Standard (Version 1.5) as "observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity." Examples of suspicious activity include surveillance, photography of facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (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 or data mining tools. Any patterns identified during SAR data mining and analysis may be investigated in coordination with the reporting agency and the state designated fusion center. 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.

Terrorism Related Information—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 confidential 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), to 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.

User Agency - The agency or entity authorized by the submitting agency or other authorized agency or entity to access ISE-SAR information in the shared space(s), 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.