SAN ANTONIO POLICE DEPARTMENT
Southwest Texas Fusion Center
Privacy Policy

RESPONSIBILITIES: To ensure personnel with direct access to the Southwest Texas Fusion Center's information comply with federal, state, and local laws regarding the collection and use of information about individuals.

TASKS:

.01 PURPOSE STATEMENTS

A. The Southwest Texas Fusion Center (hereafter referred to as SWTFC or Center) is a partnership between South Texas regional law enforcement, fire, and emergency management agencies and services. This partnership will function to enhance the safety and security of the region by serving as an all crimes / all hazards information-sharing center. The SWTFC will prioritize intelligence sharing on organized criminal gangs, border violence and terrorism through a strategy of information collection, processing, analysis and dissemination to partners in the region. Additionally, the SWTFC will serve to enhance the effectiveness, strength, and coordination of the region's public safety and private industry partners and support the overall State of Texas Homeland Security Strategy and the National Strategy for Homeland Security.

B. The gathering of information in support of these goals is vital to achieving success, but must be balanced and guided by the need and responsibility to preserve the rights and privacy of the citizens we protect. As such, this policy applies to all individuals and organizations working with or through the SWTFC. The purpose of the SWTFCs Privacy Policy is to ensure personnel with direct access to the Center's information comply with federal, state, and local laws, SWTFC policies and procedures, and assists its authorized users in:

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

C. The SWTFC Privacy Policy incorporates the principles of the Fair Information Practice Principles (FIPPs) as outlined by the National Criminal Justice Association (NCJA) as well as the Department of Justice's (DOJ) Global Justice Information Sharing Initiative.

.02 POLICY APPLICABILITY AND PROCEDURE

A. All SWTFC personnel, participating agency personnel, personnel providing information technology services to the SWTFC, private contractors, and other authorized users will comply with the SWTFCs privacy policy. This policy applies to information the Center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to Center personnel, governmental agencies (including Information Sharing Environment (ISE) participating agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

B. A printed or electronic copy of this policy will be provided to all SWTFC personnel and to other participating agencies and individual users. The Center will require a written acknowledgement of receipt of this policy and a signed MOU/User Agreement to comply with this policy and the applicable provisions it contains.

C. All SWTFC personnel, participating agency personnel, personnel providing information technology services to the Center, private contractors, agencies from which information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including but not limited to those listed in *Appendix A.2, Laws, Regulations and References.*

D. The SWTFC has adopted internal operating procedures in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including but not limited to the state and federal laws referenced in the preceding paragraph.

E. The SWTFC will make this policy available to the public through available resources, including the SWTFC website and the City of San Antonio's website.

.03 GOVERNANCE AND OVERSIGHT

A. The San Antonio Police Department (SAPD) has primary responsibility for the operation of the SWTFC. The Center's governance will consist of an Advisory Board, Operational Management Team, SWTFC Director and Privacy Officer.

B. The SAPD police chief or designee will appoint a SWTFC Director, who will be responsible for the day to day operation of the Center. The Director will establish needed procedures, practices and protocols as well as use advanced software, information technology tools, and physical security measures to ensure information and intelligence are accessed only by authorized personnel and are protected from unauthorized access, modification, theft, or sabotage, whether internal, external, or disasters or intrusions by natural or human causes. The Director will coordinate with the Privacy Officer to ensure enforcement procedures and sanctions are adequate and adhered to.

C. Overall responsibility for SWTFC justice systems, operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and the enforcement of this policy is assigned to the SWTFC Director.

D. The SWTFC is guided by an Advisory Board, comprised of South Texas regional law enforcement, fire, and members of the private sector. This Board liaises with the community to ensure privacy and civil rights are protected as provided by this policy and by the Center's information-gathering and collection, retention, and dissemination procedures. The Board will be chaired by the SAPD Chief of Police or his/her designee. The Advisory Board will meet as needed but not less than annually to review and update this policy in response to changes in laws and implementation experience, including the results of audits and inspections. The Board will have the following responsibilities:

1. Resolve conflicts or disputes that might arise related to policy or mission;

2. Establish protocol concerning the treatment of violations of the agreement;

3. Resolve disputes between Partner Agencies arising from the operations and activity of the Center; and

4. Review and update the SWTFC Privacy Policy annually based upon recommendations by the Privacy Advisory Committee (described below) and changes in applicable law.

E. SWTFC will have a trained Privacy Officer, who is appointed by the SWTFC Director. The Privacy Officer receives reports regarding alleged errors and violations of this policy, receives and coordinates complaint resolution under the Center's redress policy, and serves as the liaison for the Information Sharing Environment (ISE), ensuring privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.

1. The SWTFCs Privacy Officer is tasked with ensuring the enforcements outlined in Section O, Accountability and Enforcement, of this policy are adequate and enforced.

2. The Privacy Officer will review analytical products to ensure they provide appropriate privacy, civil rights and civil liberties protections prior to dissemination or sharing by the SWTFC.

3. The Privacy Officer can be contacted at the following address: Southwest Texas Fusion Center, c/o San Antonio Police Department, 315 South Santa Rosa, San Antonio, TX 78207 or at swtxfusion@sanantonio.gov.

F. A Privacy Policy Advisory Group will be formed to make recommendations to the SWTFC Advisory Board regarding this policy. The Group will review the Privacy Policy annually to ensure safeguards and sanctions are in place to protect personal information, and will advise the Advisory Board of its recommendations based on the purpose and mission statements of SWTFC.

1. The Group will be comprised of members of the community who represent a diverse range of interests and expertise. The meetings will be attended by the Privacy Officer to provide input on the operations of Center.

2. The Group will annually select from its membership a Chair and any additional officers the Board finds appropriate. A person may not serve as the Chair for more than two consecutive years. Upon selection of the chair and additional officers, the Group will agree upon the meeting schedule and other operational procedures.

3. The Group will provide an annual report to the Partner Agencies regarding any proposed changes to the Privacy Policy.

.04 DEFINITIONS

A. Primary terms and definitions used in this SWTFC policy are located in Appendix A.1, Terms and Definitions

.05 INFORMATION

A. The SWTFC has the potential to come into contact with a broad scope of both public and private information and data. Center personnel will not seek to collect, analyze or disseminate information or data that does not support the identified goals of supporting law enforcement, disrupting crime or preventing terrorism or violent acts. The Center prohibits its personnel and participating agencies from seeking or retaining information about individuals or organizations solely on the basis of their religious,

political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

B. The SWTFC only seeks or retains information that:

1. Is based on a criminal predicate or possible threat to public safety; or

2. Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity; or

3. Is relevant to the investigation and prosecution of suspected criminal incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime; or

4. Is useful in crime analysis or in the administration of criminal justice and public safety; and

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

6. The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

C. The Center may retain protected information that is based on a level of suspicion that is less than "reasonable suspicion," such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified in this policy. Refer to ***Section F, Tips, Leads and Suspicious Activity Reports,*** for more regarding this type of information.

D. The SWTFC applies labels to Center-originated information, and ensures that originating agencies have applied labels, to indicate to the accessing authorized user that:

1. The information is protected information as defined by the Center, to include personal information on any individual. To the extent expressly provided in this policy, organizational entities are included. See ***Appendix A.1*** for definitions of ***protected information*** and ***personal information***.

2. The information is subject to local, state or federal laws, identified in ***Appendix A.2***, restricting access, use, or disclosure.

E. SWTFC personnel or participating agencies will assign categories to the information to reflect:

1. What the information consists of - tips and leads, suspicious activity report, investigative or intelligence information.

2. The nature of the information source - anonymous tip, trained investigator, or public record.

3. The reliability of the information source - reliable, usually reliable, unreliable, or unknown.

4. The validity of the content - confirmed, probable, doubtful, or cannot be judged.

F. When a decision is made by the SWTFC to retain information, it will be labeled pursuant to applicable limitations on access and sensitivity of disclosure to:

1. Protect confidential sources and police undercover techniques and methods.

2. Not interfere with or compromise pending criminal investigations.

3. Protect an individual's right of privacy or his/her civil rights and civil liberties.

4. Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

G. The labels assigned to existing information under this section will be reevaluated whenever:

1. New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.

2. There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

.06 TIPS, LEADS AND SUSPICIOUS ACTIVITY REPORTS

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

1. Prior to allowing access to or dissemination of the information, ensure 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 standard reporting formats and data collection codes for SAR information.

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

3. Allow access to or disseminate the information using the same access and dissemination standard used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).

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

5. Retain information for 180 days in order to work an un-validated tip, lead, or SAR information to determine its credibility and value or assign a "disposition" label (cleared or unfounded) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

6. Adhere to and follow the Center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

.07 IDENTIFYING AND REVIEWING INFORMATION

A. The SWTFC 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 (ISE). 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.

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

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

2. The name of the justice information system from which the information is disseminated.

3. The date the information was collected and, where feasible, the date its accuracy was last verified.

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

C. The SWTFC will attach (or ensure 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.

D. The SWTFC will keep a record of the source of all information sought and collected by the Center.

E. The SWTFC 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.

.08 ACQUIRING AND RECEIVING INFORMATION

A. Information-gathering (acquisition), access, and investigation techniques used by the SWTFC and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including but not limited to those listed in *Appendix A.2* of this policy.

B. The SWTFCs SAR process provides for human review and vetting to ensure 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.

C. The SWTFCs 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 information that could violate civil rights and civil liberties will not be intentionally or inadvertently gathered, documented, processed, and shared.

D. Information-gathering and investigative techniques used by the SWTFC and originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

E. External agencies that access SWTFCs information or share information with the Center are expected to adhere to the same laws and rules governing the Center, including applicable federal and state laws.

F. External agencies must, upon request, provide to the SWTFC any relevant source documentation (i.e., arrest report or field intelligence notes) to support a submitted record. Supporting documentation must be maintained by the external agency for as long as the record is retained or a legal challenge to the record is pending.

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

H. The SWTFC will not directly or indirectly receive, seek, accept, or retain information from:

1. An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or Center policy.

2. An individual or information provider legally prohibited from obtaining or disclosing the information.

.09 PUBLIC SURVEILLANCE SYSTEMS

A. The SWTFC and participating agencies may use and employ certain electronic camera or surveillance systems for the enhancement of overall protection of the public, critical infrastructure, key resources or public areas easily accessed by the general public.

B. No data or images from these systems may be accessed or used by any person except for the legitimate protection of the public or the furtherance of an approved criminal investigation.

C. Any data or images stored or accessed by the SWTFC will only be retained through recording or from the use of any these systems for a period of 90 days unless specifically identified by *Reasonable Suspicion* standards as related to criminal activity. Without such correlation or analysis, all data or images will be purged and a permanent log or record kept identifying the person and method used for purging.

D. Any query or request for dissemination of stored data from these systems by any person except for furthering an authorized criminal investigation will be refused. Permanent logs regarding any request for dissemination and any such refusal, along with the method and identification of the person making routine destruction, will be available upon request at the SWTFC office.

.10 INFORMATION QUALITY ASSURANCE

A. The SWTFC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other information about the same individual or organization only when the applicable standard has been met (refer to *Section J, Merging Records*).

B. At the time of retention in the system, the information will be labeled regarding its level of quality, including accuracy, completeness, currency, verifiability and reliability.

C. The SWTFC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

D. The labeling of retained information will be reevaluated by the SWTFC or the originating agency when new information is gathered that has an impact on the source reliability and/or content validity of previously retained information.

E. The SWTFC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure the information is corrected, deleted from the system, or not used when the Center learns information 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).

F. Originating agencies external to the SWTFC are responsible for reviewing the quality and accuracy of the data provided to the Center. Center personnel will review the quality of information it has received from an originating agency and advise the appropriate contact person, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

G. The SWTFC 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. This includes information that is incorrectly merged, out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

.11 COLLATION AND ANALYSIS

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

B. Information subject to collation and analysis is information as defined and identified in *Sections E and F* of this policy.

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

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

2. Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

.12 MERGING RECORDS

A. The set of identifying information sufficient to allow merging will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

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

.13 DISSEMINATION AND DISCLOSURE

A. The SWTFC utilizes credentialed, role-based access criteria to determine dissemination and access to

information. Specifically, the Center will control the information to which a particular group or class of users can have access based on the group or class, and the information a class or user can add, change, delete, or print.

B. The SWTFC 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, commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

C. Access to or disclosure of records retained by the SWTFC will be provided only to persons within the Center or in other governmental agencies who are authorized to have access. Access will be allowed only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working.

D. Agencies external to the SWTFC may not disseminate information accessed or disseminated from the Center without approval from the Center or other originator of the information.

E. Records retained by the SWTFC 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.

F. Information gathered or collected and records retained by the SWTFC 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.

G. An audit trail sufficient to allow the identification of each individual that requested, accessed, or received information retained by the SWTFC; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of five years by the Center.

H. Information gathered or collected and records retained by the SWTFC 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.

I. The SWTFC will ensure that an audit trail sufficient to allow the identification of each individual that is requested, accessed, or received information retained by the Center is kept for a minimum of five years. The audit trail documentation will include the following information about the dissemination:

   1. The suspect and personally identifying information released.

   2. Restrictions on dissemination.

   3. The date and time of the query or related access transaction.

   4. The name of the individual and agency requesting the record.

J. Information gathered or collected and records retained by the SWTFC will not be:

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

   2. Disclosed or published without prior notice to the originating agency that such information is

subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.

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

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

1. Disclosure would interfere with, compromise or delay an ongoing investigation or prosecution; Tex Gov't Code § 552.108.

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

3. The information is a criminal intelligence information system subject to 28 CFR Part 23; Tex Gov't Code § 552.108.

4. The information relates to other matters excepted from disclosure under the Texas Public Information Act, Tex Gov't Code § 552.

5. The information does not reside with the SWTFC.

6. The SWTFC did not originate and does not have the right to disclose the information, including information that meets the definition of "classified" information as that term is defined in the National Security Act, Public Law 235, Section 606, in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

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

.14 REDRESS

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

B. The existence, content, and source of the information will not be made available by the SWTFC to an individual when:

1. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution – Tex Gov't Code § 552.108.

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

3. The information is in a criminal intelligence information system subject to 28 CFR Part 23 – Tex Gov't Code § 552.108.

4. The information relates to matters excepted from disclosure under the Texas Public Information Act – Tex Gov't Code § 552.

5. The information source does not reside with the SWTFC.

6. The SWTFC did not originate and does not have a right to disclose the information, including information that meets the definition of "classified" information as that term is defined in the National Security Act, Public Law 235, Section 606, in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.

7. Other authorized basis for denial, including but not limited to Tex Gov't Code §§ 552.101, 552.108, 552.111, 552.117, 552.1175, 552.119, 552.132, 552.1325, 552.134, 552.137, 552.138, 552.139, 552.142, 552.1425, 552.147, 552.148, 552.150, and 552.151.

C. If the information does not originate with the SWTFC, 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.

D. If an individual requests correction of information originating with the SWTFC that has been disclosed, the Center's Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

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

F. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information held by the SWTFC that is exempt from disclosure, or has been or may be shared through the ISE, and allegedly has resulted in demonstrable harm to the complainant, the Center will inform the individual of the procedure for submitting and resolving such complaints.

1. Complaints will be received by the SWTFC Privacy Officer or Director at the following address: Southwest Texas Fusion Center, c/o San Antonio Police Department, 315 South Santa Rosa, San Antonio, TX 78207 or swtxfusion@sanantonio.gov.

2. The Privacy Officer or Director 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.

3. If the information did not originate with the SWTFC, the Privacy Officer or Director 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.

4. All information held by the SWTFC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or information which is 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.

5. A record will be kept by the SWTFC of all complaints and the resulting action taken in response to the complaint.

G. To delineate protected information shared through the ISE from other data, the SWTFC maintains

records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

.15 SECURITY SAFEGUARDS

A. The Director will designate a Facilities Information Security Officer (FISO) who will be trained to serve as the SWTFCs security officer. Training will include all aspects of security, information classification, and 28 CFR Part 23.

B. The SWTFC and participating agencies will comply with the security provisions of the Criminal Justice Information Services (CJIS) Security Policy. The Center will provide:

1. Physical Security - including a secure area for placement of each item of equipment to preclude physical access by other than authorized personnel and to control visitor access.

2. Operational Security - including equipment operated to preclude system access by other than authorized personnel or for other than authorized purposes and to change system access identifiers for terminated or reassigned personnel.

3. Personnel Security - including access allowed only to law enforcement or criminal justice personnel; or technical or maintenance personnel who have been subject to character or security clearance.

C. The SWTFC 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.

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

E. Access to SWTFC information will be granted only to Center personnel whose positions and job duties require such access; who have successfully completed a background check and appropriate security clearance, if applicable; and who have been selected, approved, and trained accordingly.

F. Queries made to the SWTFCs data applications will be logged into the data system identifying the user initiating the query.

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

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

I. The SWTFC will follow Tex Gov't Code § 521.053 and notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person. The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of information and, if necessary, to reasonably restore the integrity of any information system affected by this release.

.16 INFORMATION RETENTION AND DESTRUCTION

A. The SWTFC will evaluate all applicable information at a minimum of every five years from the date of receipt, for determination of relevance and continuing criminal predicate for retention, as provided by 28 CFR Part 23.

B. When information has no further value or meets the criteria for removal according to the SWTFC retention and destruction policy or according to applicable law, it will be purged, destroyed, and deleted or returned to the originating agency.

C. The SWTFC 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.

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

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

F. The SWTFC will keep no record of individual records purged, but will identify the number of records purged.

G. A record of information to be reviewed for retention will be maintained by the SWTFC, and for appropriate systems, notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

.17 ACCOUNTABILITY AND ENFORCEMENT

A. The SWTFC will be open with the public in regard to information and intelligence practices. The Center's privacy policy will be provided to the public for review, made available upon request, and posted on the San Antonio Police Department website at www.sanantonio.gov/SouthwestTexasFusionCenter.

B. The SWTFCs 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). Complaints should be directed to: Southwest Texas Regional Fusion Center, c/o San Antonio Police Department, 315 South Santa Rosa, San Antonio, TX 78207 or swtxfusion@sanantonio.gov.

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

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

E. The SWTFC 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 quarterly and a record of the audits will be maintained by the Privacy Officer of the Center.

F. SWTFC personnel or other authorized users have an affirmative responsibility to immediately report errors and suspected or confirmed violations of Center policies relating to protected information or the loss or mishandling of any personal or sensitive information to the Privacy Officer.

G. The SWTFC will annually conduct and audit and inspection of the information contained in its criminal intelligence and other systems. The audit will be conducted by the FISO or an appointed independent representative. The audit may be conducted randomly, without announcement, at any time and without prior notice to Center personnel. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the Center's information and intelligence systems.

H. The SWTFC Advisory Board, guided by the appointed and trained Privacy Officer, will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

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

1. Suspend or discontinue access to information by the SWTFC personnel, the participating agency, the authorized user.

2. Suspend, demote, transfer, or terminate SWTFC personnel, as permitted by applicable personnel policies. Any of these actions may occur immediately and without prior notice. Suspension may be followed by termination if deemed necessary by the Director.

3. Apply administrative actions or sanctions as provided by SWTFC rules and regulations or as provided in applicable personnel policies.

4. If the authorized user is from an agency external to SWTFC, 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.

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

J. The SWTFC reserves the right to restrict the qualifications and number of personnel having access to Center information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the Center's privacy policy.

.18 TRAINING

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

1. All assigned personnel of the SWTFC.

2. Personnel providing information technology services to the SWTFC.

3. Staff in other public agencies or private contractors providing services to the SWTFC.

4. Any other users who are not employed by the SWTFC or a contractor.

B. The SWTFC 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.

C. The SWTFCs privacy policy training program will cover:

1. Purposes of the privacy, civil rights, and civil liberties protection policy.

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

3. Originating and participating agency responsibilities and obligations under applicable law and policy.

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

5. The impact of improper activities associated with infractions within or through the agency.

6. Mechanisms for reporting violations of Center privacy protection policies and procedures.

7. The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

APPENDIX A.1
PRIVACY POLICY 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. Data access is usually specified as read-only and read/write access. With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

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

Acquisition - The means by which an ISE participant obtains information through the exercise of its authorities; for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer 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.

Administration of Criminal Justice - The performance of any of the following activities: detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of a criminal offender. The term includes criminal identification activities and the collection, storage, and dissemination of criminal record information.

Administrator - The individual appointed by the San Antonio Police Department as the system administrator for intelligence systems or another individual designated to serve in that capacity.

Audit Trail - A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail - what commands were issued to the system, what records and files were accessed or modified, etc. Audit trails are a fundamental part of computer security, used to trace (albeit usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

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

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

Authorized User - An individual designated by an agency head and authorized by the Administrator for direct access to intelligence systems.

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

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

Civil Rights - The term "civil rights" is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on 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 - The protection of information assets through the use of technology, processes, and training.

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

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

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

Criminal Justice Agency - A federal, state, or local entity that is engaged in the administration of criminal justice under a statute or executive order and that allocates a substantial part of its annual budget to the administration of criminal justice.

Criminal Predicate - Articulable information exists to establish sufficient facts to give a trained criminal justice officer, investigator, or employee reasonable suspicion to believe that a particular criminal street gang or organization or criminal suspect is or may be involved in definable criminal activity or enterprise.

Criminal Street Gang or Gang - Three or more individuals having a common identifying sign or symbol or an identifiable leadership who continuously or regularly associate in the commission of identifiable criminal activities.

Criminal Street Gang Member or Gang Member - An individual who has been identified as a member of a criminal gang through documentation supported by 28 CFR Part 23 standards.

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

Data Breach - The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

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

Direct Access - The action of an individual authorized user to gain direct computer access to intelligence system.

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 disc 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, or transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, or faxback systems. It does not include faxes, telephone calls, video teleconferencing, or messages left on voicemail.

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.

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

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

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

Indirect Access - The action of an individual who is not an authorized user, to gain indirect access to intelligence systems through an authorized user based on a right and need to know.

Individual Responsibility - Because a privacy notice is not self-implementing, an individual within an organization's structure must also be assigned responsibility for enacting and implementing the notice.

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

Information Quality - The validity, accuracy, timeliness, completeness, relevancy, importance, and reliability of information supporting an intelligence system record.

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

Intelligence Information Validity - Evaluation assessed by an Authorized user or other trained person regarding the validity of the information or record submitted as to the information accuracy or truthfulness and is assigned as Confirmed, Probable, Doubtful or Can Not Be Judged, as defined by and consistent with 28 CFR Part 23 definitions.

Intelligence Led Policing (ILP) - A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Intelligence Source Reliability - Evaluation assessed by an authorized user or trained person regarding the consistency of the source in providing intelligence information and is assigned as Reliable, Usually Reliable, Unreliable or Unknown as defined by and consistent with 28 CFR Part 23 definitions.

Invasion of Privacy - Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

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

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

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

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

Local Entity - An agency or other entity of a political subdivision of the State, including a city or county. The term includes a task force, law enforcement agency of a school district or institution of higher education, whether public or private, or other local entity that is engaged in the administration of criminal justice under a statute or executive order.

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

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

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

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.

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

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

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

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

Personal Information - Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in criminal activity, including terrorism. See also Personally Identifiable Information.

Personally Identifiable Information - 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, Integrated Automated Fingerprint Identification System [IAFIS] 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 United States citizens, aliens known by the intelligence agency concerned to be permanent resident aliens, 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 - Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the capacity to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy - A printed, published statement that articulates the policy position of an organization on how it handles the personal 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 SWTFC will adhere to those legal requirements and Center 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 Center, the individual, and the public; and promotes public trust.

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

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 Texas 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, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion SWTFC or other state, local, or tribal Southwest Texas Regional Fusion SWTFC policy or regulation.

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 SWTFCs information. Media organizations. Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the SWTFC or participating agency. Public does not include employees of the SWTFC or participating agency, people or entities, private or governmental, who assist the SWTFC in the operation of the justice information system, public agencies whose authority to access information gathered and retained by the SWTFC is specified in law.

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

Reasonable Suspicion - Predicate is defined or established when information exists that substantiates sufficient facts to give a trained law enforcement or criminal investigative agency, officer, investigator or assigned employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

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 - Laws, policies, and procedures that address public agency responsibilities with regard to access/disclosure and correction of information and the handling of complaints from persons regarding protected information about them which is under the SWTFCs control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.

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

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 right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about 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 a person's privacy.

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

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

Source Agency - Source agency refers to the agency or organizational entity that originates SAR (and when authorized, ISE-SAR) information.

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 sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Report (SAR) - Official documentation of observed behavior reasonably indicative of preoperational

planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion SWTFC. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism Information - Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign **or** international terrorist groups or individuals **or** of domestic groups **or** individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

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

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

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

User Agreement - An agreement or written understanding executed under these policies and procedures between the SWTFC and a Participating Agency.

Validation - The determination of the continuing viability, accuracy, and relevancy of the criminal intelligence information supporting an intelligence record as defined by 28 CFR Part 23 standards for Reasonable Suspicion. The term includes the record review, retention, or purge and removal processes required under either 28 CFR Part 23 or CCP.

APPENDIX A.2
PRIVACY POLICY LAWS, REGULATIONS AND REFERENCES

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Classified Information, 32 CFR 2003

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a (a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a (a); see also Office of Management and Budget, Memorandum M-01- 05, ―Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy,‖ December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Department of Homeland Security published Baseline Capabilities Guidelines for Fusion SWTFCs

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Homeland Security Act of 2002 codified at 6 U.S.C. § 482(f)(1)

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

Information Sharing Environment (ISE) Privacy Guidelines as mandated by Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and Executive Order 13388

Intelligence Identities Protection Act, 50 USC 421

Internal Security Act, 50 USC 783

IRTPA, as amended by the 9/11 Commission Act Law Enforcement Intelligence Systems, National Child Protection Act of 1993, Pub. L. 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Presidential Executive Order 13526 Classified National Security Information

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

Texas Code of Criminal Procedure Chapter 61, and amendments contained in Senate Bill 418 81st Legislature regarding Gang Intelligence and 28 CFR Part 23 standards

Texas Government Code Chapter 421 regarding the Department of Public Safety and the collection of terrorist and homeland security information

Texas Government Code Chapter 552 regarding open government

Texas Penal Code Section 71.01 regarding criminal street gang information

Texas Penal Code Section 51.02 regarding information on children

U.S. Constitution, First, Fourth, Sixth, Thirteenth and Fourteenth Amendments

USA Patriot Act, Public Law No. 107-56 (October 26, 2001), 115 Stat. 272

United States Criminal Laws, including 18 USC 641, 783, 793, 794, 798, 952, 1924