Texas Fusion Center
Privacy, Civil Rights, and Civil Liberties Policy

A. Purpose Statement

[1] The powers and duties of the Texas Fusion Center (TxFC) are described in Texas Government Code Chapter 421, Subchapter E; in the Texas Homeland Security Strategic Plan 2010-2015; and in Texas Department of Public Safety policy.

[2] One of the missions of the TxFC is to collect, evaluate, analyze, and disseminate information and intelligence data regarding criminal and terrorist activity in Texas while following appropriate privacy and civil liberties safeguards as outlined in the principles of the Organisation for Economic Co-operation and Development's (OECD) Fair Information Principles (see Appendix A) to ensure that the information privacy and other legal rights of individuals and organizations are protected.

[3] The purpose of this privacy, civil rights, and civil liberties protection policy is to promote TxFC and user conduct that complies with applicable federal and state law and assists the center and its users in:

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

B. Policy Applicability and Legal Compliance

[1] In exercising the powers and duties referenced in Section A[1], the TxFC includes various components. The TxFC's Watch Center is the TxFC component that operates as a fusion center as defined by the Global Justice Information Sharing Initiative's *Fusion Center Guidelines* and *Baseline Capabilities for State and Major Urban Area Fusion Centers*. It is the only TxFC component with responsibility for sharing terrorism-related information in the Information Sharing Environment (ISE). As such, this privacy policy applies to the TxFC Watch Center.

[2] The TxFC personnel, and all assigned or detailed personnel, including personnel providing information technology services, contractors providing support services, and other authorized participants in the TxFC, shall comply with this Privacy Policy and all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information. This policy applies to information TxFC gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including ISE participating centers and agencies), and participating justice and public safety agencies as well to private contractors, private entities, and the general public.

[3] The TxFC will provide a printed or electronic copy of this policy to all center and non-center personnel who provide services and to participating agencies and individual users. The TxFC will require from all appropriate TxFC personnel who provide services and from participating agencies and their individual users both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

[4] All TxFC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, agencies from which center information originates, and other authorized users will comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. and Texas Constitutions, state law, including but not limited to the Texas Government Code Chapter 552 Public Information Act, and applicable Federal law (see Appendix B), including 28 CFR Part 23.

[5] The TxFC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the laws cited in Section B[4].

C. Governance and Oversight

[1] Ultimate responsibility for the operation of the TxFC; its 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 Director of the Texas Department of Public Safety (TxDPS), who will designate a TxFC Director to oversee the daily operation of the center.

[2] The TxFC is guided in part by the Texas Fusion Center Policy Council (TFCPC), an integrated network of fusion centers in Texas, which 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.

[3] The TxFC Privacy Officer, who is an attorney from the TxDPS Office of General Counsel, is appointed by the TxDPS General Counsel. The Privacy Officer receives

appropriate training in privacy, civil rights and civil liberties. The Privacy Officer receives reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the TxFC's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies. The Privacy Officer can be contacted at txfcprivacy@txdps.state.tx.us.

The Privacy Officer will annually review this policy and recommend revisions or changes in response to changes in law and implementation experience, including the results of audits and inspections. The TxFC Director will review these recommendations and update this policy as necessary.

[4] The TxFC's Privacy Officer ensures that enforcement procedures and sanctions outlined in Section N.3 are adequate and enforced.

D. Definitions

[1] For examples of primary terms and definitions used in this policy, see Appendix A.

E. Information

[1] The TxFC will seek or retain information that:

a) Is based on a possible threat to public safety or the enforcement of the criminal law, or
b) Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
c) Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders, or sentences; or the prevention of crime, or
d) Is useful in crime analysis or in the administration of criminal justice and public safety (including topical searches), and
e) The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
f) The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

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

[2] The TxFC will not seek or retain information about individuals or organizations solely on the basis of their religious, political, or social views or activities; their participation in a particular non-criminal organization or lawful event; or, for individuals, solely their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations. Further, these factors will not be considered as factors that create suspicion, except if used as part of a specific suspect description.

[3] This policy applies to protected information about all individuals and organizations (as expressly included by law or policy) obtained by the TxFC in furtherance of its analytical and information sharing missions. Information that furthers an administrative or other non-analytical purpose (such as personnel files, or information regarding fiscal, regulatory or other matters associated with the operation of the TxFC) will not be subject to the provisions of this policy.

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

a) The information is protected information, to include personal information on any individual entitled to protection under federal, state, local, and tribal law (See Appendix A), and, to the extent expressly provided in this policy, includes organizational entities.

b) The information is subject to applicable laws restricting access, use, or disclosure, including but not limited to the U.S. and Texas Constitutions, applicable federal law, and state law, including Texas Government Code Chapter 552 Public Information Act.

[4] The TxFC will assess and categorize information to determine:

a) Whether the information consists of tips and leads data, suspicious activity reports, criminal history or intelligence information, case records, conditions of supervision, or case progress, etc.;
b) The nature of the source as it affects veracity;
c) The reliability of the source; and
d) The validity of the content.

[5] At the time a decision is made by the TxFC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

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

[6] The labels assigned to existing information under Section E[5] will be reevaluated whenever:

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

[7] The TxFC is required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. TxFC personnel will:

a) Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place, and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process described in Section E[5]. The TxFC will use a standard reporting format and data collection codes for SAR information.

b) 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.

c) Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination).

d) 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.

e) Retain information for no more than five years to work a tip or lead or SAR information to determine its credibility and value, assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, or under active investigation) so that a subsequently authorized user knows that status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.

f) Adhere to and follow the TxFC's physical, administrative, and technical security measures that are in place for the protection and security of tips and leads information. Tips, leads, and SAR information will be secured in a system that is the

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

[8] The TxFC will incorporate 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 constitutional rights, including personal privacy and other civil liberties, and civil rights.

[9] The TxFC 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 TxFC 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.

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

a) The name of the originating center, department or agency, component, and subcomponent.
b) The name of the center's criminal justice information system from which the information is disseminated.
c) The date the information was collected and, where feasible, the date its accuracy was last verified.
d) The title and contact information for the person to whom questions regarding the information should be directed.

[11] The TxFC 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.

[12] The TxFC will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

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

a) 28 CFR Part 23 regarding criminal intelligence information.
b) The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).
c) Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).
d) Constitutional provisions and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

[2] The TxFC'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.

[3] The TxFC'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.

[4] External agencies that access the TxFC'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.

[5] The TxFC 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.

[6] The TxFC will not directly or indirectly knowingly receive, seek, accept, or retain information from:

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

G. Information Quality Assurance

[1] The TxFC 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 (see Section I) has been met.

[2] At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence).

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

[4] The labeling of retained information will be reevaluated by the TxFC or the originating agency when new information is gathered that has an impact on confidence in previously retained information.

[5] The TxFC 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).

[6] Originating agencies providing data remain the owners of the data contributed and they are responsible for the quality and accuracy of the data provided to TxFC. The TxFC will review the quality of information it has received from an originating agency and will advise the appropriate contact person in the originating agency, either in writing or electronically, if its data is alleged, suspected, or found to be inaccurate or incomplete, out of date, or unverifiable, where the TxFC is the primary or initial recipient of such information.

[7] The TxFC 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

[1] Information acquired or received by the TxFC 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.

[2] Information subject to collation and analysis is information as defined and identified in Section E.

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

a) Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.
b) Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

[4] The TxFC requires all analytical products be reviewed and approved by a supervisor or, where appropriate, the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. Merging Records

[1] Records about an individual or organization from two or more sources will not be merged by the TxFC 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 a higher accuracy of match.

[2] If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the TxFC 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

[1] Credentialed, role-based access criteria will be used by the TxFC, as appropriate, to control:

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

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

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

[4] Agencies external to the TxFC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

[5] Records retained by the TxFC 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.

[6] Information gathered or collected and records retained by the TxFC 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 one year by the center.

[7] Information gathered or collected and records retained by the TxFC 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 or by the TxDPS Office of General Counsel in the case of Attorney General request documents.

[8] Information gathered or collected and records retained by the TxFC will not be:

a) Sold, published, exchanged, or disclosed for commercial purposes by the TxFC.
b) Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
c) Disseminated to persons not authorized to access or use the information.

[9] There are several categories of records that should ordinarily not be provided to the public:

a) Records required to be kept confidential by law that are excepted from disclosure requirements under Chapter 552, Texas Government Code.

b) A record or part of a record that is confidential by law under Chapter 418, Texas Government Code, including information the public disclosure of which would have a reasonable likelihood of threatening public safety by exposing a vulnerability to terrorist attack or other criminal activity. This may include, but is not limited to a record assembled, prepared, or maintained to prevent, mitigate, or respond to an act of terrorism or an act of agricultural terrorism, vulnerability assessments, risk planning documents, needs assessments, and threat assessments.

c) Investigatory records of law enforcement agencies that are excepted from disclosure requirements under applicable public records laws. However, certain law enforcement records must be made available under Chapter 552, Texas Government Code.

d) Federal records, protected under federal law, which may include records exempt from disclosure under the Freedom of Information Act ("FOIA") that have been provided by the Federal government and 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.

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

K. Redress

K.1 Disclosure

[1] An individual may request to know the existence of and review the information about him or her that has been gathered and retained by the TxFC, pursuant to Texas Government Code Chapter 552 and subject to Section K.1[2]. The procedures to submit

requests for information, and the guidelines for TxDPS to respond to such requests, are explained on the TxDPS website at http://www.txdps.state.tx.us/pia.htm

As required by law, 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, as required by law. A record will be kept of all requests and of what information is disclosed to an individual.

[2] The existence, content, and source of the information will not be made available by the TxFC to an individual in the circumstances described below, unless such disclosure is otherwise required by law.

a) Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution.
b) Disclosure would endanger the health or safety of an individual, organization, or community.
c) The information is in a criminal intelligence information system subject to 28 CFR Part 23 [see 28 CFR § 23.20(e)].
d) The information source does not reside with the center.
e) The center did not originate and does not have a right to disclose the information, unless required by law.
f) Other authorized basis for denial under the Texas Public Information Act.

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.

K.2 Corrections

[1] If an individual requests correction of information originating with the TxFC 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.

K.3 Appeals

[1] The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for corrections are denied by the TxFC 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.

K.4 Complaints

[1] If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

a) Is exempt from disclosure,
b) Has been or may be shared through the ISE,
    1) Is held by the TxFC and
    2) Allegedly has resulted in demonstrable harm to the complainant,

The center will inform the individual of the procedure for submitting and resolving such complaints. Complaints will be received by the center's Privacy Officer or designee at the following address: txfcprivacy@txdps.state.tx.us. The Privacy Officer or designee 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 or designee 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 or 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.

[2] To delineate protected information shared through the ISE from other data, the TxFC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

L. Security Safeguards

[1] The TxDPS Intelligence & Counterterrorism Division's Facility Security Officer is designated and trained to serve as the TxFC's security officer.

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

[3] The TxFC 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.

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

[5] Access to TxFC 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.

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

[7] The TxFC will utilize watch logs to maintain audit trails of requested and disseminated information.

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

[9] The TxFC will follow the data breach notification specified in Texas Business and Commerce Code Section 521.053, to the extent that it applies.

M. Information Retention and Destruction

[1] All applicable information will be reviewed for record retention (validation or purge) by the TxFC at least every five years, as provided by 28 CFR Part 23.

[2] When information has no further value or meets the criteria for removal according to the TxFC's retention and destruction policy as provided by Texas Government Code Chapter 441, it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

[3] The TxFC 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.

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

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

[6] A record of information to be reviewed for retention will be maintained by the TxFC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

N. Accountability and Enforcement

N.1 Information System Transparency

[1] The TxFC will be open with the public in regard to information and intelligence collection practices when such openness will not jeopardize ongoing criminal investigative activities. The center's privacy policy will be provided to the public for review, made available upon request, and posted on the TxDPS Web site at: http://www.txdps.state.tx.us/

[2] The TxFC's 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 center. The Privacy Officer can be contacted at txfcprivacy@txdps.state.tx.us.

N.2 Accountability

[1] The audit log of queries made to the TxFC will identify the user initiating the query.

[2] The TxFC will maintain an audit trail of accessed and disseminated information. An audit trail will be kept for a minimum of one year of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

[3] The TxFC 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 Privacy Officer of the center.

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

[5] The TxFC will undergo an annual audit and inspection of the information contained in the TxFC's criminal intelligence systems and its compliance with this Privacy Policy. The audit will be conducted by the TxFC Privacy Officer. 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. The audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the center's information and intelligence system(s). The TxFC is also subject to peer audits as a component of the Texas Fusion Center Policy Council (TFCPC), as described in the TFCPC Umbrella Privacy Policy.

[6] The TxFC's Privacy Officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will recommend appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations. The Privacy Officer will recommend these changes to the TxFC Director, who will update this policy as necessary.

N.3 Enforcement

[1] If center 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 TxFC Director will:

a) Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.
b) Apply administrative actions or sanctions as provided by TxDPS personnel policies contained in the TxDPS General Manual, Chapter 7A.
c) If the authorized user is from an agency external to the TxDPS, 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.
d) Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

[2] The TxFC 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.

O. Training

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

a) All assigned personnel of the center.
b) Staff in other public agencies or private contractors providing services to the center.

[2] The TxFC 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.

[3] The TxFC's privacy policy training program will cover:

a) Purposes of the privacy, civil rights, and civil liberties protection policy.
b) Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained by the center.
c) Originating and participating agency responsibilities and obligations under applicable law and policy.
d) How to implement the policy in the day-to-day work of the user, whether a paper or systems user.
e) The impact of improper activities associated with infractions within or through the agency.
f) Mechanisms for reporting violations of center privacy protection policies and procedures.
g) The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

Appendix A: Terms and Definitions

The following is a list of primary terms and definitions used throughout this template. These terms may also be useful in drafting the definitions section of the center's privacy policy.

Access—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.

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.

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.

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.

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.

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.

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.

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.

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

The eight FIPs are:
Collection Limitation Principle
Data Quality Principle
Purpose Specification Principle
Use Limitation Principle•
Security Safeguards Principle
Openness Principle
Individual Participation Principle
Accountability Principle

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.

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.

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).

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.

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.

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.

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

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

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 center 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.
Protected Information—Protected information may include information about individuals and organizations that is subject to information privacy or other legal protections by law, including the U.S. Constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and tribal constitutions; and applicable state, local, and tribal laws, ordinances, and codes. Protection may be extended to other individuals and organizations by fusion center or other state, local, or tribal agency 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 center's information.
Media organizations.
Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the center or participating agency.
Public does not include:
Employees of the center or participating agency.
People or entities, private or governmental, who assist the center in the operation of the criminal justice information system.
Public agencies whose authority to access information gathered and retained by the center is specified in law.
Public Access—Relates to what information can be seen by the public; that is, information whose availability is not subject to privacy interests or rights.
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 center's control and which is exempt from disclosure and not disclosed to the individual to whom the information pertains.
Retention— Retention refers to the storage and safeguarding of protected information about individuals and organizations retained in furtherance of the TxFC's analytical mission. This includes but is not limited to terrorism-related information—including homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland.
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.
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, cyberattacks, 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 center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

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

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

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 center's information and intelligence databases and resources for lawful purposes.

Appendix B: Federal Laws Relevant to Seeking, Retaining, and Disseminating Justice Information

Excerpt from
U.S. Department of Justice's (DOJ's) Privacy, Civil Rights, and Civil Liberties Policy Templates for Justice Information Systems

The U.S. Constitution is known as the primary authority that applies to federal as well as state, local, and tribal (SLT) agencies. State constitutions cannot provide fewer privacy and other civil liberties protections than the U.S. Constitution but can (and many do) provide enhanced privacy and other civil liberties protections.

Civil liberties protections are primarily founded in the Bill of Rights. They include the basic freedoms, such as free speech, assembly, and religion; freedom from unreasonable search and seizure; due process; etc. The relationship of these fundamental rights to the protection of privacy, civil rights, and other civil liberties in the Information Sharing Environment is explored in a key issues guidance paper titled *Civil Rights and Civil Liberties Protection*, which is available on the Program Manager (PM) for the Information Sharing Environment (PM-ISE) Web site at www.ise.gov.

Statutory civil rights protections in the U.S. Constitution may, in addition, directly govern state action. These include the Civil Rights Act of 1964, as amended; the Rehabilitation Act of 1973; the Equal Educational Opportunities Act of 1974; the Americans with Disabilities Act; the Fair Housing Act; the Voting Rights Act of 1965; and the Civil Rights of Institutionalized Persons Act.

Federal laws, Executive Orders, regulations, and policies directly affect agencies'/centers' privacy policies. While SLT agencies may not be generally bound directly by most statutory federal privacy and other civil liberties protection laws in the information collection sharing context, compliance may be required **indirectly** by funding conditions (e.g., 28 CFR Parts 20, 22, and 23 or the Health Insurance Portability and Accountability Act [HIPAA]); operation of the Commerce Clause of the U.S. Constitution (e.g., Electronic Communications Privacy Act of 1986); or a binding agreement between a federal agency and an SLT agency (e.g., a memorandum of agreement or memorandum of understanding). Where relevant or possibly relevant, agencies/centers are advised to list these laws, regulations, and policies, noting those that may potentially affect the sharing of information, including sharing terrorism-related information in the Information Sharing Environment.

The development of a privacy, civil rights, and civil liberties policy is primarily designed for center personnel and authorized users to ensure that they are aware of the legal and privacy framework within which they and the center must operate. If the applicability and requirements of various laws, regulations, or sharing agreements are not spelled out or referenced in an center privacy policy, staff and user accountability is greatly diminished, mistakes are made, privacy violations occur, and the public's (and other

agencies') confidence in the ability of the center to protect information and intelligence is compromised. When staff members know the rules through sound policy and procedure communicated through ongoing training activity, information sharing is enhanced.

Following is a partial listing of federal laws that should be reviewed when developing a privacy policy for a justice information system. The list is arranged in alphabetical order by popular name.

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

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

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

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

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 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

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

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

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat. 272