WEST TEXAS HIDTA

INVESTIGATIVE SUPPORT CENTER

PRIVACY POLICY

Table of Contents

A **PURPOSE**

A.1. PURPOSE STATEMENT

A.1.1. The purpose of this policy is to provide relevant state, local and private sector partners with guidelines, standards, policies and procedures for the operation of the West Texas HIDTA Investigative Support Center (ISC). This policy is designed to bring about an equitable balance between the privacy, civil rights, and civil liberties of individuals and organizations and the needs of law enforcement to collect and disseminate criminal justice information and intelligence on persons or organizations involved in criminal activity. This Privacy Policy embraces the eight privacy design principles or "Fair Information Principles" (see definition in Appendix A) developed by the Organization for Economic Co-operation and Development (OECD) and contained within its "Guidelines on the Protection of Privacy and Trans border Flows of Personal Data," and shall be used to guide the policy wherever applicable.

A.2. MISSION STATEMENT

A.2.1. The West Texas HIDTA Intelligence Initiative is created to provide a seamless intelligence support system for the narcotics and other law enforcement operational initiatives and units in the Region. It is a multi-agency system led by the El Paso County Sheriff's Office and co-managed with the FBI and DEA that will provide timely and actionable information to the officer, agent, and/or intelligence analyst.

A.2.2. The West Texas HIDTA Intelligence Initiative includes the West Texas HIDTA Investigative Support Center (ISC) which will provide operational units with a seamless intelligence support system. The structure and policies of the entire initiative comply with the federal General Counter Drug Intelligence Plan (GCIP). The full-time participants of the ISC include:

El Paso County Sheriff's Office (EPCSO)
Federal Bureau of Investigation (FBI)
Drug Enforcement Administration (DEA)
El Paso Police Department (EPPD)
Texas National Guard (TNG)

The ISC service region includes all designated counties in West Texas. The EPPD, BP, ICE, and TDPS Intelligence units in the El Paso area, while not collocated, also support the ISC in their mission. Midland and Ector county law enforcement agencies are significant participants and contributors as well.

A.2.3. De-confliction services provided by the West Texas HIDTA ISC will improve officer safety issues and maximize the efficient use of our resources. As a central hub for LEA intelligence sharing and dissemination, the intelligence

initiative will directly improve the efficiency and effectiveness of law enforcement organizations with their efforts in disrupting and dismantling drug trafficking organizations. The ISC will provide data base query, de-confliction, pointer index services and a full range of tactical and strategic analytical support and reports. This will include LPR, Pole Cam surveillances, Data Analysis Services, Gang intelligence, Cell Phone Mining, and surge operation support. It will also develop target packages to provide to the operational units for investigative development. All Texas HIDTAs support the Texas Joint Crime Information Center (JCIC).

A.2.4. The Intelligence Initiative also consists of a Gang Intelligence unit located within the ISC. This unit provides analytical and operational support to the FBI Safe Streets Gang Task Force as well as to all other Federal, State, and Local Law Enforcement gang units assigned to the Texas Anti-gang (TAG) center located in El Paso, Texas.

B **POLICY APPLICABILITY AND LEGAL COMPLIANCE**

B.1. COMPLIANCE AND GOVERNANCE

B.1.1. The West Texas HIDTA implements these operating policies and procedures to govern the Investigative Support Center (ISC) and *Participating Agencies* in the collection, submission, analysis, query, dissemination, retention, and security of *Records* in the various electronic intelligence information systems maintained by the ISC. The purpose of this activity is to support the goals of the ISC, which are:

a) strengthen Information and Intelligence Sharing and Support to all law enforcement agencies in the West Texas area of responsibility (AOR);

b) disrupt and dismantle Drug Trafficking Organizations;

c) stop the flow of illegal narcotics into the United States;

d) provide deconfliction services to all area law enforcement officers and agents.

B.1.2. All ISC personnel, *Participating Agency* personnel, personnel providing information technology services to the agency, private contractors, and other authorized users must be in compliance with applicable constitutional and statutory laws (including but not limited to those outlined in Appendix B), and this privacy policy, concerning the laws protecting privacy, civil rights, and civil liberties in the seeking, gathering, use, analysis, retention, destruction, sharing, securing and disclosure of information and intelligence to ISC personnel, governmental agencies and participating justice and public safety agencies, as well as to private contractors and the general public.

B.1.3. 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 privacy rights of individuals, civil rights and civil liberties.

B.1.4. The ISC will provide a printed or electronic copy of this policy to all ISC and non-agency personnel who provide services and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the provisions it contains.

B.1.5. The ISC has adopted internal operating procedures and policies that are in compliance with applicable U.S. and Texas Constitutional and statutory laws (see Appendix B for a list of State and Federal laws) protecting privacy, civil rights, and civil liberties in the gathering, use, analysis, retention, destruction, sharing, securing and disclosure of information.

B.1.6. The ISC will provide a printed or electronic copy of this policy upon request by any person, corporation, or organization.

B.2. PROTECTIONS DEFINED

B.2.1. The United States was created with the principles of protecting certain privileges from government intrusion as guaranteed rights, which has led to the further refining of concepts such as right to privacy that developed from case law and statutory protections from government and others overreach into a person's life. The ISC articulates and defines the intention and commitment to protect:

a) individual "privacy" which refers to individuals' interest in preventing the inappropriate collection, use and release of personally identifiable information;

b) against the use of inappropriate or illegal means used to gather personal data and personal conduct and the inappropriate release of information that causes embarrassment, shame or loss;

c) personal identifiable information which is one or more pieces of information, such as personal characteristics and unique identifiers, that when considered together or when considered in the context of how it is present or how it is gathered is sufficient to specify a unique individual;

d) civil rights, which are those fundamental freedoms and privileges guaranteed by the 13th and 14th Amendments to the U.S. Constitution and by subsequent acts of Congress, including civil liberties, due process, equal protection of the laws, and freedom from discrimination; and,

e) civil liberties as those fundamental individual rights, such as freedom

of speech and religion, protected by law against unwarranted governmental interference.

B.2.2. The ISC intends to establish a foundation for protection by acknowledging these protections, by providing transparency in establishing processes and procedures for operation, by ensuring adequate training and understanding for users and by having sufficient audit and oversight to ensure compliance.

C. GOVERNANCE AND OVERSIGHT

C.1. Primary responsibility for the operation of the ISC, its justice systems, operations, and oversight of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, securing or disclosure of information; and the enforcement of this policy is assigned to the ISC Manager.

C.2. This policy was developed by the ISC Manager and reviewed by the West Texas HIDTA Executive Director and the West Texas HIDTA Executive Board.

C.3. The West Texas HIDTA will provide a printed or electronic copy of this policy upon request to any person, corporation, or organization making such a request.

D. DEFINITIONS

D.1. The primary terms and definitions used in this policy are set forth in Appendix A.

E. INFORMATION

E.1. GUIDING STATUTES AND POLICY APPLICABILITY

E.1.1. The West Texas HIDTA investigative support center acknowledges the application of certain law, statutes and policies which may affect the Mission and Goals of the ISC and its operation, including United States Constitution, United States Federal Code of Regulations - 28 CFR Part 23, regarding intelligence information systems; the Texas Constitution, Texas Code of Criminal Procedure Chapter 61, and amendments contained in Senate Bill 418 81st Legislature, regarding Gang Intelligence and 28 CFR standards; Chapter 421 of the Texas Government Code, regarding the Department of Public Safety and the collection of terrorist and Homeland Security information; and Chapter 552 of the Texas Government Code, regarding open government.

E.1.2. The development of ISC processes and operating procedures will be guided by privacy design principles from *Fair Information Principles;* which shall also serve to guide personnel in the application of guiding statutory authority. These principles are:

E.1.2.1. *Purpose Specification* – Define agency purposes for information to help ensure agency uses of information are appropriate.

E.1.2.2. *Collection Limitations* – Limit the collection of personal information to that required for the purposes intended.

E.1.2.3. *Data Quality* – ensure data accuracy.

E.1.2.4. *Use Limitation* – Ensure appropriate limits on law enforcement use of personal information.

E.1.2.5. *Security Safeguards* – Maintain effective security over personal information.

E.1.2.6. *Openness* – Promote a general standard of openness and transparency regarding practices, process and policy regarding collecting, disseminating and archiving personal information.

E.1.2.7. *Individual Participation* – Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency.

E.1.2.8. *Accountability* – Identify, train and hold participating personnel accountable for adhering to ISC information quality and privacy policy standards.

E.2. LIMITIATIONS & STATEMENT OF INTENT

E.2.1. The ISC is operated and managed by the West Texas HIDTA as an investigative support center. The ISC has the potential to come into contact with a broad scope of both public and private information and data. The ISC will not seek, collect, analyze, or disseminate information or data that does not support the identified goals of law enforcement, disrupt or prevent crime, terrorism or violent acts.

E.2.2. The ISC will prohibit its employees and will not seek or retain, and information-originating agencies hereby agree not to submit, 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 races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientations.

E.2.3. The ISC will only seek, retain, analyze or disseminate information that:

a) is based on a criminal predicate or possible threat to public safety; 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 conduct or activity; or

c) 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

d) is useful in a crime analysis or in the administration of criminal justice and public safety; and

e) is obtained from a reliable source and is verifiable or limitations on the quality of the information are identified; and

f) was collected in a fair and lawful manner.

E.3. INFORMATION IN GENERAL

E.3.1. The ISC 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*s (SAR).

E.3.2. This policy applies to protected information about all individuals and organizations (as expressly included by law or policy) obtained by the ISC 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 ISC) will not be subject to the provisions of this policy.

E.4. INFORMATION SYSTEMS

E.4.1. The ISC, thru its participating agencies, will have access to and utilize:

a) a Records Management System (RMS) for the collection and reporting of certain crimes and incidents.

b) a criminal investigative reporting system for the case management of criminal investigations.

c) various government, public, institutional, private and commercial databases providing information to augment existing Records and information.

E.4.2. The ISC may collect, manage and analyze information related to the collection of *Suspicious Activity Report*s (SAR).

E.4.3. The ISC may also have access to certain surveillance systems that allow the visual electronic surveillance of public areas that are protected in the region.

E.4.4. The ISC will only utilize databases and contract 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.

E.5. PUBLIC SURVEILLANCE SYSTEM

E.5.1. The ISC may access data from 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. Unless installed pursuant to an ongoing criminal investigation and appropriate court order, no such system will be placed or installed to view an area where there is a reasonable expectation of privacy by any member of the general public. 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.

E.5.2. Any Data or images stores or retained by the ISC through recording of or from the use of any of these systems may only be retained for a period of 24 months unless specifically identified by *Reasonable Suspicion* standards as related to criminal activity. Without such correlation or analysis, all data or images must be purged and a permanent log or record kept identifying the person and method used for purging. Any query or request for dissemination of stored data form these systems by any persons except for furthering an authorized criminal investigation will be refused. Permanent logs regarding any request for dissemination and any such dissemination or refusal: along with the method and identification of the person making routine destruction will be available upon request to the ISC.

E.6. TIPS, LEADS AND SUSPICIOUS ACTIVITY REPORTING

E.6.1. The ISC may access unsubstantiated or uncorroborated information or data from inside or outside the agency that alleges or indicates some form of possible criminal activity. This type of information or data is generally referred to as *tips and leads* and is sometimes referred to as *suspicious activity report* (SAR). However, SAR information should be viewed, at most, as a subcategory of *tips and leads* data.

E.6.2. The ISC may receive, collect, analyze, evaluate, retain and secure *tips and leads* and *suspicious activity report* (SAR) information. Moreover, the ISC may be called upon to:

a) identify trends and patterns of potential events which are threats to our nation, state or jurisdiction and its citizens to improve the effectiveness of the criminal justice community response to such events and bring closure to events and information which do not pose such threats;

b) in accordance with the understanding that information may not

immediately meet a *Reasonable Suspicion* standard and thus not be compliant with 28 CFR, limit the dissemination of such raw information that has not been analyzed or is not able to be labeled or elevated to finished criminal intelligence, using the same (or a more restrictive) access or dissemination standard that is used for data the rises to the level of *Reasonable Suspicion* (For example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information);

c) professionally analyze and evaluate to determine if the record can be elevated to meet 28 CFR guidelines as finished intelligence by "reasonable suspicion" standards and that the analysis conclusion is supported by relevant documentation before it can be considered for submission to an intelligence file or Records system;

d) retain and secure in an intelligence file, information elevated to meet 28 CFR guidelines as finished intelligence, 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;

e) delete if the basis for submission includes only political, religious, or other First Amendment activities or the expression of personal opinions;

f) delete regardless of the criminal activity involved, if the Authorized User making an assessment has good reason to believe that the supporting information was illegally obtained;

g) delete unless it:

(1) serves to identify an individual or organization that is involved in terrorism; or

(2) shows a nexus to violating a criminal law of the State, the United States, or any jurisdiction in the United States that would be a violation of a criminal law of Texas; or

(3) meets the legal definition of gang activity under State or federal law; or,

(4) poses a clear and present threat to public order and safety.

E.6.3. The ISC will enforce internal policies that will automatically purge tips,

leads, or SAR *Record*s which are not acted upon or evaluated within 5 years.

E.6.4. The ISC will enforce policies regarding the purging of personal identifying information which has expired according to 28 CFR standards (5 year retention or purge unless validated for an additional retention period) or deemed as not meeting minimum standards for accuracy or submission.

E.6.5. The report validation processes may include research of suspect information and personal identifying information to support or refute criminal activity. These validation processes will necessarily involve contrast and comparison from other private and public data sources that attempt to identify, establish or validate reports of suspected persons or events. There should be no merging of personally identifying data from other data sources that establish identity or criminal behavior unless multiple criteria are validated as matching.

E.6.6. While the ISC may store *Record*s supported by documented information, it also may contain anonymous reports and potential erroneous reports. Therefore, it is not designed to provide a *Record* upon which to base an official action. The ISC merely identifies that information was received which must be validated to assess the information supporting the *SAR* record. While this supporting information may be used to justify official action, the tip, lead or *SAR* record itself may not be used to provide:

a) probable cause for a warrantless arrest;

b) probable cause in an affidavit for an arrest or search warrant;

c) proof in a court procedure for enhancing the penalty for a crime; or,

d) used for background or employment application purposes.

E.6.7. For all tip, lead, and SAR information, the ISC will:

a) Allow access to or disseminate the information using the same access or dissemination standard that is used for criminal intelligence information.

b) 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.6.8. The ISC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing the information through the Information Sharing Environment.

E.7. CRIMINAL INTELLIGENCE SYSTEMS

E.7.1. A criminal intelligence file consists of stored information on the activities and associations of:

a) Individuals who:

(1) based upon reasonable suspicion are suspected of being or having been involved;

(2) are in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts;

(3) based upon reasonable suspicion are suspected of being or having been involved in criminal activities with known or suspected crime figures.

b) Organizations, business and/or groups which:

(1) based upon reasonable suspicion, are suspected of being or having been involved in the actual or attempted planning, organizing, threatening, financing, or commission of criminal acts; or

(2) that based upon reasonable suspicion are suspected of being or having been illegally operated, controlled, financed or infiltrated by known or suspected crime figures.

E.7.2. Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable suspicion as defined in 28 CFR, Part 23 entitled "Criminal Intelligence Operating Systems, and in accordance with United States Constitution, the Texas Constitution, Texas Code of Criminal Procedure Chapter 61, and amendments contained in Senate Bill 418 81st Legislature, regarding Gang Intelligence and 28 CFR standards; Chapter 421 of the Texas Government Code, regarding the Department of Public Safety and the collection of terrorist and Homeland Security information; Chapter 552 of the Texas Government Code, regarding open government. (See also Appendix B – State and Federal Law).

E.7.3. The primary purposes of these criminal intelligence systems are receipt, storage, and sharing of criminal intelligence information.

E.7.4. The goal of these criminal intelligence systems is to improve the effectiveness of the criminal justice community by providing for the timely exchange of documented and reliable information.

E.7.5. Any person involved in the submission, query, dissemination, or review of any supported or maintained intelligence systems must be an *Authorized User*

with access approved by their respective agency head or designee and the ISC Manager or designee.

E.7.6. The submission or retention of information supporting any *Record* must comply with the intelligence guidelines set forth in 28 CFR, including each of the following:

a) An intelligence record must be supported by documentation that contains information relevant to an individual criminal member (based on proper identification criteria) and/or a criminal street gang or organization (based on proper criminal predicate).

b) No political, religious, or other First Amendment activities or the expression of personal opinions may be used as a valid basis for inclusion in any supported intelligence system, unless the activity satisfies criminal predicate by:

(1) clearly violating a criminal law of the State, the United States, or any jurisdiction in the United States that would be a violation of a criminal law of Texas;

(2) meeting the legal definition of gang activity under State law; or

(3) posing a clear and present threat to public order and safety.

c) Regardless of the criminal activity involved, no *Record* may be retained or submitted if the submitting agency or authorized user has good reason to believe that the supporting information was illegally obtained.

d) Any submitted information identifying an individual or a criminal organization must meet the criminal predicate requirements of reasonable suspicion identified in 28 CFR Part 23 and the criminal activity must represent a significant and recognized threat to the public and:

(1) Are either undertaken for the purpose of seeking illegal power or profits or pose a threat to the life and property of citizens; and

(2) Involve a significant degree of permanent criminal organization; or

(3) Are not limited to one jurisdiction.

E.7.8. The ISC and any Participating Agency may not use data obtained from the

ISC to populate another intelligence system or other searchable database or to populate *another agency's* databases.

E.7.9 All other criminal intelligence systems or future intelligence systems will comply with similar ISC criminal intelligence policies.

E.8. NATURE OF INFORMATION

E.8.1. In order to accurately classify and categorize information and intelligence, the ISC will delineate each *Record* with the nature of information, i.e., *suspicious activity report, tip and lead,* criminal history, intelligence information, criminal case report, conditions of supervision, case management, et cetera.

E.9. INFORMATION CLASSIFICATION

E.9.1. The ISC will classify each *Record* in order to protect sources, investigations, and individual's rights to privacy, as well as to provide a structure that will enable the ISC to control access to intelligence.

E.9.2. Information received by *Participating Agencies* or other agencies with information classifications attached to them will be reviewed by the ISC Manager or designee, who will assign the appropriate classification; however, the ISC classification will never be lower than the classification given by *Participating Agencies* or other agencies. All classifications or re-classifications must be approved by the ISC Manager or designee.

E.9.3. Criminal intelligence information is classified according to the following system:

a) Sensitive - intelligence files include those that contain information that could adversely affect an on-going investigation, create safety hazards for officers, informants, or others and/or compromise their identities. Restricted intelligence may only be released by approval of the ISC Manager to authorized law enforcement agencies with a need and a right to know.

b) Confidential - intelligence that is less than sensitive intelligence. It may be released to law enforcement personnel when a need and a right to know have been established by the ISC Manager or designee.

c) Unclassified - intelligence contains information from the news media, public records, and other sources of a topical nature. Access is limited to individuals conducting authorized investigations that necessitate this information.

E.10. DISSEMINATION OF INFORMATION

E.10.1. The ISC will ensure that an intelligence record is directly disseminated only to an authorized user by: employing safeguards, including a special role-

based user ID and initial password; and will only disseminate a *Record* to a *Participating Agency* through a proper query by an *Authorized User* from an authorized computer terminal. Verbal disseminations to any person will require that the ISC *Authorized User* reasonably identify the requestor and the *Need to Know* and *Right to Know*.

E.10.2. The ISC will label a dissemination of any *Record* or information with the following metadata:

a) date and time the information was originally received;

b) the nature of the information, i.e., *suspicious activity report, tip and lead,* criminal history, intelligence information, criminal case report, conditions of supervision, case management, external database source, et cetera;

c) the title and contact information for the person to whom questions regarding the information should be directed.

E.10.3. All information maintained in the *Record* will be released to an authorized user who makes a proper query, without any special restriction on its dissemination beyond the general requirements of 28 CFR, unless the author or entity has specified restrictions.

F. ACQUIRING AND RECEIVING INFORMATION

F.1. The ISC will ensure that information gathering (acquisition) and access and investigative techniques used by the ISC, participating agencies, and information-originating agencies will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to:

F.1.1. 28 CFR Part 23, regarding criminal intelligence information

F.1.2. 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).

F.1.3. Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) *National Criminal Intelligence Sharing Plan* (NCISP).

F.1.4. Constitutional provisions and administrative rules, as well as regulations and policies that apply to multijurisdictional intelligence and information databases.

F.2. *Participating Agencies* that access the ISC information or share information with

the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

F.3. The ISC 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.

F.4. The ISC will not directly or indirectly receive, seek, accept, or retain information from:

F.4.1. 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.

F.4.2. An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

F.5. Information-gathering and investigative techniques used by the ISC will and those used by originating agencies should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

G. INFORMATION QUALITY ASSURANCE

G.1. The ISC is responsible for the quality and accuracy of the data accessed by the Center. Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the ISC. In order to maintain the integrity of the ISC, any information obtained through the center will be independently verified with the original source from which the data was extrapolated and subjected to review, analysis, and scrutiny to derive its meaning and value, and that the appropriate metadata is affixed to each *Record* delineating the date of receipt, nature, category, and classification before the information is qualified for use. Additionally, information will only be merged with other information about the same individual or organization when the applicable standard has been met as described in Section I, Merging Records. *Participating Agencies* and individual users are responsible for compliance with respect to use and further dissemination of such information and the purging and updating of the data. Any *Participating Agency* submitting information to the ISC remains the owner of that information and is responsible for its accuracy and must ensure the quality of each *Record* submitted by the agency and the quality of the information supporting that *Record*. After submitting information about a suspected individual criminal member to the ISC, that agency must maintain all supporting documentation for as long as: The *Record* is retained; or a legal challenge to the *Record* is pending.

G.2. The ISC will also conduct periodic data quality reviews of information it originates and receives, and will 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).

G.3. The ISC will evaluate all data, including, but not limited to the ISC data, and any *Participating Agency* data, at a minimum of every five years from the date of receipt, for determination of relevance and continuing criminal predicate for retention. *Record*s that fail to meet these evaluation criteria will be purged. The ISC will keep no record of any individual *Records* purged but will identify the number of *Record*s purged. The ISC will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when it learns that the information lacks adequate context or is erroneous, misleading, obsolete, or otherwise unreliable.

G.4. The ISC will use written or electronic notification to inform the originating entity, *Participating Agency*, another agency, or a database when information previously obtained or provided by the entity 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.

G.5. The ISC 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

H.1. Information acquired or received by the ISC 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.

H.2. Information subject to collation and analysis is information as defined and identified in Section H.

H.3. Information acquired or received by the ISC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:

H.3.1. Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the center.

H.3.2. 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.

H.4. The ISC requires that all analytical products be reviewed and approved by a supervisor or, where release is required under the Freedom of Information Act or the Texas Open Records Act, the ISC Manager to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. MERGING RECORDS

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

I.2. If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the ISC 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

J.1. Credentialed, role-based access criteria will be used by the ISC, as appropriate, to control:

J.1.1. The information to which a particular group or class of users can have access based on the group or class.

J.1.2. The information a class of users can add, change, delete, or print.

J.1.3. To whom, individually, the information can be disclosed and under what circumstances.

J.2. The ISC policy for the dissemination of information is described and defined in Section E.10.

J.3. Access to or disclosure of *Record*s retained by the ISC 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 safety, 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.

J.4. *Participating Agencies* or other agencies external to the ISC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

J.5. Information gathered or collected and *Record*s retained by the ISC 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.

J.6. Information gathered or collected and *Record*s retained by the ISC 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.

J.7. Information gathered or collected and *Record*s retained by the ISC may not be accessed or disclosed to a member of the public under certain circumstances as described and defined in Section K.1.

J.8. An audit trail will be maintained by the ISC when it disseminates an intelligence record. An audit trail will be kept for a minimum of 2 years and will include the following information about the dissemination:

J.8.1. the suspect and personally identifying information released,

J.8.2. the date and time of the query or other related access transaction; and

J.8.3. the name of the individual and agency requesting the *Record*.

J.9. A *Participating Agency* who receives and further disseminates intelligence information will create and maintain a dissemination log. The log created by the agency must:

J.9.1. comply with the principles of 28 CFR; and

J.9.2. be maintained for as long as the information supports a current *Record*.

J.10 A *Participating Agency* will permit indirect access to an intelligence record by:

J.10.1. dissemination typically through personal intervention; and

J.10.2. using a communications network only if the network involves an encrypted radio broadcast or other reasonably secure transmission method, except in the case of an emergency, when necessary to avoid imminent danger to life or property.

J.11. There are several categories of *Record*s that will ordinarily not be provided to the public:

J.11.1. Records required to be kept confidential by law are exempted from disclosure requirements under Chapter 552, Texas Government Code.

J.11.2. 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.

J.11.3. 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.

J.11.4. Investigatory records of law enforcement agencies that are exempted from disclosure requirements under Texas Government Code § 552.108. However, certain law enforcement records must be made available under Chapter 552, Texas Government Code.

J.11.5. 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.

J.11.6. Protected federal, state, local or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission, unless it is required to be disclosed under the Texas Public Information Act**.**

J.11.7. A violation of an authorized nondisclosure agreement between the ISC and any other party.

J.12. The ISC will archive all intelligence products that are received and then used to further refine ISC intelligence or are quoted or used to support disseminated intelligence products that are created. All ISC analytical products that use another agency intelligence product information or analysis will be noted in the release of the ISC product along with the value assigned by that product to the information. The ISC will archive all intelligence products that are created and disseminated from the ISC.

J.13. Information gathered and records retained by the ISC will not be:

J.13.1. Sold, published, exchanged, or disclosed for commercial purposes;

J.13.2. 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; or

J.13.3. Disseminated to persons not authorized to access or use the information.

J.13.4. The ISC 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. SECURITY SAFEGUARDS

K.1. The ISC will operate in a secure facility protected from external intrusion. The ISC will utilize secure internal and external safeguards against network intrusions. Access to the ISC databases from outside the facility will be allowed only over secure networks.

K.2. The ISC will secure tips, leads and SAR information in a separate repository system using security procedures and policies that are the same as or like those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

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

K.4. The ISC will limit data access to those individuals who have been selected, approved, and trained accordingly. Access to information contained within the ISC and its systems will be granted only to law enforcement agency personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by the West Texas HIDTA Executive Board. Each individual user must complete an Individual User Agreement in conjunction with training.

K.5. Once the requirements described and defined in Section K.4 have been satisfied the ISC Manager or designee may accept a user and provide a role-based user ID and password necessary for the individual to access any intelligence system as an Authorized User through an authorized computer terminal.

K.6. Intelligence system(s) passwords will periodically expire, and the Authorized User must then create a new password.

K.7. Access to the ISC data repositories from outside the facility will only be allowed over secure networks, encrypted radio broadcast or other reasonably secure transmission method, except in the case of an emergency, when necessary to avoid imminent danger to life or property.

K.8. The ISC will utilize logs to maintain audit trails of requested and disseminated information and will identify the user initiating the query.

K.9. The ISC will maintain logs of all access through portals and usage of the center's data repositories.

K.10. The ISC will maintain logs of the physical access through the center's access control system.

K.11. The ISC will conduct periodic audits of the watch logs to ensure that security and the integrity of the data and facility is maintained.

K.12. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

K.13. The ISC and any *Participating Agency* shall comply with the security provisions of the Criminal Justice Information Services (CJIS) Security Policy. The agency shall provide for reasonable:

K.13.1.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;

K.13.2.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; and

K.13.3.Personnel security, including access allowed only to:

a) law enforcement, military acting under Title 32 or criminal justice personnel; or

b) technical or maintenance personnel who have been subject to character or security clearance.

K.14. Compromising a user ID or password is a serious violation of system security.

K.15. A Participating Agency must notify the Administrator when an individual is terminated or reassigned and is, therefore, no longer eligible to continue as an authorized user; comply with ISC quality control, inspection, audit, and validation procedures.

L. INFORMATION RETENTION AND DESTRUCTION

L.1. All applicable information will be reviewed for record retention (validation or purge) by the ISC at least every five (5) years, as provided by 28 CFR Part 23.

L.2. When information has no further value or meets the criteria for removal according to the ISC retention and destruction policy it will be purged, destroyed, and deleted or returned to the submitting (originating) agency.

L.3. The ISC 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.

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

L.5. Notification of proposed destruction or return of *Record*s may or may not be provided to the originating agency by the ISC, depending on the relevance of the information and any agreement with the originating agency.

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

M. ACCOUNTABILITY AND ENFORCEMENT

M.1. INFORMATION SYSTEM TRANSPARENCY

M.1.1. The ISC will be open with the public regarding information and intelligence collection practices.

M.1.2. The ISC will provide a printed or electronic copy of this policy upon request by any person, corporation, or organization.

M.1.3. The ISC will post a copy of this policy on the center's website at www.westtexashidta.org.

M.2. ACCOUNTABILITY

M.2.1. The ISC will maintain logs of all access as described and defined in Section K.8.

M.2.2. The ISC 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 of all systems as described and defined in Section K. These audits will be mandated at least annually and a record of the audits and requests for information for specific purposes and of what information is disseminated to each person in response to the request will be maintained for a minimum of 3 years by the Administrator of the center.

M.2.3. The ISC may undergo an audit and inspection of the information contained in the ISC criminal intelligence systems and its compliance with this Privacy Policy. The audit will be conducted by the ISC Manager. The Manager 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).

M.2.4. Each *Participating Agency* may be subject to an audit by an ISC representative of submitted data and compliance with the Privacy Policy. The ISC may specially inquire into any demonstrated failure to comply with these policies and procedures.

M.2.5. A *Participating Agency* has an affirmative responsibility to immediately report the loss or mishandling of any personal or sensitive information to the ISC Manager, or in the Managers absence the Deputy Manager.

M.2.6. The ISC personnel or other authorized users shall report errors and violations or suspected violations of ISC policies relating to protected information to the ISC Manager.

M.2.7. The ISC requires all personnel to agree to comply with the provision of this policy in writing, as described and defined in Section B.1.4.

M.2.8. The ISC Manager or designee 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 ISC Manager will recommend these changes to the West Texas HIDTA Executive Board for review and final approval.

M.3. ENFORCEMENT

M.3.1. If an authorized user or *Participating Agency* materially violates any term of its User Agreement or is found to be in noncompliance with the provisions of this policy and procedures, the authorized user or agency risks suspension of its access to intelligence information.

M.3.2. A suspension may occur immediately and without prior notice. Suspension may be followed by termination if deemed necessary by the Administrator.

M.3.3. The Administrator shall send to the *Participating Agency* a notice within 10 working days describing:

a) the date the Administrator has suspended or proposes to terminate service;
b) the alleged violation of the User Agreement; and,
c) whether the alleged violation is criminal or under investigation.

M.3.4. If the ISC Manager or designee determines the alleged violation to be criminal in nature, an investigation shall be initiated, the results of which shall be forwarded to the appropriate authority for criminal prosecution.

M.3.5 If the authorized user is from an agency external to the ISC, 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.

M.3.6 The ISC reserves the right to restrict the qualifications and number of personnel having access to center information to any participating agency or participating agency personnel violating the ISC's privacy policy.

N. TRAINING

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

N.1.1. all personnel assigned to the center; and,

N.1.2. staff in other public agencies or private contractors providing services to the center.

N.2. The ISC 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 (ISE).

N.3. The ISC's privacy policy training program will cover:

N.3.1. purposes of the privacy, civil rights, and civil liberties protection policy;

N.3.2. 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;

N.3.3. originating and *Participating Agency* responsibilities and obligations under applicable law and policy;

N.3.4. how to implement the policy in the day-to-day work of the user, whether a paper or systems user;

N.3.5. the impact of improper activities associated with infractions within or through the agency;

N.3.6. mechanisms for reporting violations of center privacy protection policies and procedures; and,

N.3.7. the nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

N.4. The ISC will provide training for all *Authorized Users* granted *Direct Access* to any intelligence systems in the operational aspects of the systems.

N.5. The ISC may require additional training for any user or *Participating Agency* under State training requirements or law.

O. RESERVATION AND USER AGREEMENT

O.1. Agencies may choose to exercise a written User Agreement to further define roles and responsibilities to ensure compliance with this Privacy Policy and addendum. Nothing in this Privacy Policy may be used to limit the responsibility of the ISC in pursuing efforts to satisfy its other legal rights, privileges or obligations.

APPENDIX A: TERMS AND DEFINITIONS

In this PRIVACY POLICY:

1. "**Administration of criminal justice**" means 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.

3. "**Authorized user**" means an individual designated by an agency head and authorized by the ISC Manager for direct access to intelligence systems.

4. "**Direct access**" means the action of an individual authorized user to gain direct computer access to intelligence system.

6. "**CCP** " means the Texas Code of Criminal Procedure.

7. "**28 CFR**" means Title 28, Code of Federal Regulations, Part 23.1 et seq., as promulgated by the U.S. Department of Justice, Office of Justice Programs.

8. "**Criminal intelligence**" means information, material, photographs, or data that has been evaluated to determine that it is relevant to the identification of an individual or an organization for which a proper criminal predicate exists.

9. "**Criminal justice agency**" means 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.

10. "**Criminal predicate**" means reasonable suspicion or 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.

11. "**Criminal street gang**" or "**gang**" means 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.

12. "**Criminal street gang member**" or "**gang member**" means an individual who has been identified as a member of a criminal gang through documentation supported by 28 CFR Part 23 standards.

13. "**Fair Information Principles**" are contained within the Organization for Economic Co-operation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flow 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, and Accountability Principle.

15. "**Indirect access**" means the action of an individual, who is not an authorized user, to gain indirect access to intelligence systems through an A*uthorized User* based on a *right to know and/or a need to know*.

16. "**Information quality**" means the validity, accuracy, timeliness, completeness, relevancy, importance, and reliability of information supporting an intelligence system record.

17. "**Intelligence Source Reliability**" is that 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*" and "*Unknown*" as defined by and consistent with 28 CFR Part 23 definitions.

18. "**Local entity**" means 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.

19. "**Need to know**" means the necessity to obtain or receive criminal intelligence information in the performance of an official duty or responsibility for a criminal justice agency. However, the ***Need to Know*** criteria should not be weighed solely as a method to prevent dissemination but rather as an affirmative responsibility to share information where such dissemination may improve public safety or an individual officer safety or overall effectiveness of a law enforcement agency. The **Need to Know** provision shall not prohibit the release of information where there is an imminent threat to life that mandates the release of information.

20. "**Participating Agency**" or **"Participating Agencies"** means a criminal justice agency that has entered into a User Agreement.

21. **"Personal Identifiable Information (PII)"** means one or more pieces of information, such as personal characteristics and unique identifiers, that when considered together or when considered in the context of how it is present or how it is gathered is sufficient to specify a unique individual.

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

23. “**Protected Information”** includes Personal Data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the 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 and ordinances. Protection may also be extended to organizations by **ISC** policy or state, local, or tribal law.

24. “**Record**” means information accepted by the ISC for storage and retention in an intelligence system.

25. “**Record quality**” means that the data format of any record meets all Quality Control provisions and system edits under these policies and procedures.

26. “**Reasonable Suspicion**” or criminal 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

27. “**Right to know**” means the legal authority to obtain or receive criminal intelligence information under a court order, statute, or decisional law or Lead Agency policy.

28. “**Right to Know**” shall also apply to any submitting agency as the owner of applicable submitted information permitting their access to and mandating their responsibility for applicable submitted information.

29. “**Suspicious Activity Report**” (SAR) is the 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.

30. “**Tips and Leads” Information or Data** is 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.

31. "**User Agreement**" means an agreement or written understanding executed under these policies and procedures between the West Texas HIDTA, its ISC, and a *Participating Agency*.

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

APPENDIX B: STATE AND FEDERAL LAW RELEVANT TO SEEKING, RETAINING, AND DISSEMINATING JUSTICE INFORMATION

Following is a partial listing of laws arranged in alphabetical order by popular name.

State Laws

Texas Constitution

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

Chapter 421 of the Texas Government Code, regarding the Department of Public Safety and the collection of terrorist and Homeland Security information

Chapter 552 of the Texas Government Code, regarding open government

Texas Business and Commerce Code Section 521.053, regarding data breach notification

Federal Laws

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

Criminal History Records Exchanged for Noncriminal Justice Purposes, 34 U.S.C. § 41103, United States Code, Title 34, Chapter 411, Subchapter IV, § 41103

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, Chapter 121, §§ 2701–2709, and Chapter 123, §§ 2721–2725, 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