Texas Transnational Intelligence Center

Privacy and Civil Rights Policy

May 7, 2018

I. Background

The Texas Transnational Intelligence Center (hereinafter referenced to as "TTIC" or the "Center") is a collaborative effort of the McAllen Police Department, the Hidalgo County Sheriff's Office and the Texas Department of Public Safety. Their mission is to provide resources, expertise, and/or information to the TTIC.

The TTIC project is a response from the Texas Legislature to address the increased need for timely information sharing and exchange of crime-related information among members of the law enforcement and emergency management community, and to enhance the cross-jurisdictional and multi-disciplinary prediction, prevention, protection, response, and mitigation capabilities for criminal activity facing the Deep South Texas region.

The TTIC seeks to facilitate regional data gathering and intelligence sharing to achieve its core mission:

"Provide our law enforcement partners information to aid them in their mission, while protecting individual privacy and civil rights of all citizens."

One component of the TTIC focuses on the development and exchange of criminal intelligence. This component focuses on the intelligence process where information is collected, integrated, evaluated, analyzed and disseminated.

The TTIC consists of its analysts and hosted State and Local agency staff, along with operational stakeholders, which include regional law enforcement, emergency management, fire and rescue agencies. Other supporting and benefiting stakeholders may include city and county administrations, academia, state agencies, elected officials, and critical infrastructure/key resources (CIKR) owners and operators.

The TTIC communicates with many State and Federal organizations, including the Texas Joint Crime Information Center (JCIC), the Department of Homeland Security (DHS), and the Centers for Disease Control, El Paso intelligence Center (EPIC), and the Federal Bureau of Investigation (FBI).

The TTIC developed and employs the *Texas Transnational Intelligence Center Reporting System* (hereinafter referred to as the "TTICRS.") The TTICRS system supports regional information and intelligence sharing efforts.

The TTIC permits authorized personnel to access and query data from a centralized database. The database is comprised of data set compilations from federal, regional and public agency databases. The TTICRS facilitates analytical collaboration by providing its users analytical tools, open source query tools, and various means to obtain and disseminate intelligence products. The system does not include any commercial databases. It incorporates components that include software for reporting, analysis and sharing; secure networked computers; data and database interfaces.

The TTIC has developed libraries by using existing data sources from participating entities to integrate data with the goal of identifying, developing, and analyzing information and intelligence related to criminal and terrorist activity. This capabilities will facilitate integration and exchange of information between the participating agencies. The TTIC's intelligence products and services will be available to Texas law enforcement agencies and other authorized criminal justice entities.

The goal of establishing and maintaining the TTIC is to:

a. Increase and improve public safety and security in the State of Texas.
b. Coadjuvate with national security.
c. Minimize the threat and risk of injury to specific individuals.
d. Reduce the threat and risk of injury to law enforcement and others responsible for public protection, safety, or health.
e. Decrease the threat and risk of damage to real or personal property.
f. Protect individual privacy, civil rights, civil liberties, and other legally protected interests.
g. Protect the integrity of criminal investigations, criminal intelligence, and justice system processes and information.
h. Minimize reluctance of individuals or groups to use or cooperate with the justice system.
i. Support the role of the justice system in society.
j. Promote governmental legitimacy and accountability.
k. Not unduly burden the ongoing business of the justice system.
l. Make the most effective use of public resources allocated to justice agencies.

II. Purpose

This Privacy Policy will guide and govern the TTIC's procedures to ensure the lawful and appropriate access to and use of the TTIC and the data contained in it or derived from it. The purpose of this privacy policy is to ensure personnel with direct access to the TTIC information and intelligence comply with relevant federal, state and local laws, policies and regulations regarding privacy, civil rights, and civil liberties protections.

This policy will insure that safeguards to protect personal information and sanctions are in place as information and intelligence are developed and exchanged. The TTCI has adopted operating policies that comply with the *Texas Fusion Center Policy Council's* "Umbrella Privacy Policy for the Texas Fusion Center Network."

All agencies participating in the TTIC and individual TTIC users, as representatives of their agencies, will be subject to abide by this policy either by signing a Memorandum of Agreement (MOA) or a user agreement either digitally (through online services) or in writing. Both agencies and users will be required to adhere to all applicable laws, rules, regulations, TTIC policies and security requirements.

The Director of the TTIC is responsible for the overall operation of the TTIC and its services, including the development of the policy herein and its implementation.

The Director of the TTIC, or his designee, shall serve as the Privacy Officer. The Privacy Officer shall ensure the congruency of this policy and the overall mitigation of any issues within such.

The Privacy Officer shall receive reports regarding alleged errors and violations of the provisions of this policy, receive and coordinate complaint resolution under the TTIC's redress policy, and serve as the liaison for the Information Sharing Environment (ISE).

The Privacy Officer shall ensure that privacy protections are in place through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies. The Privacy Officer's mailing address is 1601 N. Bicentennial Blvd, McAllen, Texas 78501, **Attn: TTIC Privacy Officer.**

III. Vision Statement

The TTIC will protect the privacy and civil rights of all persons. The TTIC will provide full time system access to authorized users for the purposes of predicting, preventing, or mitigating the impacts of relevant hazards to the public. Additionally, the TTIC will conduct staffed operations as necessary to provide preventive and predictive intelligence analysis to enhance operational effectiveness and efficiency of organizations supporting the public safety of the counties along the Texas/Mexico border.

IV. Governance and Oversight

The McAllen Police Department and the Hidalgo County Sheriff's Office have primary responsibility for the operation of the TTIC. The center's governance shall consist of an Executive Advisory Board, Operational Management Team, TTIC Director and Privacy Officer. Each role is described below.

a. The Executive Advisory Board, or their designee, shall appoint a TTIC Director.
b. The TTIC Director will establish necessary policies, procedures, practices and protocols as well as the use of software, information technology tools and physical security measures to ensure information and intelligence are only accesses by authorized personnel and are protected from unauthorized access, modification, theft or sabotage (whether internal or external), natural or human-caused disasters and intrusions.
c. The Director and the Privacy Officer shall coordinate to ensure enforcement procedures and sanctions are adequate and adhered to.
d. Overall responsibility for TTIC 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 TTIC Director.
e. The TTIC is guided by an Executive Advisory Board (hereinafter referred to as the Board).
f. The Board is compromised by the McAllen Police Department and the Hidalgo County Sheriff's Office.
g. Texas Department of Public Safety assists the Hidalgo County Sheriff's Office and McAllen Police Department in the establishment and operation of the TTIC [refer to TGC 362.005 (b)] .
h. The Board will be chaired by the McAllen Chief of Police and the Hidalgo County Sheriff, or their designees.
i. The Advisory Board will meet as needed but not less than annually to review and update this policy in response to changes in laws and implementation experience, including the results of audits and inspections.

The Board shall have the following responsibilities:

a. Resolve conflicts or disputes that might arise related to policy or mission;
b. Establish protocol concerning the treatment of violations of the agreement;
c. Resolve disputes between Partner Agencies arising from the operations and activity of the Center; and
d. Review and update the TTIC Privacy Policy annually based upon recommendations by the TTIC's Director or designee, changes in applicable law or legal counsel.

The TTIC shall have a trained Privacy Officer. The Privacy Officer may either be the TTIC Director or be appointed by the TTIC Director.

a. The Privacy Officer receives reports regarding alleged errors and violations of this policy, receives and coordinates complaint resolution under the Center's redress policy, and serves as the liaison for the Information Sharing Environment (ISE), ensuring privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy-enhancing technologies.
b. The TTIC Privacy Officer is tasked with ensuring the enforcements of this policy are adequate and enforced.

c. The Privacy Officer shall review all analytical products to ensure they provide appropriate privacy, civil rights and civil liberties protections prior to dissemination or sharing by the TTIC.
d. The Privacy Officer can be contacted at the following address: 1601 N Bicentennial Blvd, McAllen, Texas 78501, Attn: Privacy Officer.

V. Training

TTIC and its participating agencies will require the following individuals to participate in training programs regarding the implementation of and adherence of privacy, civil rights, and civil liberties policy:

a. All of its personnel that use, contribute and/or derive data from the TTIC;
b. Personnel providing information technology services to the TTIC;
c. Staff in other public agencies or private contractors providing services to the TTIC; and
d. Users who are not employed by either the TTIC or a TTIC contractor that use, contribute and/or derive data from the TTIC.

The training program will cover:

a. Purposes of the privacy policy, civil rights and civil liberties protections.
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 TTIC or retained in the TTICRS.
c. The impact of improper activities associated with Information accessible within or through the TTIC.
d. The nature and possible penalties for policy violations, including possible transfer, dismissal, civil and criminal liability, and immunity, if any.

The TTIC will provide training to personnel authorized to share protected Information with the Intelligence Sharing Environment.

VI. Collection Limitations

The TTIC maintains the TTICRS for the purpose of collecting crime data from pand developing intelligence for agencies participating with the TTIC and TTICRS. The decision of the agencies to participate, and which information and databases to provide is voluntary and will be governed by the laws and rules governing the individual agencies respecting such data, as well as by applicable federal, state and tribal laws.

Because the rules, regulations or policies governing information collection on private individuals and intelligence released may vary from agency to agency, limitations on the collection of data concerning individuals is the responsibility of the collector of the original source data.

Each contributor of information shall abide by the collection limitations applicable to it by reason of law, rule, or policy. Information contributed to the TTIC should be that which has been collected in conformance with those limitations. Should any information be contributed to the TTIC that does not conform to these laws, rules, or policies, the TTIC will purge, delete or refuse to accept the information.

All TTIC participating agency users, TTIC personnel, private contractors, and personnel providing information technology services to the TTIC will comply with the Texas Constitution and the U. S. Constitution. This includes the Bill of Rights, and all applicable laws protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing, and disclosure of information, to include the Texas Public Information Act, and others, as referenced in Section XIV, “Privacy Policy Laws, Regulations and References”.

A project shall not include any criminal intelligence system information, obtained in violation of Federal, State, or local laws or ordinances. Because this is an interjurisdictional intelligence system, the Center is responsible for establishing that information entered is not in violation of Federal, State, or local laws. This is achieved either through examination or through other supporting information submitted by participating agencies, or by delegation of this responsibility to a properly trained participating agency, which is subject to routine inspection and audit procedures established by the Center under 28 CFR part 23 (refer to the appendix).

A. What Information May Be Sought or Retained?

1. The TTIC will retain criminal information or criminal intelligence information that is:
   - i) Based on a criminal predicate or possible threat to public safety; or
   - ii) Based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal conduct or activity that presents a threat to any individual, the community or the nation, and
   - iii) Relevant to the investigation and prosecution of suspected criminal incidents;
   - iv) The resulting justice system response;
   - v) The enforcement of sanctions, orders, or sentences; or
   - vi) The prevention of crime; or
   - vii) Useful in crime analysis or in the administration of criminal justice, or
   - viii) Collected by criminal justice agencies on specific individuals, consisting of:
     - (1) official identifiable descriptions, and
     - (2) notations of arrests, detentions, complaints, indictments, information, or other formal criminal charges and any disposition relating to these charges.
2. Where there is reasonable suspicion that a specific individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and the information is relevant to the criminal (including terrorist) conduct or activity, and
3. Where the data was collected in a fair and lawful manner, with knowledge and consent of the individual - if appropriate - and the source of the information is reliable and verifiable, or limitations on the quality of the information are identified.
4. The TTIC will collect and retain criminal information regarding, criminal combinations, and street gangs collected articles only as allowable under articles 61.07 and 61.08 of the Texas Code of Criminal Procedure.
5. The TTIC 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.
6. The TTIC will collect or retain only public health and safety information in accordance with Law, including The Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, (Dec. 31, 1974), The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) [HIPAA] and The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment) and that is relevant to the prevention, mitigation, and/or response to public health and safety emergencies, including natural disasters, man-made disasters, and disease outbreaks.
7. TTIC employees are prohibited and the originating agencies will agree not to seek, submit or retain information about an individual or organization solely on the basis of religious, political, or social views or activities; participation in a particular organization or event; or race, ethnicity, citizenship, place of origin, age, disability, gender, or sexual orientation.

B. Methods of Seeking or Receiving Information

Information gathering and investigative techniques used by the TTIC will comply with the U.S. and Texas constitutions and the Bill of Rights, The Privacy Act of 1974, 5 U.S.C. § 552a, Public Law No. 93-579, (Dec. 31,1974), Information Sharing Environment (ISE) Privacy Guidelines as mandated by Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and Executive Order 13388 and methods allowable under articles 61.07 and 61.08 of the Texas Code of Criminal Procedure and Texas Government Code Section 2161.122: Information Gathering by State Agency.

Participating agencies are responsible for ensuring that the information contained in their information systems and uploaded to the TTICRS was collected and stored in compliance with all applicable laws.

The TTIC will ensure that its products are reliable and verifiable or limitations on the quality of information are identified.

The TTIC will not directly or indirectly receive, seek, accept, or retain information from an individual or nongovernment information provider, who may or may not receive a fee or benefit for providing the information, if the TTIC knows or has reason to believe that:

1) The individual or information provider is legally prohibited from obtaining the specific information sought or disclosing it to the TTIC.
2) The individual or information provider used methods for collecting the information that the TTIC itself could not legally use.
3) The specific information sought from the individual or information provider could not legally be collected by the TTICRS; or
4) The TTIC has not taken the steps necessary to be authorized to collect the information.
5) The TTICRS will use the least intrusive methods of information gathering in any particular circumstance information gathering is authorized to seek or retain.

C. Information subject to collation and analysis

Information sought or received by the TTIC or from other sources will only be analyzed:

a. By qualified individuals who have successfully completed a background check and appropriate security clearance, if applicable;
b. By properly trained personnel concerning the policies contained within this privacy policy;
c. To 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 generally;
d. To further crime (including terrorism) prevention, enforcement, force deployment, or prosecution of public safety and health objectives and priorities established by the TTIC;
e. To further crime (including terrorism) prevention objectives and priorities established by the TTIC.

The TTIC requires that all analytical products be reviewed and approved by the Privacy Officer to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the TTIC.

The TTIC shall keep an electronic record of the source of all information retained in the TTICRS.

All TTICRS users will be able to access the system via a hyperlink on the log-in page or an alternate system which may be developed or identified for this purpose.

Users will be required to acknowledge that they have reviewed and will comply with this policy in order to log in to the system.

This policy will also be included in the training materials provided to new users prior to their access to the system.

All TTIC internal policies and procedures will be in compliance with this policy.

All staff members of the TTIC will be provided a copy of the Privacy and Civil Rights Policy and will be required to provide their signature to acknowledge they have read and understood the policy.

VII. Data Quality

All data submitted to the TTICRS is normalized, merged and maintained by the McAllen Police Department Information Technology Department. It will obtain guidelines and reviews from the Director of the TTIC.

The agencies participating in the TTIC or the TTICRS retain ownership of the data contributed and are, therefore, responsible for the quality and accuracy of the data accessed by the TTIC or the TTICRS.

Where appropriate, TTIC will ensure that originating agencies apply labels to the information that is shared with TTIC regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

The labeling of information will be reevaluated by the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

Inaccurate personal information can have a damaging impact on the person concerned and on the integrity and functional value of the TTIC and the TTICRS. In order to maintain the integrity of the TTIC as well as the TTICRS, any information obtained through the TTIC shall be independently verified with the original source from which the data was extrapolated before any official action (e.g., warrant or arrest) is taken.

User agencies and individual users are responsible for compliance with respect to the use and further dissemination of such information and the purging and updating of the data.

The TTIC will ensure that its analytical products contain sources of information that are reliable and verifiable, or limitations on the quality of information are identified (accuracy, completeness, currency, and confidence [verifiability and reliability])

The TTIC will make every reasonable effort to ensure that information sought or retained is:

a. Derived from dependable and trustworthy sources of information;
b. Accurate;
c. Current;
d. Complete, including the relevant context in which it was sought or received and other related information; and
e. Records about an individual or organization from two or more sources will not be merged by TTIC unless there is sufficient identifying information to reasonably conclude that the information is about the same individual or organization.
f. The set of identifiers sufficient to allow merging will consist of all available attributes that can contribute to a higher accuracy of a match.
g. TTIC will not merge Information based on partial matches.

The TTIC will make every reasonable effort to ensure that only authorized users are allowed to add, change, or delete Information in the system.

TTIC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency). The TTIC will make every reasonable effort to ensure that Information will be deleted from the system when the TTIC learns that:

a. The Information is erroneous, misleading, obsolete, or otherwise unreliable;
b. The source of the Information did not have authority to gather the information or to provide the information to the TTIC; or
c. The source of the Information used prohibited means to gather the information.

The TTIC will electronically advise recipient agencies when information previously provided to them is deleted or changed pursuant to the provisions in this section.

TTIC will electronically notify originating agencies when information received from them is deleted or changed pursuant to the provisions in this section.

The TTICRS will ensure that their products and the originating agency have labels applied to indicate to the accessing authorized user that:

1) The information is "protected information" as defined in Part XIII, and to the extent expressly provided in this policy, includes organizational entities.
2) The information is subject to local, state or federal laws restricting access, use, or disclosure.

VIII. Use Limitation

Information obtained from or through the TTIC or the TTICRS can only be used for lawful purposes. A lawful purpose means the request for data can be directly linked to a law enforcement agency's active criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal act. A project shall not include in any criminal intelligence system Information which has been obtained in violation of Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination or supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project as established under 28 CFR Part 23 and the Texas Public Information Act.

The Executive Advisory Board of the TTIC will take necessary measures to make certain that access to the TTICRS' information and intelligence resources is secure and will prevent any unauthorized access, dissemination or use. The Board reserves the right to restrict the qualifications and number of personnel who will be accessing the TTIC and to suspend or withhold service to any agency or individual violating this Privacy Policy. The Board, or persons acting on behalf of the Board, further reserves the right to conduct audits concerning the proper use and security of the information received from the TTIC.

A. Sharing Information for Specific Purposes

1. Information gathered and retained by the TTIC may be disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses or purposes specified in the law.
2. An audit trail will be kept of the requests for access and of what Information is disseminated to such persons.

3. Agencies external to the TTICRS may not disseminate information accessed or disseminated from the TTIC without approval from the TTIC or other originator of the information.

B. Sharing Information within the TTIC and with other Justice System Partners

1. Access to Information retained in the TTICRS will only be provided to persons within the TTIC 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 the Law and procedures applicable to the agency for whom the person is working.
2. An audit trail will be kept of access by or dissemination of information to such persons.

C. Sharing Information with those responsible for Public Protection, Safety, or Public Health

1. Information retained by the TTIC may be disseminated to individuals in public or private entities only for public protection, safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures.
2. Nothing in this policy shall limit the dissemination, including unsolicited, of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger or certain danger to life or property.
3. The TTIC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself.
4. An audit trail will be kept of the access by or dissemination of information to such persons.

IX. Security Safeguards

TTIC's Senior Intelligence Analyst is designated and trained to serve as the TTIC security officer.

Security for Information derived from the TTIC will be provided in accordance with applicable laws, rules, regulations and within —Information Sharing Environment (ISE) Privacy Guidelines as mandated by Section 1016(d) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) and Executive Order 13388.

Furthermore, all personnel who receive, handle, or have access to TTIC or TTICRS data and/or sensitive Information will be trained as to those requirements.

Special consideration will be followed pertaining to information related to gang membership and activities and pertaining to information gathered regarding children under Articles 61.07 and 61.08 to the Texas CCP.

A. All personnel having access to the TTIC or the TTICRS' data agree to abide by the following rules:
    1. The TTIC's data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the user's employer.
    2. Individual passwords will not be disclosed to any other person except as authorized by TTIC management.
    3. Individual passwords will be changed if authorized personnel of the agency or members of the TTIC suspect the password has been improperly disclosed or otherwise compromised.
    4. Background and criminal background checks will be completed on all personnel who will have direct access to the TTIC or TTICRS.
B. Use of the TTIC or TTICRS' data in an unauthorized or illegal manner will subject the user to denial of further use of the TTIC or TTICRS and may face disciplinary action by the user's employing agency.
C. Each authorized user understands that access to the TTIC or the TTICRS can be denied or rescinded for failure to comply with the applicable restrictions and use limitations.

D. Information obtained from or through the TTIC or TTICRS will not be used or publicly disclosed for purposes other than those specified in the Memorandum of Understanding that each participating agency must sign. Information cannot be (1) sold, published, exchanged, or disclosed for commercial purposes; (2) disclosed or published without prior approval of the contributing agency; or (3) disseminated to unauthorized persons.
E. Use of the TTIC's or the TTICRS' data is limited to those individuals who have been selected, approved, and trained accordingly.
F. Access to information contained within the TTICRS will be granted only to law enforcement agency personnel who have been vetted by the Director of the TTIC, or the Director's designee, as well as any additional background screening processes using procedures and standards established by the Executive Advisory Board.
G. Each individual user must complete an Individual User Agreement in conjunction with training.
H. **The TTIC reserves the right to restrict the qualifications and number of personnel having access to TTIC Information and to suspend or withhold service and deny access to any participating agency or participating agency personnel violating the TTIC's privacy policy.**
I. Access to the TTICRS' databases from outside of the TTIC is only allowed over secure network lines.

A. Information Retention and Destruction

a. Review of information regarding retention: all applicable information will be reviewed for record retention (validation or purge) by TTIC at least every five (5) years, in compliance with applicable State and Fedeal law.
b. When Information has no further value or meets the criteria for removal under applicable law; it will be purged, destroyed, deleted, or returned to the submitting source.
c. Information may be retained for up to 180 days in order to work an un-validated tip, lead or SAR information to determine its credibility and value, or assign a disposition label (clear or unfounded), so that a subsequent authorized user knows the status and purpose of the retention and will retain the information based on the retention period associated with the disposition label.

B. Destruction of Information

1. Specified Information will be deleted from the TTICRS pursuant to requests from the participating agency that owns the Information and in accordance with any inter-local agreement or memorandum of understanding with the participating agency.
2. The TTIC will delete Information from any analytical product that contains Information from deleted or purged records.
3. Notification of the destruction or return of records will be provided to:
    a. The participating agency that provided the data
    b. The TTIC intelligence analyst.
4. A record that Information has been purged or returned shall be maintained by the TTIC and a record shall be kept.

C. Classification of Information Regarding Validity and Reliability

1. The TTICRS will ensure that their products and the originating agency have labels applied to indicate to the accessing authorized user that:
    i. The Information is protected Information as defined in Part IV, section D, and to the extent expressly provided in this policy, includes organizational entities.
    ii. The Information is subject to local, state or federal law restricting access, use, or

disclosure TTIC personnel will, upon receipt of information, assess the Information to determine or review its nature, usability, and quality. Personnel will assign categories to the Information (or ensure that the originating agency has assigned categories to the Information) to reflect the assessment, such as:

1. Whether the Information consists of criminal history, intelligence Information, case records, conditions of supervision, case progress, or other Information category.
2. Content validity (for example, confirmed, probable, doubtful, cannot be judged);
3. Nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector); and
4. Source reliability (for example, reliable, usually reliable, unreliable, unknown).

iii. The categorization of retained Information will be reevaluated when new Information is gathered that has an impact on the validity and reliability of retained Information.

D. Classification of Information Regarding Limitations on Access and Disclosure

1. At the time a decision is made to retain Information, it will be labeled (by record, data set, or system of records) pursuant to the applicable limitations on access and sensitivity of disclosure in order to:
   i. Protect confidential sources and police undercover techniques and methods;
   ii. Not interfere with or compromise pending criminal investigations;
   iii. Protect an individual's right of privacy and civil rights
   iv. Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

E. Reclassification of existing information

1. Existing information will be reevaluated whenever:
   a. New Information is added that has an impact on access limitations or the sensitivity of disclosure of the Information; or
   b. There is a change in the use of the Information affecting access or disclosure limitations.
2. The access classifications will be used to control:
   a. What Information a class of users can have access to;
   b. What Information a class of users can add, change, delete, or print; and
   c. To whom the Information can be disclosed and under what circumstances.

TTIC will identify and review protected information that may be accessed from or disseminated by the TTIC prior to sharing that information through the Information Sharing Environment (ISE). Further, the TTIC 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.

TTIC 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:

1) The name of the originating center, department or agency, component, and subcomponent.
2) The name of the center's justice information system from which the Information is disseminated.
3) The date the Information was collected and, where feasible, the date its accuracy was last verified.

4) The title and contact Information for the person to whom questions regarding the Information should be directed.

Where appropriate, TTIC 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.

TTIC 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.

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

X. Openness

It is the intent of the TTIC and its participating agencies to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. Participating agencies will refer members of the public to the original owner of the data as the appropriate entity to address any concern about data accuracy and quality, when this can be done without compromising an active inquiry or investigation.

A. Disclosing Information to the Public

Information collected and retained by the TTIC will continue to be owned by the participating agency that submitted such data to the TTIC, and such information will only be disclosed to a member of the public when it is determined by the owner agency to be a public record as a matter of law, and is not excepted from disclosure by law, and it may only be disclosed in accordance with the law and procedures applicable to the owner for this type of information.

The TTIC's Privacy Officer will be responsible for receiving and responding to information requests, inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center and to provide notice of information requests, inquiries and complaints about privacy to originating agencies. All information requests should be addressed to the following address: 1601 N Bicentennial Blvd, McAllen, Texas 78501, **Attn: TTIC Privacy Officer**.

XI. Individual Participation

The data maintained by the TTIC is provided, on a voluntary basis, by the participating agencies. The participating agencies shall continue to be the owners of the information they submit to the TTIC. Each individual user affiliated with the TTIC which conduct searches against the data and databases as described herein will be required to acknowledge that he or she remains solely responsible for the interpretation, further dissemination, and use of any information that results from the search process and is responsible for ensuring that any information relied upon is accurate, current, valid, and complete, especially before any official action is taken in full or partial reliance upon the Information obtained.

Members of the public are prohibited from directly accessing the TTIC's applications, databases and/or Information technology systems. Members of the public who desire to access data pertaining to themselves should request such information through a Public Information Act request submitted to the originating agency or entity that is the source of the data in question.

If appropriate or required, the TTIC will notify the originating agency of the request and its determination that disclosure by the TTIC or referral of the requestor to the source agency is neither required nor appropriate under

applicable law. [See Texas Attorney General ORD 576 (1990)]. The source agency shall, nevertheless, be responsible for responding or seeking protection of responsive information under the Public Information Act.

A. Disclosing Information to the Individual About Whom Information Has Been Gathered

1. Upon satisfactory verification of his or her identity and subject to the conditions specified in XI. A. 4., an individual is entitled to know the existence of and review Information about himself or herself that has been gathered and retained in the TTICRS.

i) Participating agencies providing data remain the owners of the data contributed.
ii) TTIC personnel will direct individuals who seek such information, if appropriate, to request it from the participating agencies that own and have supplied the data to the TTIC.
iii) The TTIC will advise the requestor that if TTIC holds information within the scope of the request, it will forward that request to the owning agency.
iv) There are exceptions to the production or disclosure of materials or information gathered and/or retained in the TTICRS. Information obtained, derived or shared through the FBI's N-Dex system is governed by the the FBI's published policies governing Personal Identifying Information (PIA).
v) The TTIC personnel have a User Agreement with the FBI to access N-Dex data.
vi) TTIC personnel shall adhere to all FBI's CJIS policies, to include those on the production, disclosure and/or dissemination of materials or information obtained, derived or submitted via N-Dex which contains PIA.
vii) The CJIS FBI's policy may be found at https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center/view
viii) This policy adopts, by reference, CFR Title 28, Part 16, Subpart E, §16.96 "Exemption of Federal Bureau of Investigation Systems—limited access." The full text may be found at https://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=524e56b7bd8379a830d157f937ad5a82&mc=true&n=pt28.1.16&r=PART&ty=HTML#se28.1.16_196
ix) This exceptions are justified for the following reasons:
(1) making available to a record subject the accounting of disclosures from records concerning him/her would reveal investigative interest by not only the FBI, but also by the recipient agency. This would permit the record subject to take appropriate measures to impede the investigation, e.g., destroy evidence, intimidate potential witnesses or flee the area to avoid the thrust of the investigation.
(2) These provisions concern individual access to investigative records, compliance with which could compromise sensitive information classified in the interest of national or state security, interfere with the overall law enforcement process by revealing a pending sensitive investigation, possibly identify a confidential source or disclose information which would constitute an unwarranted invasion of another individual's personal privacy, reveal a sensitive investigative technique, or constitute a potential danger to the health or safety to law enforcement personnel.
(3) Individual access to non-criminal investigative records, e.g., civil investigations and administrative inquiries, as described in subsection (k) of the Privacy Act, could also compromise classified information related to national security, interfere with a pending investigation or internal inquiry, constitute an unwarranted invasion of privacy, reveal a confidential source or sensitive investigative technique, or pose a potential threat to law

enforcement personnel.

(4) In addition, disclosure of information collected pursuant to an employment suitability or similar inquiry could reveal the identity of a source who provided information under an express promise of confidentiality, or could compromise the objectivity or fairness of a testing or examination process.

(5) To require the TTIC to amend information from derived from other agencies thought to be incorrect, irrelevant or untimely, because of the nature of the information collected and the essential length of time it is maintained, would create an impossible administrative and investigative burden by forcing the agency to continuously retrograde its investigations attempting to resolve questions of accuracy, etc.

(6) The nature of criminal and other investigative activities is such that vital information about an individual can only be obtained from other persons who are familiar with such individual and his/her activities. In such investigations it is not feasible to rely upon information furnished by the individual concerning his own activities.

(7) Disclosure would provide the subject with substantial information which could impede or compromise the investigation. The individual could seriously interfere with undercover investigative activities and could take appropriate steps to evade the investigation or flee a specific area.

(8) In the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by CFR 5 U.S.C. 552 subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, because many of these records come from other federal, state, local, joint, foreign, tribal, and international agencies, it is administratively impossible to ensure compliance with this provision.

(9) The notice requirements of CFR 5 U.S.C. 552 could seriously interfere with a law enforcement activity by alerting the subject of a criminal or other investigation of existing investigative interest.

2. If an individual has objections to the accuracy or completeness of the Information retained about himself or herself that has been disclosed, upon receipt of notification of such concerns the TTIC will notify the agency that is the owner of the Information and provide the individual with appropriate contact information for that agency. Thereafter the resolution of objections as to the accuracy or completeness of the information shall be between the individual and the agency, which owns such information. The TTIC will not expunge or amend Information unless requested by the agency that owns the Information.

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

i) is exempt from disclosure, ii) has been or may be shared through the ISE; iii)is held by TTIC; and iv) allegedly has resulted in demonstrable harm to the complainant, the TTIC will inform the individual of the procedure for submitting (if needed) and resolving such complaints.

Complaints from individuals regarding these matters should be submitted to the TTIC's Privacy Officer at the following address: 1601 Bicentennial Blvd, McAllen, Texas 78501, **Attn: Privacy Officer**. The Privacy Officer will

acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the Information to the complainant unless otherwise required by Law. The Privacy Officer will notify the originating agency which is the owner of such Information 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 TTIC that is the subject of a complaint will be reviewed by the owner agency 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 from the date TTIC provides notification of the complaint to the owner of such Information, the TTIC will not share the Information until such time as the complaint has been resolved. A record will be kept by the TTIC of all complaints and the resulting action taken in response to the complaint.

4. The existence, content, and source of the information will not be disclosed (by an owner agency) to an individual when:

a. Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution; (Tex. Gov't Code § 552.108)
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; (Tex. Gov't Code § 552.108)
d. The Information relates to matters excepted from disclosure under the Texas Public Information Act, ch 552 Tex. Gov't Code;
e. Other ***authorized*** basis for denial, including but not limited to Tex. Gov't Code §§ 552.101, 552.108, 552.111, 552.117, 552.1175, 552.119, 552.132, 552.1325, 552.134, 552.137, 552.138, 552.139, 552.142,552,1425, 552.147, 552.148, 552.150, and 552.151A record will be kept of all requests and of what information is disclosed to an individual by an owner agency, and such owner agency shall notify TTIC of such disclosures.

Participating agencies that are not the owners of the information requested agree that they will promptly refer requests for information in their possession to the owners of the Information. TTIC will comply with the Texas Public Information Act in responding to requests for public information for documents or reports that originate with the TTIC and which do not comprise information owned by an owner agency and shared with TTIC.

XII. Accountability

A. Queries

1. When a query is made to the TTIC or the TTICRS as well as any of its data applications, the original request is automatically logged by the system identifying the user initiating the query.
2. When such information is disseminated outside of the agency from which the original request is made, a secondary dissemination log must be maintained in order to correct possible erroneous Information and for audit purposes, as required by applicable law.
3. Secondary dissemination of information can only be to a law enforcement agency for a law enforcement investigative purpose, or to other agencies as provided by law.
4. The agency from which the information is requested will maintain a record (log) of any secondary dissemination of Information. This record will reflect as a minimum:
    a. Date of release.
    b. To whom the information relates.
    c. To whom the Information was released (including address and telephone number).

d. An identification number or other indicator that clearly identifies the data released.
e. The purpose for which the information was requested.

B. Accountability for Activities

Primary responsibility for the operation of this justice information system— including operations; coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, and disclosure of Information; and the enforcement of this policy—is assigned to the Director of the TTIC.

The TTIC will establish procedures, practices, and system protocols and use software, information technology tools, and physical security measures that protect Information from unauthorized access, modification, theft, or sabotage, whether internal or external and whether due to natural or human-caused disasters or intrusions.

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

The TTIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users and the TTICRS itself with the provisions of this policy and applicable law. The TTIC will require any individuals authorized to use the system to agree in writing to comply with the provisions of this policy.

The TTIC will periodically conduct audits and inspections of the information contained in the TTICRS. The audits will be conducted randomly by a designated representative of the TTIC or by a designated independent party. The audit will be conducted in such a manner so as to protect the confidentiality, sensitivity, and privacy of the Information contained in the TTICRS.

The TTIC's Privacy Officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable law, technology, the purpose and use of the information systems, and public expectations.

The TTIC will notify an individual about whom unencrypted personal Information was or is reasonably believed to have been obtained by an unauthorized person and access to which threatens physical or financial harm to the person.

The notice will be made promptly and without unreasonable delay following discovery or notification of the access to the Information, consistent with the legitimate needs of law enforcement to investigate the release or any measures necessary to determine the scope of the release of Information and to reasonably restore the integrity of the information system.

Any breach in the system or misuse of information shall be handled in accordance to the TTIC's Standard Operational Procedure as outlined in Section 6 thru 8.

Failure to abide by the restrictions and use limitations set forth by the TTIC may result in the suspension or termination of use privileges, discipline sanctions imposed by the user's employing agency, or criminal prosecution. There will be no web access to the public. Individuals vetted for access shall read and agree to restriction, and terms of use agreements before every log in process.

TTIC personnel or other authorized users shall report errors and suspected or confirmed violations of TTIC policies relating to protected Information to the TTIC Privacy Officer at the following address: 1601 Bicentennial Blvd, McAllen, Texas 78501, **Attn: Privacy Officer**.

The Executive Advisory Board will be responsible for conducting or coordinating audits and investigating misuse of

the TTIC's data or Information. After violations are identified they will be reported to the originating agencies which will be responsible for corrective action; however, the Executive Advisory Board reserves the right to bar the Participating Agency and/or its employees from further use of the TTIC and TTICRS.

XIII. Terms and Definitions

Access: Data access is being able to get to particular data on a computer (having permission to use a computer. Data access is usually specified as read-only and read/write access. Web access means having a connection to the World Wide Web through an access provider or an online service provider. With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain intelligence, to include terrorism-related information, homeland security information and law enforcement information obtained in the first instance by another ISE participant.

Access Control:

Mechanism to limit access to certain information, based on user's identity and membership on various predefined groups. Access control can be:

1) Mandatory
2) Discretionary
3) Role-based

Acquisition: Means by which an ISE participant obtains information through the exercise of its authorities.

Administration of criminal justice: Has the meaning assigned by Article 60.01, Texas Code of Criminal Procedure.

Administrator: Individual appointed by the Hidalgo County Sheriff's Office and the McAllen Police Department as the system administrator for intelligence systems or another individual designated to serve in that capacity.

Audit Trail: A term used to log or record a sequence of activities. In the context of computer and network systems, the audit trail tracks the sequence of activities on the system, such as log-ins and log-outs. Expansive audit trails also record each user's activities in detail, to include commands issued to the system, what records and filed were accessed or modified. Audit trails are a fundamental part of computer security; often used to trace unauthorized users and unauthorized use. Audit trails can be useful for recovery efforts in case of system failure.

Authentication: Process of validating the credentials of a person, computer process or device with access to certain information, process or device, making the request provide a credential that proves it is what or who it says it is. Common methods are digital certificates, digital signatures, smart cards, biometric data and a combination of user names and passwords.

Authorization: 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.

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

Biometrics: Biometrics methods are divided in two categories:

1) Physiological: face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography) and hand geometry.
2) Behavioral: voiceprints and handwritten signatures.

Civil Liberties: Term used to refer to fundamental individual rights, such as freedom of speech, press or religion, due process of law, and other limitations of the power of the government to restrain of dictate the actions of individuals. These freedoms are guaranteed by the Bill of Rights – the first ten Amendments to U.S Constitution. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Civil liberties involves restrictions on the government.

Civil Rights: Term used to imply that the State has a role ensuring all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of characteristics unrelated to the worth of the individual, such as race, religion, age, gender, etc. Civil rights are obligations imposed upon the government to promote equality. They are the rights to personal liberty guaranteed under the 13th and 14th Amendments and by acts of Congress.

Child: Has the meaning assigned by Section 51.02, Texas Family Code.

Combination: Has the meaning assigned by Section 71.01, Texas Penal Code.

Computer security: Protection of information assets through use of technology, processes and training.

Confidentiality: Refers to individual and institutional obligations to use the information under their control appropriately once is as been disclosed to them. Confidentiality is observed out of respect for and to protect and preserve the privacy of others.

Credentials: Information that includes identification and proof of identification use to gain access to local and network resources. Credentials can ben user-names, passwords, smart-cards, certificates, etc.

Criminal activity: Conduct subject to prosecution

Criminal information: Means facts, material, photographs, or data reasonably related to the investigation or prosecution of criminal activity.

Criminal Intelligence Information: Means data that has been evaluated to determine that:

1) Is relevant to the identification of criminal activity engaged in by an individual or an organization which is reasonably suspected of involvement in criminal activity, and
2) Meets criminal intelligence system submission criteria and is maintained in a criminal intelligence system maintained under 28 CFR Part 23.

Criminal justice agency: Has the meaning assigned by the Texas Code of Criminal Procedure, Article 60.01. It includes a municipal or county agency, or school district law enforcement agency that is engaged in the administration of criminal justice under a statute or executive order.

Criminal street gang: Have the meanings assigned by Section 71.01, Texas Penal Code.

Criminal street gang member or gang member: Individual that has been identified as a member of a criminal gang through documentation supported by standards set in 28 CFR Part 23.

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

Data breach: The unintentional release of secure information to an untrusted environment. This may include:

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

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

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

Disclosure: The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

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

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

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

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

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

Identification: A process whereby a real-world entity is recognized and its identity established. In the abstract world of information systems, “identity” is as a set of information about an entity that uniquely differentiates it from other similar entities. The set of information may be as small as a single code, specifically designed as an identifier, or a

collection of data, such as a given and family name, date of birth, and address. An organization's identification process consists of the acquisition of the relevant identifying information.

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

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

Information: Includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists.

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

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

Intelligence database: Means a collection or compilation of data organized for search and retrieval to evaluate, analyze, disseminate, or use intelligence information relating to a criminal combination or a criminal street gang for the purpose of investigating or prosecuting criminal offenses.

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

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

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

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

Law: As used in this policy, includes any local, state, tribal, territorial, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order, as construed by appropriate local, state, tribal, territorial, 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:

1) Related to terrorism or the security of our homeland, and
2) Relevant to a law enforcement mission, including, but not limited to
    a. information pertaining to an actual or potential criminal, civil, or administrative investigation,

or

b. a foreign intelligence, counterintelligence, or counterterrorism investigation;
c. assessment of or response to criminal threats and vulnerabilities;
d. 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
e. assisting or associated with criminal or unlawful conduct;
f. the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law;
g. identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and
h. victim/witness assistance.

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

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

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

Logs: A necessary part of an adequate security system. Logs are needed to ensure that data is properly tracked, and that only authorized individuals get access to the data. Refer to Audit Trail.

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

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

Need to Know: Refers to access to sensitive information or intelligence necessary for the conduct of an individual's official duties, who is 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), as a result of jurisdictional, organizational, or operational necessities.

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

Origination 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 the TTIC.

Participating Agency: A local, County, State, Tribal, Federal, or another governmental entity which exercises law enforcement authority, and which is authorized to submit and receive criminal information and criminal intelligence information through the TTIC, within the framework of an inter-local agreement or Memorandum of Agreement with the TTIC. Public or private entities of any type, whether for profit or nonprofit, that are authorized by law, and obtain requisite permission to submit and/or receive information through the TTIC.

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

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

1) 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.
2) 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(s) or credit card number(s) and associated PIN number(s), Automated Integrated Fingerprint Identification System [AFIS] identifier, or booking or detention system numbers.
3) Descriptions of event(s) or point(s) in time. For example, information contained in documents such as police reports, arrest reports, and medical records.
4) Descriptions of location(s) or place(s). It may include 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 TTIC 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 TTIC, the individual, and the public; and promotes public trust.

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

Protected Information: Includes information about individuals and organizations that is subject to information privacy or other legal protections by law, including:

1) The U.S. Constitution;
2) The Texas Constitution;
3) Applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23;
4) Applicable State and Tribal constitutions; and
5) Applicable State, local, and Tribal laws, ordinances, and codes.
6) Protections may be extended to other individuals or organizations by TTIC policy or by State, local, or Tribal law.

Public: Is any person, and any for-profit, or non-profit entity, organization, or association; any governmental entity for which there is no existing specific law authorizing access to the TTIC's information; media organizations; and entities that seek, receive, or disseminate information for whatever reason, regardless of whether done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the TTIC.

Public does not include:

1) Employees of the TTIC or participating agencies;
2) People or entities, private or governmental, who assist the TTIC in the operation of the justice information system; and
3) Public agencies whose authority to access information gathered and retained by the TTIC is specified in Law.
4) Public or private entities of any type, whether for-profit or nonprofit, that are authorized by Law and obtain requisite permission to receive information in bulk from the TTIC/TTICRS.

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

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

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

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

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

can contradict that claim.

Right to Know: Is 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 law enforcement, homeland security, or counterterrorism activities.

Right to Privacy: The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

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

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

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

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

Suspicious Activity Report (SAR): Official documentation of observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Suspicious activity report (SAR) information offers a standardized means for feeding information repositories or data analysis tools. Patterns identified during SAR information analysis may be investigated in coordination with the reporting agency and, if applicable, a state or regional fusion TTIC. SAR information is not intended to be used to track or record on going enforcement, intelligence, or investigatory activities, nor is it designed to support interagency calls for service.

Terrorism: There is no single, universally accepted definition of terrorism. Terrorism is defined in the *Code of Federal Regulations* as — "...the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. (28 C.F.R. Section 0.85).

The FBI further describes terrorism as either domestic or international, depending on the origin, base, and objectives of the terrorist organization. The FBI uses the following definitions of terrorism:

"Domestic terrorism" refers to activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any state; appear to be intended to intimidate or coerce a civilian population; to influence the policy of a government by mass destruction, assassination, or kidnapping; and occur primarily within the territorial jurisdiction of the United States. [18 U.S.C. § 2331(5)]

"International terrorism" involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state.

These acts intend to intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; or alter the conduct of a government by mass destruction, assassination or kidnapping, and occur primarily outside the territorial jurisdiction of the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum. [18 U.S.C. § 2331(1)]

The FBI further divides terrorist-related activity into two categories:

A terrorist *incident* is a violent act or an act dangerous to human life, in violation of the criminal laws of the United States, or of any state, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

Terrorism *prevention* is a documented instance in which a violent act by a known or suspected terrorist group or individual with the means and a proven propensity for violence is successfully interdicted through investigative activity.

Terrorism Information: Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to:

1) The existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism:
2) 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;
3) Communications of or by such groups or individuals; or
4) 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. These reports allege or indicate some form of possible criminal activity:

1) Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview report (FIR) information.
2) SAR information should be viewed, at most, as a subcategory of tip or lead data.
3) Tips and leads information does not include incidents that do not have a criminal offense attached or indicated, criminal history records, or CAD data.
4) Tips and leads information should be maintained in a secure system, similar to data that rises to the level of

reasonable suspicion.

5) 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.
6) 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.
7) 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.

Transnational organized crime: Those self-perpetuating associations of individuals who operate transnationally for the purposes of:

1) Obtaining power, influence, monetary and/or commercial gains,
2) Wholly or in part by illegal means,
3) While protecting their activities through a pattern of corruption and/ or violence,
4) Or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms.
5) There is no single structure under which transnational organized criminals operate;
6) They vary from hierarchies to clans, networks, and cells, and may evolve to other structures.
7) The crimes they commit also vary.

Transnational organized criminals act conspiratorially in their criminal activities and possess certain characteristics which may include, but are not limited to:

1) In at least part of their activities they commit violence or other acts which are likely to intimidate, or make actual or implicit threats to do so;
2) They exploit differences between countries to further their objectives, enriching their organization, expanding its power, and/or avoiding detection/apprehension.
3) They attempt to gain influence in government, politics, and commerce through corrupt as well as legitimate means.
4) They have economic gain as their primary goal, not only from patently illegal activities but also from investment in legitimate businesses, and
5) They attempt to insulate both their leadership and membership from detection, sanction, and/ or prosecution through their organizational structure.

User: Any individual representing a participating agency, authorized to submit information to the TTIC and access or receive and use intelligence and other resources from the TTIC for lawful purposes.

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

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

XIV. Privacy Policy Laws, Regulations and References

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

Chapter 362, Texas Government Code, Section 362.005 (Texas Transnational Intelligence Center);

Chapter 412, Texas Government Code, Sec. 421.085 (Privacy Policy Required)

Chapter 552, Texas Government Code (Texas Public Records Act);

Classified Information, 32 CFR 2003

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

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

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

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

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

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

Department of Homeland Security published Baseline Capabilities Guidelines for Fusion SWTFCs

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

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

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

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

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

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

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

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

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

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

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

Intelligence Identities Protection Act, 50 USC 421

Internal Security Act, 50 USC 783

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

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

Presidential Executive Order 13526, Classified National Security Information

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, Code of Federal Regulations, Title 16, Chapter I, Part 313

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

Public health and safety information in accordance to The Privacy Act of 1974, 5 U.S.C. §552a, Public Law No. 93-579, (Dec. 31, 1974);

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

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

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

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

Texas Code of Criminal Procedure, Article 60.01 (Administration of criminal justice)

Texas Code of Criminal Procedure, Articles 61.07 and 61.08 (methods allowable and information related to gang membership and activities and pertaining information gathered from children);

Texas Constitution;

Texas Government Code Chapter 552, regarding open government.

Texas Penal Code Section 51.02, regarding information on children

Texas Penal Code Section 71.01, regarding criminal street gang information

Texas Government Code, Section 2161.122: Information Gathering by State Agency.

The Family Educational Rights and Privacy Act of 1974 (FERPA or the Buckley Amendment);

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191) [HIPAA];

Title 28 Code of Federal Regulations, Part 23;

U.S. Constitution

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

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

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

APPENDIX

28 CFR Part 23 Guideline

Executive Order 12291

These regulations are not a "major rule" as defined by section 1(b) of Executive Order No. 12291, 3 CFR part 127 (1981), because they do not result in: (a) An effect on the economy of $100 million or more, (b) a major increase in any costs or prices, or (c) adverse effects on competition, employment, investment, productivity, or innovation among American enterprises.

Regulatory Flexibility Act

These regulations are not a rule within the meaning of the Regulatory Flexibility Act, 5 U.S.C. 601-612. These regulations, if promulgated, will not have a "significant" economic impact on a substantial number of small "entities," as defined by the Regulatory Flexibility Act.

Paperwork Reduction Act

There are no collection of information requirements contained in the proposed regulation.

List of Subjects in 28 CFR Part 23

Administrative practice and procedure, Grant programs, Intelligence, Law Enforcement.

For the reasons set out in the preamble, title 28, part 23 of the Code of Federal Regulations is revised to read as follows:

PART 23--CRIMINAL INTELLIGENCE SYSTEMS OPERATING POLICIES

- Purpose.
- Background.
- Applicability.
- Operating principles.
- Funding guidelines.
- Monitoring and auditing of grants for the funding of intelligence systems.

Authority: 42 U.S.C. 3782(a); 42 U.S.C. 3789g(c).

§ 23.1 Purpose.

The purpose of this regulation is to assure that all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647), are utilized in conformance with the privacy and constitutional rights of individuals.

§ 23.2 Background.

It is recognized that certain criminal activities including but not limited to loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials often involve some degree of regular coordination and permanent organization involving a large number of participants over a broad geographical area. The exposure of such ongoing networks of criminal activity can be aided by the pooling of information about such activities. However, because the collection and exchange of intelligence data necessary to support control of serious criminal activity may represent potential threats to the privacy of individuals to whom such data relates, policy guidelines for Federally funded projects are required.

§ 23.3 Applicability.

(a) These policy standards are applicable to all criminal intelligence systems operating through support under the Omnibus Crime Control and Safe Streets Act of 1968, 42 U.S.C. 3711, et seq., as amended (Pub. L. 90-351, as amended by Pub. L. 91-644, Pub. L. 93-83, Pub. L. 93-415, Pub. L. 94-430, Pub. L. 94-503, Pub. L. 95-115, Pub. L. 96-157, Pub. L. 98-473, Pub. L. 99-570, Pub. L. 100-690, and Pub. L. 101-647).

(b) As used in these policies: (1) Criminal Intelligence System or Intelligence System means the arrangements, equipment, facilities, and procedures used for the receipt, storage, interagency exchange or dissemination, and analysis of criminal intelligence information; (2) Interjurisdictional Intelligence System means an intelligence system

which involves two or more participating agencies representing different governmental units or jurisdictions; (3) Criminal Intelligence Information means data which has been evaluated to determine that it: (i) is relevant to the identification of and the criminal activity engaged in by an individual who or organization which is reasonably suspected of involvement in criminal activity, and (ii) meets criminal intelligence system submission criteria; (4) Participating Agency means an agency of local, county, State, Federal, or other governmental unit which exercises law enforcement or criminal investigation authority and which is authorized to submit and receive criminal intelligence information through an interjuris-dictional intelligence system. A participating agency may be a member or a nonmember of an interjurisdictional intelligence system; (5) Intelligence Project or Project means the organizational unit which operates an intelligence system on behalf of and for the benefit of a single agency or the organization which operates an interjurisdictional intelligence system on behalf of a group of participating agencies; and (6) Validation of Information means the procedures governing the periodic review of criminal intelligence information to assure its continuing compliance with system submission criteria established by regulation or program policy.

§ 23.20 Operating principles.

(a) A project shall collect and maintain criminal intelligence information concerning an individual only if there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

(b) A project shall not collect or maintain criminal intelligence information about the political, religious or social views, associations, or activities of any individual or any group, association, corporation, business, partnership, or other organization unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

(c) Reasonable Suspicion or Criminal Predicate is established when information exists which establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or 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. In an interjurisdictional intelligence system, the project is responsible for establishing the existence of reasonable suspicion of criminal activity either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(d) A project shall not include in any criminal intelligence system information which has been obtained in violation of any applicable Federal, State, or local law or ordinance. In an interjurisdictional intelligence system, the project is responsible for establishing that no information is entered in violation of Federal, State, or local laws, either through examination of supporting information submitted by a participating agency or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures established by the project.

(e) A project or authorized recipient shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(f) (1) Except as noted in paragraph (f) (2) of this section, a project shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination which are consistent with these principles.

(2) Paragraph (f) (1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

(g) A project maintaining criminal intelligence information shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to insure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the project shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of submitting agencies and control officials. Each project must establish written definitions for the need to know and right to know standards for dissemination to other agencies as provided in paragraph (e) of this section. The project is responsible for establishing the existence of an inquirer's need to know and right to know the information being requested either through inquiry or by delegation of this responsibility to a properly trained participating agency which is subject to routine inspection and audit procedures

established by the project. Each intelligence project shall assure that the following security requirements are implemented:

(1) Where appropriate, projects must adopt effective and technologically advanced computer software and hardware designs to prevent unauthorized access to the information contained in the system;

(2) The project must restrict access to its facilities, operating environment and documentation to organizations and personnel authorized by the project;

(3) The project must store information in the system in a manner such that it cannot be modified, destroyed, accessed, or purged without authorization;

(4) The project must institute procedures to protect criminal intelligence information from unauthorized access, theft, sabotage, fire, flood, or other natural or manmade disaster;

(5) The project must promulgate rules and regulations based on good cause for implementing its authority to screen, reject for employment, transfer, or remove personnel authorized to have direct access to the system; and

(6) A project may authorize and utilize remote (off-premises) system data bases to the extent that they comply with these security requirements.

(h) All projects shall adopt procedures to assure that all information which is retained by a project has relevancy and importance. Such procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections. All information retained as a result of this review must reflect the name of the reviewer, date of review and explanation of decision to retain. Information retained in the system must be reviewed and validated for continuing compliance with system submission criteria before the expiration of its retention period, which in no event shall be longer than five (5) years.

(i) If funds awarded under the Act are used to support the operation of an intelligence system, then:

(1) No project shall make direct remote terminal access to intelligence information available to system participants, except as specifically approved by the Office of Justice Programs (OJP) based on a determination that the system has adequate policies and procedures in place to insure that it is accessible only to authorized systems users; and

(2) A project shall undertake no major modifications to system design without prior grantor agency approval.

(j) A project shall notify the grantor agency prior to initiation of formal information exchange procedures with any Federal, State, regional, or other information systems not indicated in the grant documents as initially approved at time of award.

(k) A project shall make assurances that there will be no purchase or use in the course of the project of any electronic, mechanical, or other device for surveillance purposes that is in violation of the provisions of the Electronic Communications Privacy Act of 1986, Public Law 99-508, 18 U.S.C. 2510-2520, 2701-2709 and 3121-3125, or any applicable State statute related to wiretapping and surveillance.

(l) A project shall make assurances that there will be no harassment or interference with any lawful political activities as part of the intelligence operation.

(m) A project shall adopt sanctions for unauthorized access, utilization, or disclosure of information contained in the system.

(n) A participating agency of an interjurisdictional intelligence system must maintain in its agency files information which documents each submission to the system and supports compliance with project entry criteria. Participating agency files supporting system submissions must be made available for reasonable audit and inspection by project representatives. Project representatives will conduct participating agency inspection and audit in such a manner so as to protect the confidentiality and sensitivity of participating agency intelligence records.

(o) The Attorney General or designee may waive, in whole or in part, the applicability of a particular requirement or requirements contained in this part with respect to a criminal intelligence system, or for a class of submitters or users of such system, upon a clear and convincing showing that such waiver would enhance the collection, maintenance or

dissemination of information in the criminal intelligence system, while ensuring that such system would not be utilized in violation of the privacy and constitutional rights of individuals or any applicable state or federal law.

§ 23.30 Funding guidelines.

The following funding guidelines shall apply to all Crime Control Act funded discretionary assistance awards and Bureau of Justice Assistance (BJA) formula grant program subgrants, a purpose of which is to support the operation of an intelligence system. Intelligence systems shall only be funded where a grantee/subgrantee agrees to adhere to the principles set forth above and the project meets the following criteria:

(a) The proposed collection and exchange of criminal intelligence information has been coordinated with and will support ongoing or proposed investigatory or prosecutorial activities relating to specific areas of criminal activity.

(b) The areas of criminal activity for which intelligence information is to be utilized represent a significant and recognized threat to the population 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.

(c) The head of a government agency or an individual with general policy making authority who has been expressly delegated such control and supervision by the head of the agency will retain control and supervision of information collection and dissemination for the criminal intelligence system. This official shall certify in writing that he or she takes full responsibility and will be accountable for the information maintained by and disseminated from the system and that the operation of the system will be in compliance with the principles set forth in § 23.20.

(d) Where the system is an interjurisdictional criminal intelligence system, the governmental agency which exercises control and supervision over the operation of the system shall require that the head of that agency or an individual with general policymaking authority who has been expressly delegated such control and supervision by the head of the agency:

1. assume official responsibility and accountability for actions taken in the name of the joint entity, and
(2) certify in writing that the official takes full responsibility and will be accountable for insuring that the information transmitted to the interjurisdictional system or to participating agencies will be in compliance with the principles set forth in § 23.20.

The principles set forth in § 23.20 shall be made part of the by-laws or operating procedures for that system. Each participating agency, as a condition of participation, must accept in writing those principles which govern the submission, maintenance and dissemination of information included as part of the interjurisdictional system.

(e) Intelligence information will be collected, maintained and disseminated primarily for State and local law enforcement efforts, including efforts involving Federal participation.

§ 23.40 Monitoring and auditing of grants for the funding of intelligence systems.

(a) Awards for the funding of intelligence systems will receive specialized monitoring and audit in accordance with a plan designed to insure compliance with operating principles as set forth in § 23.20. The plan shall be approved prior to award of funds.

(b) All such awards shall be subject to a special condition requiring compliance with the principles set forth in § 23.20.

(c) An annual notice will be published by OJP which will indicate the existence and the objective of all systems for the continuing interjurisdictional exchange of criminal intelligence information which are subject to the 28 CFR Part 23 Criminal Intelligence Systems Policies.