300 - Privacy Policy

301 – Privacy Policy Purpose

A. The mission of the Dallas Police Department's Dallas Fusion Center (DFC) is to collect, evaluate, analyze and disseminate information and intelligence data regarding criminal activity, criminal enterprises, and suspected terrorist activity within the Dallas Police Department's area of operations, and provide the same to other law enforcement and public safety entities with a need and right to know. These include regional, state, and federal law enforcement and intelligence organizations. All DFC activities will be accomplished following Fair Information Practices to ensure the rights and privacy of our citizens.

B. As an underlying principle in support of our actions, DFC recognizes the mandate to ensure the protection of individual information privacy rights, federal and state civil rights laws, and constitutionally guaranteed civil liberties throughout the intelligence process. The purpose of this Privacy Policy is to ensure that safeguards and sanctions are in place to protect: the privacy, civil rights and civil liberties of all individuals; the protected interests of organizational entities as expressly provided herein; as well as the integrity of criminal investigations and justice system processes. It is also the purpose of this Privacy Policy to ensure accuracy and completeness of information and intelligence to the maximum extent feasible, and to ensure compliance with applicable law as information and intelligence are gathered or collected and exchanged.

C. The DFC Standard Operations Procedures (SOP) contains the standards that Fusion Center Officers and participants will adhere to for the collection, utilization, security, storage and retention of information and intelligence, as well as accountability guidelines for the management of such intelligence and/or information.

D. The Nationwide Suspicious Activity Reporting Initiative (NSI), identified within DFC SOP, Section 300 – Privacy Policy, reflects additional Collection and Privacy Safeguards governing the actions of all DFC personnel.

E. Primary responsibility for the operation of the DFC is assigned to the Dallas Police Department (DPD.) The DPD Chief of Police, or designee, will appoint a DPD Lieutenant (Unit Commander) who will be responsible for the day-to-day operation of the DFC. The DFC Unit Commander will establish needed procedures, practices and protocols as well as use advanced software, information technology tools, and physical security measures to ensure information and intelligence are accessed only by authorized personnel and are protected from unauthorized access, modifications, theft or sabotage, whether internal or external, or disasters or intrusions by natural or human causes.

302 – Collection Limitations

Information and intelligence will be obtained by fair and lawful means. Intelligence collected will be based on a criminal predicate or threat to public safety. DFC will follow 28 CFR Part 23 with regard to criminal intelligence information. Each contributor (and recipient) of information and intelligence shall abide by the collection (and use) limitations applicable to it by reason of law, rule, or policy. DFC will also adhere to criminal intelligence guidelines established under the National Criminal Intelligence Sharing Plan (NCISP).

A. The DFC will collect and retain only information that the source/submitting agency acquired in accordance with applicable laws and agency policy, using the least intrusive information gathering and investigative techniques necessary for each particular circumstance, and the information is obtained for one the following purposes:

    1. 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 terrorism) 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; or

    2. Relates to non-criminal threats to public health or infrastructure, and disaster response and relief; or

    3. Is relevant to the investigation and prosecution of suspected criminal, including terrorist, activity, the justice system response, and the prevention of crime; or

    4. Is useful in crime analysis or in the administration of justice and public safety (including topical searches of open source information).

B. In addition, all information obtained by the DFC will adhere to the following conditions:

    1. The content is verifiable and from a reliable source, or limitations regarding the quality of the information are identified, and

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

C. This policy applies to information or intelligence that identifies any individual or organization as a possible criminal or terrorism subject. The DFC will not collect or retain information about an individual or organization, and originating agencies will not submit such information, solely on the basis of religious, political or social views or activities; participation in a particular non-criminal organization or lawful event; or for an

individual, based solely on race, ethnicity, citizenship, place of origin, age, disability, gender or sexual orientation.

D. All Suspicious Activity Reporting (SARs) and terrorism-related SARs (ISESARs) will be collected and disseminated following the approved DFC Nationwide Suspicious Activity Initiative Privacy, Civil Rights and Civil Liberties Protection Policy as identified in the Dallas Police Department – DFC SOP, Section 300 - Privacy Policy.

E. DFC will make available an electronic copy of its Dallas Police Department – DFC SOP, Section 300 - Privacy Policy to all DFC personnel, non-agency personnel who provide services to DFC and to each source agency and DFC authorized user who will be notified of their required compliance with provisions of this policy. The Dallas Fusion Center Privacy Policy is available for review at the Dallas Police Department website - www.dallaspolice.net.

F. All DFC personnel, participating agency personnel, personnel providing information technology services to the agency, private contractors, and other authorized participants shall comply with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to the U.S. and Texas Constitutions, federal law, state law, and municipal ordinances addressing privacy, civil rights, and civil liberties legal requirements applicable to DFC and/or other participating agencies, including the Texas Public Information Act, Chapter 552, Texas Government Code.

G. All DFC personnel, participating agency personnel, personnel providing information technology services to DFC, private contractors, and any other authorized users will comply with the Privacy Policy concerning information and intelligence the DFC collects, gathers, receives, maintains, accesses, or discloses to such persons (including ISE participating agencies), homeland security and public safety agencies, and private partners.

H. The DFC has adopted internal operating policies that comply with applicable law cited above.

303 – Data Quality Assurance

A. All data maintained by DFC will be accurate, complete, current, and verifiable. DFC will check information and intelligence submitted from within the Department, as well as from outside agencies to ensure compliance with this data quality principle. Information identified as inaccurate will be immediately removed from all records.

B. Once information is collected and DFC has determined it will be retained, the information will be assessed to determine its nature, usability and quality, and will be

assigned to appropriate information categories reflecting the assessment, and labeled pursuant to applicable limitation on access and level of disclosure in order to protect confidential sources and police undercover techniques and methods.

C. Information will also be classified and labeled in order to protect an individual's right of privacy, civil rights, and civil liberties, to indicate whether the information is subject to specific information privacy or other similar restrictions on access, use, or disclosure and, if so, the nature of the restrictions, and any legally required protections based on the individual's status as a victim of a crime or as a witness. Such classifications shall be reevaluated whenever new information is added that affects access status, limitations or sensitivity of disclosure, or a change occurs in the use of the information affecting such access or disclosure limitations. Access classification will also be used to control dissemination.

D. DFC will identify and review protected information held by the DFC prior to sharing information through the Information Sharing Environment (ISE) in order to ensure DFC provides notice as stated in DFC SOP, Subsection 303 - Data Quality Assurance, Section C.

E. DFC requires certain basic descriptive information to be entered and electronically associated with data (or content) for which special laws, rules or policies regarding access, use, and disclosure have been established. These types of information include:
- Name of the originating department, component, and subcomponent
- Name of the agency's justice information system from which the information is disseminated
- Date the information was gathered or collected, and where feasible, the date its accuracy was last verified
- Title and contact information for the person to whom questions regarding the information should be directed.

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

G. DFC will keep a record of the source of all information retained by the DFC.

H. DFC participating agencies remain the owners of the data contributed by each participating agency and are, therefore, responsible for the quality and accuracy of data provided to the DFC. The DFC will make every reasonable effort to seek and retain only information that is derived from credible sources and is accurate, current, and complete. Such information, other than SAR and ISE-SAR information (not merged), will be

merged with existing information pertaining to an individual or organization only when sufficient identifying information is available to reasonably conclude the information is about the same individual or organization. An audit trail will be kept of access by or dissemination of the information to all recipients. In accordance with this policy, all information will, when retained, be labeled as accurate, complete, current, verifiable and/or reliable regarding its level of quality.

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

J. Labeling of retained information will be reevaluated when new information is gathered that has an impact on the confidence (validity and reliability) in previously retained information.

K. DFC will make every reasonable effort to ensure that information will be corrected, deleted from the system, or not used when the DFC learns the information is erroneous, misleading, obsolete, or otherwise unreliable; the source of the information did not have authority to gather or collect the information or to provide the information to the DFC; or the source used prohibited means to gather or collect the information (except when the source did not act as an agent to a bona fide law enforcement officer.)

L. The DFC will advise the appropriate contact person within the originating agency, in writing, when data submitted to DFC by that agency is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

M. The DFC will use written or documented electronic notification to inform all recipient agencies when information previously provided to the recipient agency is deleted or changed by the DFC; for example, when the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

304 – Limitations on Disclosure and Use

A. Access to or disclosure of information or intelligence retained by the DFC will be provided to only authorized persons in governmental agencies for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes, and only for the performance of official duties in accordance with applicable law and procedures. An audit trail sufficient to allow the identification of each individual who accessed information retained by the DFC and the nature of the information accessed will be kept by the DFC.

1. Disclosure of Information - DFC will only disseminate information to personnel assigned to the DFC or in other governmental agencies who are authorized by law to have access for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes in accordance with a "right to know," and who will use the information only in the performance of official duties where the recipient can demonstrate a "need to know." See DPD – Dallas Fusion Center SOP, Section 300, Appendix A for definitions of "right to know" and "need to know" as defined by this policy.

2. Disclosure of Criminal Intelligence
   a. Intelligence obtained from or through DFC can only be used for lawful purposes. A lawful purpose means the request for information can be directly linked to a criminal justice agency's active criminal investigation, an intelligence organization's activities or operations as authorized by legal statute in support of national security and/or homeland security, or is a response to confirmed information that requires intervention to prevent a criminal act or threat to public safety. All information disseminated from the DFC related to criminal activity must be relevant and useful in aiding an authorized and active criminal or background investigation.

   b. DFC shall not confirm the existence or nonexistence of criminal intelligence to any person, agency, or organization not authorized to access, receive, or use the information.

B. DFC reserves the right, with approval from the Dallas Police Department Chief of Police, or his/her designee, to determine qualifications and restrict the number of personnel granted direct access to DFC information and intelligence. Access to information and intelligence contained with DFC databases will be granted only to DFC and authorized Participating Agency user personnel who have been screened with a state and national fingerprint-based background check, as well as any additional background screening processes using procedures and standards established by an individual Participating Agency. Each individual user obtaining information will be notified in writing that he/she remains solely responsible for the interpretation, further dissemination, and use of the information 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. Further access is limited to legitimate law enforcement, public protection, including homeland security, public prosecution, public health or justice purposes, and only in the performance of official duties in accordance with the law and policies applicable to the agency that employs each individual user.

C. Participation by each partner agency in DFC programs and determination of databases controlled by a partner agency that will be made available to DFC are voluntary decisions. Data contained within each database utilized by DFC will comply with all applicable laws and regulations of the DFC and participating partner agencies. Additionally, all information gathered and investigation techniques used by the DFC and its participating partner agencies will comply with all applicable law.

D. The DFC will not knowingly receive, seek, accept or retain information from an individual or non-government information provider, including commercial data providers, if the DFC knows or has reason to believe the individual or information provider obtained specific information that could not be legally obtained by the DFC. The DFC will ensure the provider has taken the steps necessary to be authorized to collect the information. In addition, commercial data providers shall provide assurance that the data was lawfully gathered using methods not based on misleading information collection practices. The DFC will only pay a fee or benefit for information provided by authorized commercial database entities or paid informants authorized under applicable Dallas Police Department and DFC policies, and will not directly or indirectly seek, receive, accept, or retain information from a provider that is legally prohibited from obtaining or disclosing the information.

E. The DFC will not allow original materials gathered or collected under these policies to be removed from the DFC unless necessary to be used as evidence in a criminal matter, with the exception of removal in accordance with applicable laws and records retention policies.

F. In order to maintain the integrity of the DFC, any information obtained through the DFC must be independently verified with the source from which the data originated prior to any official action being taken.

G. DFC supervisors, further reserve the right to conduct internal inspections or audits concerning the proper use of information and intelligence provided by the DFC and compliance with the DFC Privacy Policy.

H. DFC will, in consultation with the Unit Commander and under Dallas Police Department and City of Dallas rules and regulations, develop and implement a consistent sanction policy for DFC personnel who fail to comply with this Privacy Policy.

I. Intelligence and information disseminated by the DFC will be authorized on a ‘need to know’ and ‘right to know’ basis in accordance with applicable laws, rules and regulations. All personnel who receive, handle, or have access to DFC data will receive training regarding these requirements. The DFC will use credentialed, role-based access criteria, as appropriate, to control information access, authority to add, change, delete, or

print, and to whom the information can be disclosed and under what circumstances. All personnel with access to DFC data must abide by the following rules:

1. DFC data will be used only in support of official law enforcement or intelligence activities in a manner authorized by the requestor's employer.

2. Use of DFC data in an unauthorized or illegal manner may subject the requestor to denial of further use of the DFC; discipline by the requestor's employing agency, and/or criminal prosecution.

J. DFC reserves the right to suspend, deny or withhold service to any personnel violating the privacy policy.

K. Individual users of the DFC's information remain responsible for the lawful and appropriate use of the information and intelligence provided by the DFC. Failure to abide by the restrictions and use limitations for DFC's data may result in the suspension or termination of individual user privileges, disciplinary sanctions imposed by the user's employing agency, or criminal prosecution. Each individual user and agency participating in the DFC is required to abide by this privacy policy in providing information and intelligence to the DFC and in the access, use, security, and disclosure of information and intelligence obtained by and through the DFC.

L. Information that would interfere with or compromise pending criminal investigations shall not be disseminated publicly unless required by law or as determined by the Dallas Chief of Police or his/her designee, and with agreement of all contributing agencies.

M. A participating agency will not disclose information originating from another agency except as authorized by the originating agency.

N. Members of the general public cannot access individually identifiable information on themselves or others from the DFC's databases unless disclosure is required by the Texas Public Information Act, Chapter 552, Texas Government Code. The DFC shall not confirm the existence or nonexistence of information to any person or agency that would not be eligible to receive the information itself, unless otherwise required by law. Persons wishing to access data pertaining to themselves should communicate directly with the agency or entity that is the source of the data in question. DFC will coordinate with source agencies to ensure appropriate handling of such requests. Responses to such requests shall be documented by the source agency, including what information, if any, was disclosed to a member of the public. The DFC Privacy Officer shall be the individual responsible for receiving, responding, and coordinating all responses to such inquiries and/or complaints regarding information held by DFC.

O. When information originated by DFC is required to be disclosed, DFC will follow the Texas Public Information Act, Chapter 552, Texas Government Code, with regard to verification of identity and requests for correction of information alleged to be inaccurate, incomplete, or otherwise deficient. An individual to whom information has been disclosed will be given reasons if requests for correction are denied by the DFC or originating agency, including ISE participating agencies. The individual will also be informed of the procedures for appeal when the DFC or originating agency has declined to correct challenged information to the satisfaction of the individual to whom the information relates. A record will be kept of all requests for corrections and all actions taken by DFC in response to these requests.

P. If an individual has a complaint or objection to the accuracy or completeness of terrorism-related protected information that has been or may be shared through the ISE that meets the following criteria: (a) held by the DFC; (b) allegedly has resulted in demonstrable harm to the complainant; and (c) is exempt from disclosure, the DFC will inform the individual of the procedure for submitting and resolving complaints or objections. All inquiries and complaints should be addressed to the DFC Privacy Officer at the following address:

Dallas Police Department,
Jack Evans Building,
Attn: DFC Privacy Officer
1400 S. Lamar St.
Dallas, TX 75215

Q. The DFC will acknowledge all complaints described in DFC SOP, Subsection 304 – Limitations on Disclosure and Use, Section O, and confirm the complaint will be reviewed, without confirming the existence of any information that is exempt from disclosure. If the information did not originate with the DFC, the DFC will notify the originating agency in writing and, upon request, assist such agency to correct or purge any identified data/record deficiencies or to verify the record is accurate. Any personal information originating with the DFC will be reviewed and corrected in or deleted from DFC data/records, if the information is determined to be erroneous, to include incorrectly merged or outdated information. A record will be kept of all complaints or requests for corrections and the resulting actions taken by the DFC.

R. The DFC delineates protected information shared through the ISE from other data, by maintaining records of agencies that have shared terrorism-related information using audit logs and employing system mechanisms to identify the originating agency for specific shared information.

305 – Security Safeguards

A. Information obtained from or through DFC will not be used or publicly disclosed for purposes other than those specified by the DFC. Information cannot be:

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

2. Disclosed or published without prior approval from DFC; or

3. Used for any purpose that is inconsistent with or violates all applicable statutes, rules, policies or procedures which govern the DFC and its participating agencies; or

4. Disseminated to unauthorized persons.

B. Only DFC personnel who have been selected, approved, and trained accordingly will have access and/or use of the DFC's data and information. Access to DFC information will be granted only to fully authorized DFC personnel who have successfully completed a Dallas Police Department background check and received appropriate Dallas Police Department clearance, if applicable. DFC personnel must complete an Individual User Agreement after receiving training, but prior to, accessing DFC data and information.

C. The Unit Commander and DFC supervisors will ensure adherence to all applicable security measures for the operation of the DFC within a secure facility with protections from external intrusion. Additionally, DFC will utilize secure internal and external safeguards against network intrusions. Access to DFC databases from outside the facility will only be permitted over secure networks, in compliance with Dallas Police Department, City of Dallas, and current and accepted industry security standards.

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

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

F. Queries made to DFC data applications will be logged into the data system where each user initiating a query is identifiable.

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

H. The DFC will notify any individual about whom the DFC has reason to believe personal information regarding that person has been breached or obtained by an unauthorized person or organization, where a reasonable belief exists that access to the information may threaten physical, reputational, or financial harm to the subject of the breach. Notice will be made without unreasonable delay, following discovery by or notification to DFC of an unauthorized access, and in compliance with legitimate needs of law enforcement to investigate actions that resulted in the unauthorized release or any measures necessary to determine the scope of the release of information, and if necessary, to reasonably restore the integrity of any affected information system.

306 – Accountability

A. The DFC Unit Commander will designate in writing the DFC Privacy Officer who is responsible for compliance with the DFC Privacy Policy. The Privacy Officer will receive appropriate training for review and determination of practices, procedures, and actions that may violate the DFC Privacy Policy. The Privacy Officer shall receive and investigate possible violations of DFC policies relating to protected information, and reports of alleged errors in information and intelligence. The Privacy Officer will also coordinate error resolution, serve as the DFC liaison for the Information Sharing Environment (ISE), and coordinate with other fusion centers throughout the fusion center network. The Privacy Officer will have access to and be accountable for DFC data to ensure:

1. DFC personnel and authorized participating agency employees access and disseminate personally identifiable information (PII) in accordance with the DFC Privacy Policy,

2. System logs that document access and dissemination of PII are being utilized and maintained,

3. DFC assigned personnel are trained in the requirements of the DFC Privacy Policy, to include:
   a. DFC requires all assigned personnel to participate in training programs regarding implementation of and adherence to privacy, civil rights and civil liberties policies pertaining to PII and other protected information, and
   b. The DFC will provide special training to personnel authorized to share protected information through the ISE regarding the DFC's requirements and policies for collection, gathering, use, and sharing of such information, and
   c. The DFC's Privacy Policy training program will cover:
   - Purposes of the privacy, civil rights, and civil liberties protection policy

- Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing and disclosure of information retained by the DFC
- How to implement the policy in the day-to-day work of the user, whether information is accessed via electronic or paper transmission,
- The impact of improper activities associated with infractions within or through the DFC
- Mechanisms for reporting violations of DFC/agency privacy protection policies
- The nature and possible penalties for policy violations, including possible transfer, dismissal, criminal liability, and immunity, if any.

B. DFC Supervisors will be responsible for ensuring a yearly audit is conducted for compliance with 28 CFR Part 23, applicable federal and state laws, statutes, or regulations, and this privacy policy. All confirmed or suspected violations detected by this audit will be reported to the Unit Commander. All recommendations for improved procedures and processes will also be reported to the Unit Commander. These audits will be mandated and a record of the audits will be maintained by the DFC Privacy Officer.

C. It is the intent of the DFC to be open with the public concerning data collection practices when such openness will not jeopardize ongoing criminal investigative activities. This policy will be posted on the Dallas Police Department website - www.dallaspolice.net.

D. All agencies participating in the DFC will make this Privacy Policy available to the public upon request.

E. The DFC's personnel or other authorized users shall report violations or suspected violations of DFC policies relating to protected information to the DFC Privacy Officer.

F. The DFC Privacy Officer will establish a privacy policy review committee to annually review changes in law and experiences in implementation of this policy and make recommendations for changes to the Dallas Police Department Chief of Police, or designee.

307 – Record Retention

A. The DFC will comply with all applicable federal, state and local statutes, ordinances, rules, and applicable originating agency policies regarding the retention of records held by the DFC.

B. All information held by the DFC will be subject to ongoing review by the Unit Commander. Information that is misleading, obsolete, irrelevant to ongoing criminal investigations, or otherwise unreliable will be immediately purged, with no requirement

for approval of the originating agency, from the DFC information system. The DFC will notify originating agencies in writing of all alleged errors, changes made, and data purged.

C. The DFC will maintain a record of information to be reviewed for retention and will identify any information with pending expiration dates. Notification will not be made to originating agencies for submitted information held at the DFC with pending expiration dates. Prior to the expiration date, it is the responsibility of the originating agency or any other agency partner to validate information with a pending expiration date by providing an update or supplement to the information to prevent it from being purged from DFC systems. All DFC purges of expired information will be performed with no requirement for approval from an originating agency.

D. Criminal intelligence information retained after the DFC ongoing review or originating agency review must reflect the name of the reviewer, date of review, and reason for retention, in accordance with 28 CFR Part 23. Ongoing review of all information will continue until the expiration of the retention period.

E. The retention period of all information held by the DFC will be no longer than five years unless validated for an additional retention period prior to its expiration.

308 – Collation and Analysis

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

B. Information subject to collation and analysis is "information" as defined in DFC SOP, Section 300, Appendix A – Terms and Definitions.

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

1. Further crime prevention, including terrorism, enforcement, force deployment, or prosecution objectives and priorities established by the DFC, and

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

Section 300, Appendix A - Terms and Definitions

The definitions in DFC SOP, Section 300 – Privacy Policy shall also apply to the entirety of the DFC SOP.

Access - Data access is the ability to view (usually with permission to use) particular data on a computer or computer system. Web access enables the user to have a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only or read/write access.

Acquisition - Acquisition refers to the means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports, or to the receipt of information shared by another ISE participant who originally acquired the information.

Audit Trail - A generic term for recording (logging) a sequence of activities. More expansive audit trail mechanisms would record each user's activity in detail - what commands were issued to the system, what records and files were accessed or modified, etc.

Civil Liberties - Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. Civil Liberties are freedoms guaranteed by the Bill of Rights - the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Civil Rights - The term "civil rights" is indicates governments have a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, civil rights are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Computer Security - The protection of information assets made available through the use of computing technology, processes, and training.

Confidentiality – Obligation of individuals and institutions to use information under their control appropriately once it has been disclosed to them. Each individual or agency observes rules of confidentiality out of respect for and to protect and preserve the privacy of others.

Criminal Intelligence - Information that has been collected, analyzed, and developed with a purpose of advising and assisting law enforcement and partner agencies in combating crime.

Disclosure - The release, transfer, sharing, publication, or divulging of personal information in any manner - electronic, verbal, or in writing - to an individual, agency, or organization outside the collection agency. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes, and is not available to everyone.

Fair Information Principles - The Fair Information Principles (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. While these principles were developed around commercial transactions and the trans-border exchange of information, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that must be performed with a regard to privacy within integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system.

The eight FIPs are:

1. Collection Limitation Principle
2. Data Quality Principle
3. Purpose Specification Principle
4. Use Limitation Principle
5. Security Safeguards Principle
6. Openness Principle
7. Individual Participation Principle
8. Accountability Principle

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. General information or data is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. This information may be either resolved or unresolved, with the record 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.

Information - Any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be

categorized into four general areas: general data, including investigative information; tips and leads data; suspicious activity reports; and criminal intelligence information. Such data may comprise personally identifiable information.

Need to Know - Determination made by a possessor of sensitive information that as a result of an individual's official duties, a jurisdictional, organizational, or operational necessity exists that requires a prospective recipient to be provided access to sensitive information or intelligence for the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

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

Participating Agency - Refers to any criminal law enforcement agency that agrees to comply with the DFC Privacy Policy and receive or submit information or intelligence from or to the DFC.

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

- Personal characteristics (such as height, weight, gender, 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, biometrics information such as fingerprints, DNA, and retinal scans).
- A unique set of numbers of characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Fingerprint Identification Systems [AFIS] identifier, or booking or detention system number)
- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).
- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Right to Know – Legal entitlement for an individual or organization who can demonstrate that access to sensitive information and intelligence is necessary for the official performance of a law enforcement, homeland security, or counterterrorism activity.